

ВЕДЬ ЭТО ТАК ПРОСТО!



Блокчейн

для
Чайников[®]

Издательство ДИАЛЕКТИКА



Оцените
потенциальные
возможности блокчейна

Узнайте, как блокчейн может
улучшить ваш бизнес

Выясните, как использовать
блокчейн для защиты своих
данных

Тиана Лоуренс

Сооснователь компании Factom



Блокчейн

для
чайников[®]
Издательство ДИАЛЕКТИКА



Blockchain

by Tiana Laurence

for
dummies[®]
A Wiley Brand



Блокчейн

Тиана Лоуренс

для
чайников[®]
Издательство ДИАЛЕКТИКА



Москва ♦ Санкт-Петербург ♦ Киев
2018

ББК 32.973.26-018.2.75
Л81
УДК 681.3.07

Компьютерное издательство “Диалектика”
Главный редактор *С.Н. Тригуб*
Перевод с английского и редакция *А.В. Слепцова*

По общим вопросам обращайтесь в издательство “Диалектика” по адресу:
info@dialektika.com, <http://www.dialektika.com>

Лоуренс, Тиана.

Л81 Блокчейн для чайников. : Пер. с англ. — СПб. : ООО “Альфа-книга”, 2018. — 272 с. : ил. — Парал. тит. англ.

ISBN 978-5-9500295-6-1 (рус.)

ББК 32.973.26-018.2.75

Все названия программных продуктов являются зарегистрированными торговыми марками соответствующих фирм.

Никакая часть настоящего издания ни в каких целях не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитный носитель, если на это нет письменного разрешения издательства John Wiley & Sons, Inc.

Copyright © 2018 by Dialektika Computer Publishing.

Original English language edition Copyright © 2017 by John Wiley & Sons, Inc., Hoboken, New Jersey.

All rights reserved including the right of reproduction in whole or in part in any form. This translation is published by arrangement with John Wiley & Sons, Inc.

Wiley, For Dummies, the Dummies Man logo, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Научно-популярное издание

Тиана Лоуренс

Блокчейн для чайников

В издании использованы карикатуры банка изображений Cartoonbank.ru

Литературный редактор *Л.Н. Красножон*

Верстка *Л.В. Чернокозинская*

Художественный редактор *В.Г. Павлютин*

Корректор *Л.А. Гордиенко*

Подписано в печать 19.02.2018. Формат 70х100/16.

Усл. печ. л. 21,9. Уч.-изд. л. 14,8.

Тираж 500 экз. Заказ № 1598.

Отпечатано в АО “Первая Образцовая типография”

Филиал “Чеховский Печатный Двор”

142300, Московская область, г. Чехов, ул. Полиграфистов, д. 1

Сайт: www.chpd.ru, E-mail: sales@chpd.ru, тел. 8 (499) 270-73-59

ООО “Альфа-книга”, 195027, Санкт-Петербург, Магнитогорская ул., д. 30, лит А, пом. 848

ISBN 978-5-9500295-6-1 (рус.)

© Компьютерное изд-во “Диалектика”, 2018,
перевод, оформление, макетирование

ISBN 978-1-119-36559-4 (англ.)

© John Wiley & Sons, Inc., Hoboken, New Jersey, 2017

Оглавление

Введение	15
Часть I. Введение в блокчейн-технологию	19
Глава 1. Знакомьтесь: блокчейн	21
Глава 2. Выбираем тип блокчейна	33
Глава 3. Пробуем блокчейн в работе	43
Часть II. Углубляем свои знания	59
Глава 4. Знакомьтесь: блокчейн Биткойна	61
Глава 5. Встречайте: блокчейн Эфириум	75
Глава 6. Поговорим о блокчейне Ripple	93
Глава 7. Новый подход: блокчейн Factom	105
Глава 8. Майнинг по-новому: DigiByte	123
Часть III. Мощные блокчейн-платформы	133
Глава 9. Консорциум Hyperledger: ведущая сила блокчейн-технологии	135
Глава 10. Используем Microsoft Azure	147
Глава 11. Выясняем возможности платформы IBM Bluemix	159
Часть IV. Блокчейн и экономика, право, государство	171
Глава 12. Финансовые технологии	173
Глава 13. Управление недвижимостью	187
Глава 14. Страхование	199
Глава 15. Блокчейн и государство	209
Глава 16. Прочие применения блокчейна	225
Часть V. Великолепные десятки	237
Глава 17. Десять бесплатных блокчейн-ресурсов	239
Глава 18. Десять правил, которые никогда не следует нарушать в мире блокчейна	245
Глава 19. Десять самых интересных блокчейн-проектов	255
Предметный указатель	265

Содержание

Об авторе	13
Посвящение	14
Благодарности	14
Введение	15
Об этой книге	15
Предположения автора	16
Условные обозначения, принятые в этой книге	17
Пиктограммы, используемые в этой книге	17
Что делать дальше	18
От издательства “Диалектика”	18
Часть I. Введение в блокчейн-технологии	19
Глава 1. Знакомьтесь: блокчейн	21
Начнем с начала: что такое блокчейн-технология	22
Как функционирует цепь блокчейна	23
Почему блокчейн-технология так важна	24
Структура блокчейн-цепи	25
Блокчейн-приложения	26
Этапы развития блокчейн-технологии	27
Консенсус: правящая сила блокчейна	28
Блокчейн-технология в действии	29
Существующие применения блокчейн-технологии	30
Будущее блокчейн-приложений	31
Глава 2. Выбираем тип блокчейна	33
Где блокчейн может быть полезен	34
Определяем свои потребности	34
Формулируем цели	36
Выбираем решение	36
Строим дерево решений блокчейна	38
Составляем план	40
Глава 3. Пробуем блокчейн в работе	43
Начнем с блокчейна биткойна	44
Создаем первый биткойн-кошелек	45
Создаем второй биткойн-кошелек	45

Генерируем красивый биткойн-адрес	46
Пересылаем красивый адрес	47
Делаем запись в блокчейне биткойна	48
Читаем запись в блокчейне биткойна	49
Смарт-контракты на базе биткойна	49
Создаем первое смарт-обязательство	50
Проверяем статус контракта	54
Docker: создаем частную блокчейн-сеть в Эфириум	54
Готовим компьютер к работе	55
Создаем собственный блокчейн	56
Часть II. Углубляем свои знания	59
Глава 4. Знакомьтесь: блокчейн Биткойна	61
Краткая история блокчейна Биткойна	62
Некоторые заблуждения в отношении Биткойна	67
Биткойн: новый Дикий Запад	68
Поддельные сайты	69
Нет, сначала вы!	69
Схемы быстрого обогащения	70
Майнинг биткойнов	70
Создаем первый бумажный кошелек	72
Глава 5. Встречайте: блокчейн Эфириум	75
Знакомимся с историей появления и развития Эфириума	76
Эфириум: Всемирный компьютер с открытым кодом	78
Децентрализованные приложения: добро пожаловать в будущее	79
Сила децентрализованных автономных организаций	79
Взлом блокчейна	83
Познакомимся ближе со смарт-контрактами	83
Знакомьтесь: криптовалюта “эфир”	84
Подключаемся и начинаем работать в Эфириуме	85
Майнинг эфиров	85
Получаем эфириум-кошелек	86
Создаем свою первую децентрализованную автономную организацию	87
Тестовая сеть и обсуждение	88
Управление и голосование	89
Поговорим о будущем децентрализованных организаций	90
Вкладываем деньги в DAO	91
Создаем более “умные” смарт-контракты	91
Ищем информацию об ошибках в системе	92

Глава 6. Поговорим о блокчейне Ripple	93
Краткая история блокчейна Ripple	94
Ripple: здесь все вертится вокруг доверия	96
Чем система Ripple отличается от других блокчейнов	97
Открываем для себя всю мощь системы Ripple	100
Некоторые предупреждения относительно системы Ripple	102
Глава 7. Новый подход: блокчейн Factom	105
Вопрос доверия	106
Назначение блокчейна Factom: публикация чего угодно	108
Стимулы к объединению	109
Создание приложений в среде Factom	113
Аутентификация документов и обеспечение подлинности с использованием API	113
Знакомимся с криптовалютой Factoid: необычный токен	114
Привязывание приложений	114
Помещение информации в систему Factom	115
Повышение прозрачности в ипотечной индустрии	117
Проверка физических документов: dLoc и Factom	120
Глава 8. Майнинг по-новому: DigiByte	123
Знакомимся с DigiByte: быстрый блокчейн	124
Майнинг в системе DigiByte	125
Подписывание документов в сервисе DiguSign системы DigiByte	129
Зарабатываем токены DigiByte играя	130
Часть III. Мощные блокчейн-платформы	133
Глава 9. Консорциум Hyperledger: ведущая сила блокчейн-технологии	135
Знакомимся с Hyperledger: мечты о гипербудущем	136
Сосредоточимся на приложении Fabric	138
Создание собственной системы в среде Fabric	139
Работа с контрактами типа Chaincode	139
Исследуем проект Iroha	142
Знакомьтесь: Sumeragi, новый алгоритм консенсуса	142
Разработка мобильных приложений	143
Блокчейн-платформа Sawtooth Lake	144
Алгоритм консенсуса платформы: Proof of Elapsed Time	145
Развертывание среды разработки Sawtooth	146

Глава 10. Используем Microsoft Azure	147
Bletchley: модульная блокчейн-“материя”	148
Криплеты для шифрования и аутентификации	149
Криплеты типа Utility и Contract, функция CryptoDelegate	151
Создание приложений в экосистеме Microsoft Azure	152
Начинаем работу с Chain в Azure	154
Установка среды программирования Chain	154
Создание собственной закрытой сети	155
Использование финансовых служб Chain в Azure	156
Развертывание блокчейн-инструментов в Azure	156
Использование Эфириума в Azure	156
Cortana: аналитический инструмент машинного обучения	157
Визуализация данных посредством Power BI	158
Управление доступом в Azure с использованием Active Directory	158
Глава 11. Выясняем возможности платформы IBM Bluemix	159
Бизнес-блокчейны в среде Bluemix	160
Ваша собственная изолированная среда	161
Примеры использования Bluemix	162
Умный блокчейн в системе Watson	163
Построение собственной стартовой сети в Big Blue	166
Часть IV. Блокчейн и экономика, право, государство	171
Глава 12. Финансовые технологии	173
Заглянем в хрустальный шар: новые тренды в банковском деле	174
Быстрый перевод денег: без границ и прочих помех	176
Создание перманентной истории	177
Выход на международную сцену: глобальные финансовые продукты	179
Начисление зарплаты без границ	180
Торговля быстрее и лучше	181
Гарантированные платежи	182
Микроплатежи: новая природа транзакций	182
Вытеснение мошенничества	183
Глава 13. Управление недвижимостью	187
Исключение титульного страхования	188
Защищенные отрасли	189
Клиенты ипотеки и “Фанни Мей”	191
Ипотека в мире блокчейна	192
Сокращение стоимости получения кредита	192
Знай свой последний известный документ	193

Прогнозирование региональных тенденций	194
Соединенные Штаты Америки и Европа: перегруженность инфраструктуры	195
Китай: первый, кто вышел за ворота	196
Развивающийся мир: блокпосты на пути к блокчейну	197
Глава 14. Страхование	199
Точный раскрой страхового покрытия	200
Индивидуальное страхование	200
Новый мир микрострахования	201
Свидетельство для вас: Интернет вещей	203
Проекты Интернета вещей в области страхования	203
Последствия появления действительно больших данных	204
Устраняем третью сторону из страхования	205
Децентрализованная безопасность	205
Краудфандинговое страховое покрытие	206
Использование DAO как системы страхования	207
Глава 15. Блокчейн и государство	209
Смарт-города в Азии	210
Города-спутники в Индии	211
Китай и проблема больших данных	213
Битва за статус финансовой столицы мира	214
Первые блокчейн-инициативы Лондона	215
Регулируемая песочница Сингапура	216
Инициатива “Дубай-2020”	217
Регулирование посредством битлицензий: город Нью-Йорк	219
Блокчейн на защите границ всего мира	220
Министерство внутренней безопасности и идентичность вещей	221
Паспорта будущего	222
Новый тип документов	222
Глава 16. Прочие применения блокчейна	225
Правительства, отклонившиеся от общепринятых (пока) норм	226
Сингапурский проект смарт-нации	227
Эстонская инициатива электронного резидентства	227
Повышение качества нотариальных услуг в Китае	229
Доверительный уровень для Интернета	230
Электронная почта без спама	230
Владение собственным свидетельством идентичности	231
Источники информации и блокчейн-технология	232
Доверенное авторство	233
Права на интеллектуальную собственность	234

Часть V. Великолепные десятки	237
Глава 17. Десять бесплатных блокчейн-ресурсов	239
Университет корпорации Factom	240
Сайт Ethereum 101	240
Разработки в сети Ripple	240
Программируемые деньги на основе Ripple	241
Информация о проекте DigiByte	241
Университет блокчейн-технологии	242
Основы системы Биткойн	242
Блокчейн-альянс	242
Блог Multichain	243
Платформа HiveMind	243
Глава 18. Десять правил, которые никогда не следует нарушать в мире блокчейна	245
Не используйте криптовалюты или блокчейн-приложения, чтобы обойти требования закона	246
Делайте свои контракты настолько простыми, насколько это возможно	247
Публикуйте данные с осторожностью	248
Сохраняйте, делайте резервные копии и тщательно оберегайте свои закрытые ключи	248
Трижды проверяйте все адреса, прежде чем отправлять на них валюту	250
Пользуйтесь биржами с осторожностью	251
Относитесь к сетям Wi-Fi с осторожностью	251
Тщательно выбирайте блокчейн-разработчиков	252
Не дайте обвести себя вокруг пальца	252
Не занимайтесь торговлей токенами, если вы не вполне понимаете, как это делается	253
Глава 19. Десять самых интересных блокчейн-проектов	255
Консорциум R3	256
Платформа T ZERO: расширение фондового рынка	257
Распределенные системы компании Blockstream	258
Блокчейн проекта OpenBazaar	259
Ищем себе кодировщика: компания Code Valley	260
Цифровые активы компании Bitfury	260
На ShapeShift есть любые монеты	261
Приложения машинных платежей от компании 21	262
Анонимные транзакции в системе Dash	263
Компания ConsenSys: децентрализованные приложения	264
Предметный указатель	265

Об авторе

Тиана Лоуренс является сооснователем компании *Factom, Inc.* и одним из первых энтузиастов биткойна. Ее страсть — растущие компании, занимающие передовые позиции в своих сегментах. Будучи неутомимым предпринимателем, Тиана начала заниматься бизнесом уже в 16 лет. Позднее она получила степень бакалавра в области ведения бизнеса и лидерства в Портлендском государственном университете. Тиана любит помогать молодым целеустремленным предпринимателям познавать тонкости бизнеса и новейших технологий. Если она не занята своим бизнесом и не занимается с молодежью, ее, скорее всего, можно найти либо на пробежке где-нибудь неподалеку, либо в Остине, штат Техас, с увлечением лазающей по скалам.

Посвящение

Посвящается Кристал и Джессике за ободрение и поддержку во время написания этой книги.

Благодарности

Эта книга появилась как результат реализации идей и увлеченного труда многих людей. Ее просто было бы невозможно написать, если бы не полная открытость и поддержка со стороны мира криптовалют и блокчейна. Особо я хотела бы поблагодарить Поля Сноу (Paul Snow), Петера Кирби (Peter Kirby), Брайана Дири (Brian Deery) и Дэвида Джонстона (David Johnston) за те бесчисленные часы, которые они провели, обучая меня тонкостям блокчейна и криптографии. Я также хотела бы поблагодарить Эбхи Добхала (Abhi Dobhal), Лоуренса Руфрано (Lawrence Rufrano), Риана Фаггера (Ryan Fugger), Чарли Купера (Charley Cooper), Элайзу Киллин (Alyse Killeen), Джереми Канда (Jeremy Kandah), Клеменса Вэна (Clemens Wan), Грегга Уоланса (Greg Wallace), Брайана Белендорфа (Brian Behlendorf), Эмира Четрит (Amir Chetrit), Джареда Тейта (Jared Tate), Кейси Лоулора (Casey Lawlor) и Скотта Робинсона (Scott Robinson) за их указания и рекомендации в отношении эволюционирующего мира блокчейна, а также за то, что они при всей своей занятости нашли время на вычитку и устранение ошибок в моей работе.

Также эта книга потребовала немалых редакторских усилий. Я не шучу: редакторы действительно потратили на нее много сил и времени. Мой главный редактор, Элизабет Кубал (Elizabeth Kuball), не раз помогала мне сосредоточиться на этом проекте и напоминала о графике, которого следует придерживаться, а Стив Хайес (Steve Hayes), мой выпускающий редактор, сделал все возможное, чтобы эта книга вышла в свет. Я еще раз благодарю Скотта Робинсона, на этот раз — за тщательную вычитку макета и важные замечания, а также Пэта О. Брайена и других членов выпускающей команды — за всю неблагодарную работу по приведению этой книги в надлежащий вид. Я всегда буду перед ними в долгу.

Введение

Добро пожаловать! Вас приветствует *Блокчейн для чайников*! Если вы хотите понять, что такое блокчейн и как его можно использовать, эта книга — именно то, что вам нужно. Многие люди полагают, что блокчейн — это что-то весьма трудное для понимания. Они даже могут считать, что блокчейн — это нечто схожее с криптовалютами, подобно биткойну, хотя на самом деле блокчейн — это нечто гораздо большее. И при этом любой человек в состоянии овладеть основами блокчейн-технологии.

В этой книге вы найдете полезные советы и необходимые разъяснения, чтобы суметь проложить собственный путь в мире блокчейна и основанных на нем криптовалют. Здесь также представлены практические пошаговые руководства, которые позволят вам достичь полного понимания того, как блокчейн работает и где его можно с пользой применить. Для того чтобы освоить материал этой книги, вам вовсе необязательно разбираться в программировании, экономике или международных отношениях, хотя речь обо всем этом действительно пойдет на ее страницах, поскольку блокчейн-технология находит свое применение в каждой из этих областей.

Об этой книге

В этой книге рассматриваются основы блокчейн-технологии, смарт-контрактов и криптовалют. Вы, вероятно, выбрали эту книгу потому, что уже что-то слышали о блокчейне и понимаете важность этой технологии, но не представляете, что же это такое на самом деле, как это работает и почему этим стоит заниматься. Здесь вы найдете ответы все эти вопросы, сформулированные так, чтобы у вас не возникало сложностей в их понимании.

Эта книга немного отличается от остальных книг о блокчейнах, представленных на книжном рынке. Здесь вы найдете обзор всех ключевых практических реализаций блокчейн-технологии, доступных в сети на момент издания книги, с пояснениями в отношении того, как они работают, для чего предназначены и как их можно опробовать на практике прямо сегодня.

Здесь рассмотрены все аспекты блокчейн-технологии и даны указания в отношении некоторых ключевых моментов, о которых следует помнить при развертывании собственных блокчейн-проектов. Кроме того, здесь представлены подсказки о том, как установить эфириум-кошелек, создать и установить смарт-контрат, как выполнять операции с биткойном и валютой “фактом”, как зарабатывать на рынке криптовалют.

Вовсе необязательно читать эту книгу от корки до корки; можно ограничиться лишь той темой, которая вас интересует в данный момент.

И наконец, здесь вы встретите немало полезных веб-адресов. Если захотите посетить какой-то из указанных сайтов или ознакомиться с интересующим вас документом, просто наберите приведенный адрес в браузере на любом из ваших устройств, имеющих доступ к Интернету. Обратите внимание на то, чтобы адрес был набран в точности так, как приведено в книге (не забывайте, что в веб-адресах не может быть символов перевода строки). Если с момента выхода в свет этой книги указанный сайт не сменил свой адрес и продолжает функционировать, его содержимое появится в вашем браузере, хотя, возможно, в несколько ином виде, не таком, как на иллюстрациях. Что поделаешь, в мире нет ничего постоянного!

Предположения автора

Работая над книгой, я не делала каких-либо предположений по поводу наличия у читателя определенного опыта в криптографии, программировании или юриспруденции, однако я предполагала следующее.

- » У вас есть компьютер и доступ к Интернету.
- » У вас есть достаточные навыки и опыт работы с компьютером и пользования Интернетом.
- » Вы знаете, как работать с командными меню в программах.

Вы только знакомитесь с блокчейном и не являетесь опытным программистом. Если же мое последнее предположение неверно и для вас программирование — совсем не тайна за семью печатями, вы также найдете немало полезного в этой книге. Просто пропустите очевидные для вас пошаговые инструкции.

Условные обозначения, принятые в этой книге

В книге используются определенные соглашения, направленные на облегчение восприятия материала.

- » Адреса веб-сайтов и названия файлов указаны с помощью вот такого шрифта.
- » Названия элементов управления, представленных на экране компьютера в текстовом виде, выделяются в книге специальным рублевым шрифтом.

Пиктограммы, используемые в этой книге

В тех случаях, когда необходимо было подчеркнуть что-нибудь очень важное или особенное, на страницах слева я помещала приведенные ниже пиктограммы.



СОВЕТ

Эта пиктограмма сопутствует полезным советам в отношении того или иного обсуждаемого аспекта блокчейн-технологии. Отмеченные ею абзацы часто включают сведения, которые помогают достичь желаемого максимально быстро и эффективно.



ЗАПОМНИ

Такой пиктограммой помечается информация, которую непременно следует запомнить. Чтобы отфильтровать самую важную информацию в каждой главе, просто просмотрите все абзацы, помеченные этими пиктограммами.



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

Данной пиктограммой помечается более углубленная техническая информация, которую, в принципе, можно пропустить без особого вреда для понимания последующего материала. Однако интересующимся она поможет лучше понять те или иные особенности обсуждаемой темы.



ВНИМАНИЕ!

Назначение этой пиктограммы — предупредить вас: “Осторожно! Обратите внимание вот на это!” В книге так отмечены предупреждения о типичных ошибках и разных опасностях. Надеюсь, это поможет вам сохранить душевное равновесие и... свои токены.

Что делать дальше

Блокчейн-технологии можно применить для виртуализации бизнеса в любой сфере человеческой деятельности. Прямо сейчас наблюдается взрывной рост его использования в финансах, здравоохранении, страховании, государственных службах. И это только начало. В конечном счете измениться может весь наш мир, а возможности здесь просто бесконечны.

От издательства “Диалектика”

Вы, читатель этой книги, и есть главный ее критик. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересны любые ваши замечания в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо либо просто посетить наш веб-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится ли вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Отправляя письмо или сообщение, не забудьте указать название книги и ее авторов, а также свой обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию новых книг.

Наши электронные адреса:

E-mail: info@dialektika.com

WWW: <http://www.dialektika.com>

Наши почтовые адреса:

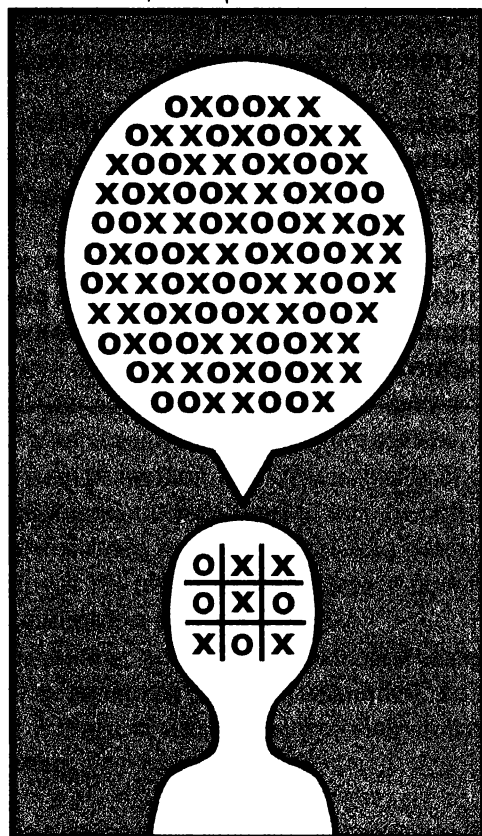
в России: 195027, Санкт-Петербург, Магнитогорская ул., д. 30, ящик 116

в Украине: 03150, Киев, а/я 152

Часть I

Введение в блокчейн- технологиию

© Конельницкий Игорь/cartonbank.ru



ПРОСТО -
О СЛОЖНОМ...

В ЭТОЙ ЧАСТИ...

- » Узнайте, что собой представляет блокчейн-технология, каковы ее особенности и какие преимущества она может дать вашей организации**
- » Ознакомьтесь с четырьмя типами блокчейн-технологии и четырьмя этапами разработки и реализации эффективного блокчейн-проекта**
- » Создайте собственные смарт-контракты в среде биткойна и определите, где эта технология может быть полезной в вашей организации**
- » Ознакомьтесь с инструментами, которые вам потребуются для подготовки и развертывания вашей приватной блоковой цепи (блокчейна) в среде криптовалюты “эфир”**



Глава 1

Знакомьтесь: блокчейн

В ЭТОЙ ГЛАВЕ...

- » Откройте для себя новый мир блокчейн-технологии
- » Уясните, почему это так важно
- » Познакомьтесь с тремя типами блоковых цепей — блокчейнов
- » Разберитесь в том, как работает блокчейн-технология

По своей сути *блокчейн* (или *блоковая цепь*) — это всего лишь термин из области компьютерных наук, определяющий, как в системе выполняются структурирование и обмен данными. Сегодня блокчейн-технологию расценивают как “пятый виток” в эволюции компьютерного мира.

Блокчейн-технология — это новый подход к построению распределенных баз данных. Эта инновация возникла как объединение новым способом ранее известных технологий. Блокчейн можно воспринимать как распределенную базу данных, которую контролирует группа индивидуумов с целью обеспечения совместного хранения информации и доступа к ней.

Существуют разные типы блокчейнов, т.е. блоковых цепей, а также блокчейн-приложений. Блокчейн-технология является всеохватывающей, т.е. интегрирующей в себе любые платформы и типы компьютерного оборудования, существующего в мире на данный момент.

Начнем с начала: что такое блокчейн-технология

Блокчейн (блоковая цепочка) представляет собой такую структуру данных, которая делает возможным создание цифрового распределенного журнала (или реестра) данных и организацию совместного доступа к нему в сети из независимых участников. Существуют различные типы блокчейн-цепей.

- » **Публичная блокчейн-цепь.** Публичные блокчейны (*public blockchains*), такие как Биткойн, представляют собой большую распределенную сеть, в которой запущен собственный токен. Присоединиться к ней может любой желающий и на любом уровне. Публичный блокчейн имеет открытый код, который поддерживается его сообществом.
- » **Эксклюзивная блокчейн-цепь.** Эксклюзивные блокчейны (*permissioned blockchains*), такие как Ripple (*Punl*), предполагают наличие центрального органа, определяющего все те действия, которые сторонним лицам разрешено осуществлять в этой сети. Это также большие распределенные системы, в которых используется собственный токен. Ядро их программного кода может быть как открытым, так и закрытым.
- » **Частная блокчейн-цепь.** Частные блокчейны (*private blockchains*), как правило, имеют относительно небольшой размер и обычно не предполагают использование токена. Их членский состав строго фиксирован, все транзакции отслеживаются и контролируются центральным органом. Это тот тип блокчейна, который предпочитают консорциумы, имеющие доверенных членов, манипулирующих конфиденциальной информацией.

Во всех трех типах блокчейна используется криптография, что позволяет каждому участнику любой отдельно взятой сети манипулировать своими активами совершенно безопасным способом, без необходимости иметь в ней какой-то центральный орган, уполномоченный обеспечивать безопасность ее функционирования. Исключение какого бы то ни было центрального органа из структуры базы данных — одна из наиболее важных и сильных сторон технологии блокчейна.



ЗАПОМНИ!

Технология блокчейна предполагает создание постоянных записей и истории транзакций, но ничего такого, что было бы реально постоянным. Постоянство записи основано на постоянстве сети.

В контексте блокчейн-технологии это означает, что при любой попытке изменения информации с этим должна согласиться большая часть блокчейн-сообщества, изначально мотивированная *не* изменять данные.

В результате, когда данные записаны в блокчейн-цепочку, изменить или удалить их невероятно сложно. Когда кто-то хочет добавить в цепь блокчейна запись, которую здесь принято называть *транзакцией* или *входными данными*, пользователи в сети, контролирующие достоверность операций, проверяют предложенную транзакцию. И как раз здесь все усложняется, поскольку в каждой реализации блокчейн-цепи ее создатели имеют свой, несколько отличающийся от прочих, взгляд на то, как это должно происходить и кто имеет право проверять транзакции.

Как функционирует цепь блокчейна

Цепь блокчейна представляет собой одноранговую систему, не имеющую какого-либо центрального органа, управляющего потоком данных. Один из ключевых способов устранения централизованного контроля, обеспечивающих при этом сохранение целостности данных, состоит в организации большой распределенной сети из независимых пользователей. Это означает, что компьютеры, обеспечивающие работу сети, будут находиться более чем в одном физическом местоположении. Такие компьютеры обычно называют *полными узлами*.

На рис. 1.1 представлена визуализация структуры блокчейн-цепи в сети Биткойна. Вы можете увидеть ее в реальном режиме времени на сайте <http://dailyblockchain.github.io>.

Для предохранения сети от разрушения, помимо децентрализации структуры ее блокчейн-цепи, очень часто используется криптовалюта. *Криптовалюта* — это цифровой токен, который имеет рыночную стоимость. С криптовалютами осуществляются биржевые операции, аналогичные операциям с акциями.

Криптовалюты каждого из блокчейнов функционируют по собственным правилам, которые могут заметно различаться между собой. Как правило, программное обеспечение предусматривает оплату работы компьютерного оборудования. Здесь под программным обеспечением понимается протокол блокчейн-цепи. Самыми известными блокчейн-протоколами являются Биткойн (*Bitcoin*), Эфириум (*Ethereum*), Ripple (*Ripple*), Hyperledger (*Гиперледжер*) и Factom (*Фактом*). Компьютерное оборудование включает полные узлы, которые обеспечивают защиту данных в сети.

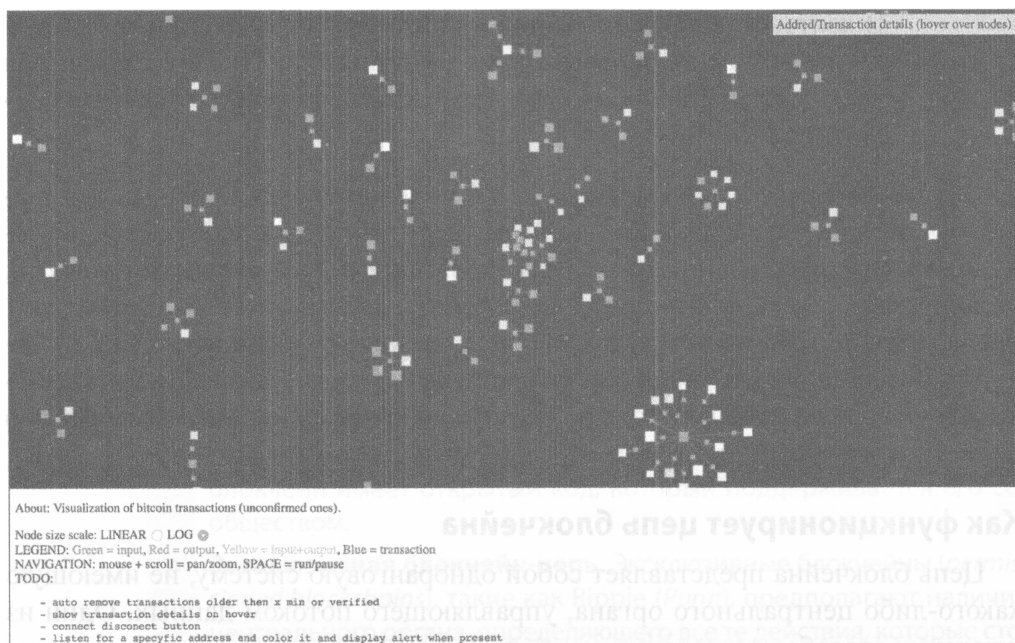


Рис. 1.1. Динамическая структура блокчейн-цепи сети Биткойна

Почему блокчейн-технология так важна

Сейчас блокчейн-технология признана как “пятая волна” в компьютерной революции, принеся в мир тот самый недостающий уровень доверия к Интернету. Это одна из причин, по которым такое множество людей сейчас заинтересовались данной темой.

Блокчейн-технология позволяет создать необходимый уровень доверия на основе цифровых данных. Как только информация будет записана в базу данных блокчейна, станет практически невозможно удалить ее оттуда или изменить. Такой возможности никогда ранее не существовало.

Когда данные в цифровой форме обретают надежные качества постоянства и достоверности, в интерактивном режиме можно заключать деловые сделки в таком формате, который ранее был доступен только вне сети. Все, что ранее представлялось в аналоговом виде, включая права собственности и подтверждение подлинности, теперь может создаваться и обслуживаться интерактивно. Медленные банковские и бизнес-процессы, такие как банковские переводы или фондовые выплаты, теперь могут быть выполнены почти мгновенно. Для мировой экономики последствия внедрения защищенных цифровых расчетов будут огромны.

Первые созданные приложения были предназначены для защищенной передачи цифровых ценностей, которые в блокчейн-технологии осуществлялись

посредством манипуляции их собственными токенами. В частности, эти манипуляции включали такие операции, как перевод денег и активов. Но возможности блокчейн-сетей выходят далеко за пределы задачи перемещения ценностей.

Структура блокчейн-цепи

Цепь блокчейна состоит из трех основных частей.

- » **Блок.** Блок содержит перечень транзакций, занесенных в реестр за некоторый период. Размер блока, период накопления транзакций и иницилирующее запись блока событие различаются в каждой конкретной реализации блокчейна.

Не во всех блокчейн-проектах основной целью являются запись и хранение информации о перемещениях их собственной криптовалюты. Однако во всех без исключения блокчейн-проектах записываются перемещения их криптовалюты или токена. *Транзакцию* можно понимать просто как запись некоторых данных. Назначение им ценности (как это имеет место в финансовых транзакциях) используется лишь для интерпретации того, что эти данные означают.

- » **Цепочка.** *Хеш* — число, полученное как результат математической операции хеширования — связывает один блок данных с другим, математически объединяя их в единую цепь. Это одна из самых сложных для понимания концепций блокчейн-технологии. В действительности это та самая “магия”, которая склеивает элементы блокчейна в единое целое, обеспечивая тем самым математический гарантированный уровень доверия.

В технологии блокчейна хеш очередного блока создается с использованием данных предыдущего блока. Такой хеш является как бы “отпечатком пальца” этих данных, позволяя объединить последовательность блоков в единую цепь в порядке их создания во времени.

Хотя сама блокчейн-технология является относительно новым явлением, о хешировании этого не скажешь. Метод хеширования был предложен более 30 лет назад. Он получил широкое признание, поскольку позволял получать одностороннее преобразование, которое было невозможно расшифровать. Функция хеширования представляет собой математический алгоритм, позволяющий отобразить данные любого размера в виде битовой строки заданной длины. Такая строка обычно имеет длину 32 символа и однозначно представляет данные, которые подверглись хешированию. В блокчейн-технологии в качестве криптографической хеш-функции обычно



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

используется алгоритм SHA (*Secure Hash Algorithm*). Как правило, это SHA-256 — стандартный алгоритм, позволяющий генерировать фактически уникальные хеши фиксированной длины в 256 бит (это и есть 32 символа). Для практических целей удобнее всего представлять себе хеш как цифровой отпечаток пальца данных в блоке, который используется для его закрепления на соответствующем месте в цепи блокчейна.

- » **Сеть.** Сеть блокчейна состоит из “полных узлов”. Их можно представлять себе как компьютеры, на которых выполняются программы, алгоритм которых обеспечивает защиту всей системы. На каждом узле хранится *полная копия* всех транзакций, которые когда-либо были записаны в блокчейн-цепь.

Эти узлы расположены в разных местах по всему миру и могут контролироваться кем угодно. Следует отметить, что поддержка полного узла — дело сложное, дорогое и требующее немалых затрат времени, поэтому люди не будут делать это бесплатно. Главным стимулом, который поддерживает в них желание обеспечивать работу полного узла блокчейн-сети, является возможность заработать криптовалюту. Предоставление вознаграждения за их труд всегда заложено непосредственно в сам алгоритм блокчейна. Вознаграждением обычно являются токены или криптовалюта, например биткойн.



СОВЕТ

Термины *биткойн* и *блокчейн* часто понимаются как взаимозаменяемые, но на самом деле это вовсе не одно и то же. Система Биткойн имеет собственный блокчейн, который здесь является сетевым протоколом, обеспечивающим выполнение защищенных транзакций биткойн-платежей. Термин *биткойн* — это название криптовалюты, существование которой обеспечивается сетью системы Биткойна. Блокчейн — это класс программного обеспечения, тогда как биткойн — это название конкретной криптовалюты.

Блокчейн-приложения

Все блокчейн-приложения строятся вокруг главной идеи, утверждающей, что компьютерная сеть может выступать в качестве арбитра. Системы такого типа представляют собой беспощадную, неумолимую и слепую среду. Компьютерная программа становится законом, и его правила выполняются в точности так, как они были прописаны и истолкованы в сети. У компьютеров нет никаких социальных предубеждений и особенностей поведения, как это свойственно людям.

Компьютерная сеть не может интерпретировать намерения (по крайней мере, пока). Поэтому в качестве одного из потенциальных вариантов применения новой технологии в свое время было проведено детальное изучение возможности заключения в блокчейн-системе страховых контрактов.

Другим интересным примером, где могут использоваться преимущества блокчейн-технологии, является реализация безупречного учета. Такие реестры позволяют создать во времени ясную и неизменную картину того, кто, что и когда сделал. Многие организации и контролирующие органы тратили бесчисленные часы в попытках решить эту проблему. Запись и хранение информации в блокчейн-реестре может существенно облегчить нам задачу правильной интерпретации прошлого.

Этапы развития блокчейн-технологии

Блокчейн-цепь была создана в процессе реализации проекта Биткойн. Опыт ее эксплуатации убедительно показал, что группа независимых личностей, никогда не встречавшихся друг с другом, способны в онлайн-режиме успешно работать в системе, которая нечувствительна к попыткам махинаций со стороны других лиц, присутствующих в той же сети.

Изначально сеть биткойна создавалась для поддержки и защиты этой криптовалюты. Сейчас в ней более пяти тысяч полных узлов, разбросанных по всему миру. Прежде всего эта сеть используется для торговли за биткойны и их обмена на другие валюты, но ее сообщество видит большой потенциал и для реализации иных применений. Благодаря своему размеру и проверенной временем защите сейчас она используется и для организации защиты других, меньших по размеру блокчейн-цепей и связанных с ними приложений.

Сеть Эфириум (*Ethereum*) стала второй важной ступенью в развитии концепции блокчейна. В ней сохранена традиционная структура блокчейн-цепи, но добавлен собственный язык программирования, встроенный непосредственно в систему. Как и в сети Биткойна, в этой сети более пяти тысяч полных узлов, разбросанных по всему миру. Сеть Эфириум в основном используется для торговли эфиром (ее криптовалютой), заключения смарт-контрактов и поддержки децентрализованных автономных организаций (DAO — Decentralized Autonomous Organization). Она также использовалась для защиты блокчейн-приложений и блокчейнов меньшего размера.

Третьим этапом эволюции блокчейн-технологии можно считать сеть Factom. В ней используется упрощенная система консенсуса с поддержкой голосования и обеспечивается хранение гораздо большего количества информации. В первую очередь, она была создана для защиты данных и систем. Factom

взаимодействует с сайтами федеральных служб США и бесчисленных аудиторских компаний. Эта сеть невелика, поэтому закрепилась в других распределенных сетях, построив мосты через несущие блокчейн-цепи.

Консенсус: правящая сила блокчейна

Технология блокчейна — это мощный инструмент, поскольку она позволяет создавать честные системы, обеспечивающие самокоррекцию без необходимости подключения третьих сил с целью контроля за соблюдением правил. Соблюдение установленных правил в блокчейн-технологии реализуется за счет использования алгоритма консенсуса.

В мире блокчейна термин *консенсус* определяет процесс достижения соглашения среди группы исходно не доверяющих друг другу участников системы. В данном случае ими являются полные узлы, функционирующие в сети. Полные узлы проверяют транзакции, которые были созданы в сети и должны быть записаны в реестр.

На рис. 1.2 представлено, как в технологии блокчейна достигается консенсус.

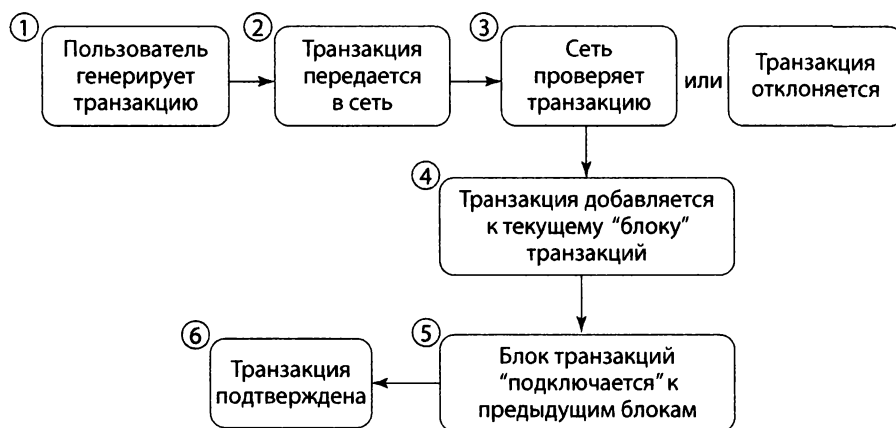


Рис. 1.2. Как работает блокчейн

В каждой конкретной реализации блокчейн-технологии используется собственный алгоритм достижения соглашения в сети при добавлении новой транзакции. Существует множество различных моделей достижения консенсуса, поскольку в каждой реализации блокчейна используются различные типы входных записей. В одних цепях блокчейна хранятся валютные активы, в других — некоторые данные, а третьи представляют собой защитные системы для контрактов.

В системе биткойна, например, между членами сети осуществляется торговля на основе ее токена. Этот токен имеет определенную рыночную стоимость,

поэтому требования в отношении производительности, масштабирования, целостности, методов защиты от внешних угроз и отказов оборудования должны быть очень высокими. Работа системы биткойна построена в предположении, что злоумышленник может предпринять попытку нарушить историю записей о транзакциях с целью похищения токенов. В биткойне эта опасность предотвращается за счет использования модели консенсуса, называемой “доказательство выполнения работы” (*proof-of-work*). Такой подход позволяет успешно решить задачу византийских генералов: “Как можно узнать, что поступившая информация не была искажена изнутри или извне?” Поскольку изменение данных или манипуляция ими возможна практически всегда, обеспечение надежности данных — это большая проблема в компьютерных науках.

Большинство блокчейн-систем функционируют в предположении, что они будут атакованы — со стороны или изнутри, самими пользователями системы. Ожидаемые угрозы и степень доверия, которую сеть предъявляет к узлам, контролирующим запись в блокчейн, определяют тип консенсусного алгоритма, который используется в этой сети для обоснования достоверности записей ее реестра. Например, в сетях Биткойн и Эфириум предполагается очень высокая степень угрозы, и по этой причине используется очень жесткий алгоритм консенсуса, называемый *proof-of-work*. В такой сети доверие априори к кому-либо полностью отсутствует.

На другой стороне спектра находятся блокчейн-сети, созданные для записи финансовых транзакций между известными сторонами, в которых могут использоваться более простые и быстрые варианты консенсуса. В данном случае потребность в высокой скорости выполнения транзакций для них важнее. Алгоритм *proof-of-work* оказывается слишком медленным и дорогостоящим, поскольку в сети сравнительно небольшое число участников, которые нуждаются в немедленном завершении каждой транзакции.

Блокчейн-технология в действии

На сегодняшний день существуют сотни блокчейн-реестров и блокчейн-приложений. Весь мир одержим идеями более быстрого перемещения денег, интеграции и управления в распределенной сети, а также создания защищенных приложений и оборудования.

Работу многих открытых блокчейн-систем можно наблюдать, просто зайдя на сайт криптовалютной биржи. Так, на рис. 1.3 показана страница сайта компании Bitfinex (<https://www.bitfinex.com>), представляющей собой платформу для торговли криптовалютами-альткойнами.



Рис. 1.3. Сайт биржи, работающей с электронными валютами

Однако блокчейн-технология уже вышла за пределы рынка торговой стоимости и нашла применение во многих иных областях человеческой деятельности. Причина в том, что технология блокчейна предоставила новый уровень доверия, что позволило сделать работу в онлайн-режиме безопасной в такой степени, которая прежде была просто недостижима.

Существующие применения блокчейн-технологии

Большинство функционирующих блокчейн-приложений тяготеет к области быстрого и недорогого перемещения денежных средств и других форм ценности. Сюда можно отнести торговлю акциями и ценными бумагами, оплату труда работникам в других странах и обмен одной валюты на другую.

Блокчейн-технология сейчас также используется как часть инструментария, предназначенного для защиты программного обеспечения. Управление национальной безопасности США провело исследование в отношении использования программного обеспечения на основе блокчейн-технологии, предназначенного для защиты устройств в сетях *Internet of Things* (IoT — Интернет вещей¹). Технология IoT получила определенные преимущества от внедрения

¹ Интернет вещей (IoT) — концепция вычислительной сети, объединяющей физические предметы (“вещи”), оснащенные встроенными средствами взаимодействия между собой или с внешней средой. — *Примеч. пер.*

этой инновации, поскольку по своей сути она изначально была особенно уязвима для спуфинга и других форм взлома сетей. Также в результате сами IoT-устройства получили большее распространение, а защита сети уже в большей степени опирается на них самих. Хорошими примерами здесь могут быть клинические системы, самоуправляемые автомобили и системы безопасности.

Проект DAO (*Decentralized Autonomous Organization* — децентрализованная автономная организация) является еще одной интересной блокчейн-инновацией. Этот тип блокчейн-проекта представляет собой новое средство организации работы и объединения усилий множества различных компаний в интерактивном режиме. В частности, проект DAO используется для объединения единомышленников с целью инвестирования фондов в совместные проекты в среде сети Эфириум.

Будущее блокчейн-приложений

В настоящее время разрабатываются более масштабные и в потенциале более долгоживущие блокчейн-проекты, в число которых входят поддерживаемые государством системы регистрации земель, а также приложения для идентификации личности и обеспечения безопасности международных поездок.

Возможности, которые в будущем станут доступными благодаря внедрению блокчейн-технологии, будоражат воображение деловых людей, правительств, политических групп и гуманитарных организаций по всему миру. Такие страны, как Великобритания, Сингапур и ОАЭ, рассматривают эту технологию как средство для снижения затрат, создания новых финансовых инструментов и надежного хранения различных сведений. В этих странах были сделаны значительные инвестиции и развернуты исследования в области блокчейн-технологий.

Блокчейн-технология заложила основу для того, чтобы проблему необходимого доверия можно было, наконец, исключить из рассмотрения. Там, где раньше требовалось немало усилий, чтобы добиться доверия, с появлением блокчейна все стало легко и просто. Кроме того, инфраструктура, необходимая для проведения в жизнь правил, если это доверие было нарушено, теперь может быть существенно упрощена. Множество аспектов жизни общества построено на доверии и соблюдении установленных правил. Социальные и экономические последствия распространения блокчейн-приложений могут быть эмоционально и политически противоположными, поскольку блокчейн-технология изменит и то, как мы будем классифицировать и структурировать ценностные и социально-ориентированные взаимодействия.



Глава 2

Выбираем тип блокчейна

В ЭТОЙ ГЛАВЕ...

- » Выбираем блокчейн для своих целей
- » Составляем план проекта
- » Уточняем детали проекта
- » Рисуем схему выполнения проекта

Индустрия блокчейна сложна, и ее размеры и возможности возрастают с каждым днем. Только узнав особенности трех основных типов блокчейн-сетей и уяснив свойственные им ограничения, вы действительно поймете, каковы возможности этой новой технологии.

В этой главе есть все необходимое, чтобы оценить значение блокчейн-технологии и разработать план собственного соответствующего проекта. В следующей главе речь пойдет об индивидуальных блокчейн-платформах и приложениях в их контексте.

Здесь же будет рассказано, как оценить возможности трех разных типов блокчейн-платформ и что обычно строится на платформах каждого типа и почему. Также вам будет предложено несколько инструментов, которые помогут разработать схему собственного проекта, спрогнозировать возможные препятствия и преодолеть возникшие проблемы.

Где блокчейн может быть полезен

В последние годы отмечается большая шумиха вокруг технологии блокчейна и криптовалют, которые функционируют на ее основе. Часть этой шумихи происходит просто по причине колебаний рыночной стоимости криптовалют и страха, что блокчейн-технология разрушит многие хозяйственные и государственные институты. Как бы там ни было, огромные суммы денег были затрачены на исследования и новые разработки, поскольку держатели токенов не хотят отстать от времени, а предприниматели стремятся исследовать новые бизнес-модели.

Когда заходит речь о поиске благоприятных возможностей для внедрения блокчейн-технологии с целью повысить ценность организации, часто возникает вопрос “Где именно технология блокчейна может оказаться полезной и чем она отличается от уже существующих технологий?”

Блокчейн-цепи представляют собой особый тип баз данных, поэтому их можно использовать во всех случаях, в которых могут использоваться любые иные виды баз данных. Однако может оказаться и так, что нет никакого смысла заново преодолевать трудности и нести дополнительные затраты там, где обычная база данных и так прекрасно справляется с поставленной задачей.

Но если вам приходится делиться важной информацией с другими сторонами, которым вы не вполне доверяете, либо если ваши данные нуждаются в аудите, либо существует риск, что данные будут нарушены или подменены изнутри либо извне, вы действительно сможете оценить все преимущества использования блокчейна определенного типа. К сожалению, ни на один из поставленных выше вопросов нельзя дать простых ответов, и принять правильное решение может оказаться непросто.

Этот раздел поможет вам уменьшить количество возможных вариантов.

Определяем свои потребности

Блокчейн может быть построен в большом числе вариантов. Среди них вы непременно найдете такой, который будет в точности соответствовать вашим потребностям. Вопрос лишь в том, как его отыскать! При выборе наиболее подходящего варианта прямое сопоставление ваших потребностей с характеристиками различных блокчейнов может оказаться заданием почти невыполнимым. Что касается меня, то всякий раз, когда приходится иметь дело со множеством доступных вариантов и часто конфликтующими между собой потребностями, я предпочитаю пользоваться матрицей взвешенных решений.

Матрица взвешенных решений — это прекрасный инструмент для оценки критериев проекта с последующим их сопоставлением с возможными решениями. Главное достоинство матрицы состоит в том, что она помогает выявить все возможные критерии проекта и присвоить им приоритеты, что существенно упрощает принятие решения. Матрица взвешенных решений также поможет не потеряться в путанице отдельных критериев. При правильном употреблении этот инструмент позволяет прийти к единственному решению, которое будет учитывать все поставленные цели.

Для создания матрицы взвешенных решений выполните следующие действия.

1. Организуйте мозговой штурм для поиска ключевых критериев или целей, которых ваша команда должна будет достичь.



СОВЕТ

Если вы не вполне уверены в том, какие критерии следует принимать во внимание при оценке блокчейн-проекта, примите к сведению несколько показателей, о которых в любом случае не следует забывать:

- масштаб и объем;
- скорость работы и время ожидания;
- защищенность и неизменность;
- объем информации в транзакции и потребность ее структурирования.

Каждый член вашей команды должен составить собственный список целей и приоритетов. Вам потребуется учитывать лишь некоторые из них при выборе подходящей платформы, отвечающей всем вашим нуждам.

2. Сократите список критериев до десяти позиций максимум.



СОВЕТ

Если вы испытываете затруднения в очистке списка критериев от излишних позиций, попробуйте построить из них матрицу сравнения.

3. Создайте новую таблицу в Microsoft Excel или любой другой аналогичной программе.

4. В первый столбец таблицы введите отобранные вами критерии.

5. Каждому критерию присвойте относительный вес, исходя из того, насколько важно, чтобы эта цель была достигнута при реализации проекта.

Каждому оставшемуся критерию, общим числом не более 10, присвойте определенный вес по простой шкале, например 1 — малая важность, 2 — средняя важность, 3 — высокая важность и т.д.

Если вы работаете в команде, пусть каждый ее член присвоит критериям весовые коэффициенты независимо от других ее членов.



СОВЕТ

6. Просуммируйте числовые значения коэффициентов для каждого критерия и разделите эту сумму на количество членов в команде.

В результате вы получите усредненное значение, соответствующее мнению всей команды в целом.

7. Проанализируйте полученные результаты и при необходимости внесите корректировки, чтобы в конечном счете каждый критерий был оценен правильно.

Поздравляю! Теперь у вас есть ранжированный список всех критериев, которые должны быть удовлетворены после реализации вашего блокчейн-проекта.

Формулируем цели

Вы не сможете довести свой блокчейн-проект до успешного завершения, если не будете четко понимать его назначение или конечную цель. Не пожалейте времени на то, чтобы детально разобраться, чего вы и ваша команда хотите достичь и в чем состоит конечная цель. Например, целью может быть продажа активов компании-партнеру без посредников. Это будет важная цель для многих держателей токенов.

Начните с небольшого проекта, представляющего собой минимально возможный жизнеспособный вариант использования новой технологии, но при этом очевидным образом демонстрирующий получаемые дополнительные ценности или экономию для вашей компании. Если вернуться к приведенному выше примеру, наименьшей целью в нем может быть создание частной сети, в которой будет осуществляться обмен ценностями между доверенными сторонами.

Далее приступайте к расширению уже достигнутого. Очередным этапом может быть создание некоторого инструментария, предназначенного для осуществления торговых сделок на вашей новой платформе. Каждый этап должен приносить вам определенные преимущества и рост ценности.

Выбираем решение

Существует три основных типа блокчейнов: публичные сети, подобные Биткойну; эксклюзивные сети, такие как Ripple, и частные сети, например финансовая платформа для глобальной торговли Nijro.

Каждый блокчейн-проект позволяет достичь следующих очевидных результатов.

- » Быстрое перемещение ценностей или выполнение торговых операций с очень небольшими издержками.
- » Создание практически неизменяемых архивов данных, упорядоченных по времени их поступления.

Блокчейн-технология позволяет реализовать и несколько менее очевидных решений, таких, например, как возможность доказать, что у вас есть “вещь”, без необходимости явно продемонстрировать ее другой стороне. Возможно также “доказать отрицание” или доказать, что нечто отсутствует в наборе данных или в системе. Эта возможность будет особенно полезной при аудите и для доказательства соответствия.

В табл. 2.1 перечислены основные задачи, которые могут быть решены за счет применения блокчейн-технологии.

Таблица 2.1. Задачи, решение которых обеспечивает блокчейн-технология

Основная цель	Тип блокчейна
Перемещение ценностей между сторонами, не являющимися доверенными	Публичный
Перемещение ценностей между доверенными сторонами	Частный
Торговля за валюту разного вида	Эксклюзивный
Торговля за валюту одного вида	Публичный
Создание децентрализованных организаций	Публичный или эксклюзивный
Создание децентрализованных контрактов	Публичный или эксклюзивный
Торговля секьюритизированными активами	Публичный или эксклюзивный
Обеспечение идентификации для людей или вещей	Публичный
Запись информации для открытого учета	Публичный
Запись информации для закрытого учета	Публичный или эксклюзивный
Обеспечение аудита записей или систем	Публичный или эксклюзивный
Запись информации о правах собственности на землю	Публичный
Торговля цифровыми валютами или активами	Публичный или эксклюзивный
Обеспечение защиты систем типа Internet of Things (IoT)	Публичный
Организация защиты систем	Публичный

Ниже приведены общая характеристика различных типов блокчейн-сетей и их сильные и слабые стороны, хотя в зависимости от проекта здесь возможны те или иные исключения. Кроме того, для достижения поставленных целей можно использовать различные типы блокчейнов.

- » **Публичные сети** обычно очень большие и децентрализованные. Любой может принять участие в их работе и на любом уровне — поддерживать работу полного узла, майнить криптовалюту, торговать токенами или записывать новые данные. Эти сети обычно лучше обеспечивают свою защиту и неизменяемость, чем частные или эксклюзивные сети. Однако работают они, как правило, медленнее и их эксплуатация обходится дороже. Они манипулируют защищенной криптовалютой и имеют строгие ограничения на размер сохраняемых в записи данных.
- » **Эксклюзивные сети** открыты для широкой публики, но участие в их работе контролируется. Многие из них используют криптовалюту, но при этом за приложения, работающие с сетью, может взиматься небольшая плата. Этот подход упрощает масштабирование проекта и повышение объема транзакций. Эксклюзивные сети могут работать очень быстро при малом времени подтверждения транзакций и обычно допускают больший объем сохраняемых в записи данных в сравнении с публичными сетями.
- » **Частные сети** совместно используются доверенными сторонами и могут быть полностью невидимыми для широкой публики. Они, как правило, чрезвычайно быстрые при полном отсутствии времени ожидания. Кроме того, стоимость их эксплуатации обычно невелика, а развернуть их можно за один уик-энд. Большинство частных сетей не использует криптовалют и не обеспечивает той неизменяемости и защищенности, которые характерны для децентрализованных сетей. Объем сохраняемых в записи данных может быть неограниченным.

Также могут существовать гибридные варианты между тремя основными типами блокчейн-сетей. Цель такого подхода — найти необходимый баланс между защищенностью, контролируемостью, возможностями масштабирования и сохранения данных в записях для приложений, функционирующих поверх этих сетей.

Строим дерево решений блокчейна

Некоторые из решений, которые вам потребуется принимать в процессе работы над блокчейн-проектом в своей организации, могут оказаться достаточно сложными. Принимая важные решения, следует внимательно отнестись к следующим обстоятельствам.

- » **Неопределенность.** Многие факты в отношении блокчейн-технологии могут быть вам неизвестны или оказаться непроверенными.
- » **Сложность.** Блокчейн-технологии присуще множество взаимосвязанных факторов, которые следует учитывать.
- » **Высокий уровень риска.** Влияние принятого решения на организацию может оказаться весьма значительным.
- » **Наличие альтернатив.** Могут существовать альтернативные технологии или типы блокчейнов со своими наборами неопределенностей и следствий.
- » **Межличностные проблемы.** Необходимо понимать, как внедрение блокчейн-технологии может повлиять на различных людей в организации.

Дерево решений — это полезный вспомогательный инструмент, который помогает выявлять последствия, контролировать результаты, определять стоимость ресурсов и оценить в целом полезность реализации блокчейн-проекта.

Вы можете нарисовать дерево решений на бумаге или воспользоваться подходящим компьютерным приложением. Вот что следует выполнить, чтобы выявить прочие возможные проблемы в отношении своего проекта.

1. Возьмите большой лист бумаги.



СОВЕТ

Чем больше вариантов и чем сложнее решение, которое следует принять, тем больший лист бумаги вам потребуется.

2. Нарисуйте квадрат на листе бумаги слева.

3. В этом квадрате опишите основную цель и укажите все критерии, которым должен удовлетворять ваш проект.

4. Справа от квадрата нарисуйте линию для каждой выявленной проблемы или вопроса.

5. Вдоль каждой линии добавьте описание соответствующей проблемы.



СОВЕТ

В описании укажите вероятность возникновения проблемы.

6. Организуйте мозговой штурм в поисках решения каждой выявленной проблемы.

7. Запишите каждое из предложенных решений данной проблемы вдоль ее линии.

8. Продолжайте этот процесс до тех пор, пока не будет проанализирована каждая выявленная проблема и не будет найдено ее возможное решение.

Прежде чем завершить эту работу, попросите членов вашей команды проанализировать и прокомментировать все сделанные вами записи о проблемах и возможных способах их решения.

Составляем план

К этому моменту у вас должно сложиться четкое понимание поставленных целей, имеющихся препятствий и того, из каких вариантов блокчейна вы можете выбирать.

Вот простой план действий, который позволит вам успешно создать свой проект.

- 1. Расскажите о своем проекте главным заинтересованным лицам и держателям токенов и обсудите с ними его основные элементы и предполагаемые результаты.**
- 2. Составьте и запишите план проекта.**
- 3. Разработайте показатели производительности, опишите область применения, составьте график работ и примерный бюджет проекта.**
- 4. Подумайте о создании плана управления рисками и плана укомплектования персоналом.**
- 5. Сделайте необходимые закупки и определите роли и обязанности участников.**
- 6. Проведите стартовое собрание, чтобы запустить проект.**

На этом собрании обязательно должны быть освещены следующие вопросы:

- ваше видение значения и особенностей данного проекта;
- стратегия выполнения проекта;
- график выполнения работ;
- роли и обязанности исполнителей;
- обязательства, возлагаемые на команду;
- мероприятия по сплочению команды;
- как в команде будут приниматься решения;
- ключевые показатели, по которым будет контролироваться ход выполнения проекта.



ЗАПОМНИ

Когда проект будет завершен, ваша работа еще не закончится! Вернитесь к началу и проанализируйте достигнутые успехи и то, что вам осуществить не удалось. Вот несколько вопросов, на которые нужно дать ответы.

- » Довольны ли результатами главные держатели токенов?
- » Соблюдался ли намеченный график работ?
- » Если график не соблюдался, то что служило причиной задержки?
- » Чему я научился благодаря этому проекту?
- » Что сейчас я хотел бы сделать по-другому?
- » Удалось ли мне действительно создать для компании новую ценность или добиться экономии?



СОВЕТ

Возможно, вам захочется вновь обратиться к этой главе, когда ваши знания о блокчейн-технологии станут глубже и придет время начать разработку плана собственного проекта.



Глава 3

Пробуем блокчейн в работе

В ЭТОЙ ГЛАВЕ...

- » Создание и использование биткойн-кошелька
- » Создание простого смарт-контракта
- » Разворачиваем частный блокчейн

Блокчейн-технология — очень мощный инструмент, и предполагается, что она способна изменить то, как в мире перемещаются денежные средства, осуществляется защита систем и создаются цифровые идентифицирующие документы. Если вы не программист-разработчик уровня создания ядер операционных систем, вам, вероятно, в ближайшем будущем не удастся внести какой-либо существенный вклад в программную реализацию блокчейн-технологии. Тем не менее вам все равно необходимо понимать, как эта технология работает и какие у блокчейна принципиальные ограничения, поскольку эта технология очень скоро будет интегрирована во множество повседневных интерактивных взаимодействий (начиная с того, как наниматели будут платить исполнителям, и заканчивая тем, как правительственные организации будут обеспечивать целостность и защищенность своих компьютерных систем и данных).

В этой главе вы сделаете свои первые шаги в мире блокчейна. Вы ознакомитесь со многими наиболее важными аспектами работы с криптовалютой и блокчейн-сетями, но при этом будете пользоваться инструментами, которые позволят вам оставаться на комфортной дистанции от интригующе сложной и даже пугающей работы внутренних механизмов блокчейн-сетей и соответствующих приложений. В этой главе вам также будет рассказано, как открыть собственный счет в криптовалюте, который потребуется вам для изучения последующих глав книги.

Начнем с блокчейна биткойна

Биткойн — одна из крупнейших и наиболее мощная блокчейн-сеть в мире. Изначально она была создана для поддержки криптовалюты с тем же названием — биткойн. Поэтому вполне естественно, что для создания в блокчейне Биткойна новой записи необходимо отправить какое-то количество биткойнов с одного счета на другой.

Когда вы пересылаете биткойны с одного счета на другой, сведения об этой транзакции записываются в блокчейн Биткойна. После того как транзакция внесена в блокчейн, эту информацию уже невозможно оттуда удалить — сведения о вашей операции будут храниться в блокчейне Биткойна столько, сколько он будет существовать. Эта концепция неизменности является чрезвычайно мощной — это наиболее важное качество любой блокчейн-цепи.

Существует несколько способов добавить в запись транзакции немного дополнительной информации, но в некоторых случаях эти методы необязательно позволяют получить легко читаемое сообщение. В этом разделе будет рассказано, как можно встроить сообщение непосредственно в биткойн-транзакцию.

Внедрение данных в биткойн-адрес гарантирует, что они будут легко читаемыми. Это можно сделать, используя “красивый” биткойн-адрес. Красивый биткойн-адрес можно представлять себе как красивый номерной знак на автомобиле. Шестибуквенный красивый биткойн-адрес можно получить бесплатно, тогда как за более длинные вам придется заплатить. Чем длиннее красивый адрес, тем дороже он стоит.

В этом разделе вам предстоит создать два биткойн-кошелька и поместить в один из них некоторое количество денег, получить для себя красивый биткойн-адрес и перевести небольшую сумму в биткойнах из одного своего кошелька в другой.



СОВЕТ

Если у вас уже есть биткойн-кошелек с некоторой суммой в нем, можете пропустить следующий подраздел, а при чтении остальной части этого раздела просто им воспользоваться.

Создаем первый биткойн-кошелек

Адрес биткойн-кошелька состоит из 32 символов, образующих уникальную комбинацию. С его помощью вы сможете отправлять и получать биткойны¹. С этим кошельком связан закрытый (*private*) ключ, представляющий собой секретный код, знание которого позволяет доказать, что именно вы являетесь владельцем тех биткойнов, которые хранятся в кошельке с данным адресом.



ВНИМАНИЕ!

Любой, кто узнает закрытый ключ вашего кошелька, сможет потратить хранящиеся в нем биткойны, поэтому всегда держите его в секрете.

Ваш первый биткойн-кошелек должен быть связан с кредитной картой или банковским счетом. Я рекомендую воспользоваться одним из следующих типов биткойн-кошельков.

» **Coinbase** (<https://www.coinbase.com>)

» **Харо** (<https://www.circle.com>)

Для получения первого кошелька, просто перейдите на один из указанных выше сайтов и создайте счет. Это потребует всего нескольких минут. Когда счет будет открыт, положите на него небольшую сумму денег, чтобы можно было продолжить эксперименты. (Полагаю, что пяти долларов для этого будет вполне достаточно.)

Создаем второй биткойн-кошелек

Чтобы получить биткойны, которые вы в скором времени отправите, необходимо иметь второй биткойн-кошелек. Для создания второго кошелька не заходите на сайты компании Circle или Coinbase, поскольку кошельки этих типов не предоставляют тех функциональных возможностей, которые нам вскоре потребуются.

Самым простым биткойн-кошельком, который позволяет выполнить все то, что мы собираемся сделать, является кошелек от компании Blockchain.info. Для его создания выполните следующее.

1. **Зайдите на сайт Blockchain.info** (<http://www.blockchain.info>).
2. **На главной странице сайта перейдите на вкладку Wallet.**

¹ Подробнее о биткойне и биткойн-кошельках, их закрытых и открытых ключах, а также о многом другом имеющем отношение к биткойну, читайте в книге “Биткойн для чайников” издательства “Диалектика”.

3. На открывшейся странице щелкните на кнопке **Get a Free Wallet** (вверху справа).
4. В выведенной на экран форме укажите адрес своей электронной почты, задайте пароль, установите флажок (внизу) и щелкните на кнопке **Продолжить**. Выполните все прочие необходимые действия, связанные с созданием кошелька, указанные на страницах этого сайта.

Генерируем красивый биткойн-адрес

Красивый биткойн-адрес — это что-то наподобие именного номерного знака на автомобиле. В сущности, это просто биткойн-адрес, в котором есть привлекательная для вас последовательность букв и/или цифр. Иметь красивый адрес совсем необязательно, это просто забавный способ увидеть свои сообщения в системе Биткойн. Есть несколько бесплатных способов создать красивый адрес биткойн-кошелька. Я предпочитаю компанию [BitcoinVanityGen.com](http://www.bitcoinvanitygen.com). Чтобы создать красивый биткойн-адрес с помощью этой компании, выполните следующее.

1. **Зайдите на сайт компании [BitcoinVanityGen.com](http://www.bitcoinvanitygen.com) (<http://www.bitcoinvanitygen.com>).**
2. **На открывшейся странице введите шесть букв (и/или цифр) в поле Type Letters.**

Блокчейн Биткойна позволяет вводить только небольшие сообщения, и ваш красивый адрес, в сущности, и будет составлять то содержание вашего сообщения, которое вы сможете легко прочитать в среде Биткойна.



СОВЕТ

Выберите для себя что-нибудь эдакое, поскольку, как только ваш красивый адрес будет создан, вы сможете многократно использовать его везде, где вам захочется. (Учтите, что красивый адрес из шести знаков² будет бесплатным, а за более длинный придется платить, и чем он будет длиннее, тем больше будет стоить!)

3. **Щелкните на кнопке **Generate**.**
4. **Для доставки вам сгенерированного адреса щелкните на кнопке **Email**.**
5. **Укажите свой адрес электронной почты.**

Компания [BitcoinVanityGen.com](http://www.bitcoinvanitygen.com) отправит вам электронное письмо по указанному адресу, как только ваш красивый адрес будет сгенерирован.

² Шестизначный номер будет бесплатным только в том случае, если на странице заказа флажок *Case sensitive* (С учетом регистра) будет сброшен. Если этот флажок установлен, бесплатными будут адреса из пяти символов, а за шестисимвольный придется платить 0,004 биткойна). — *Примеч. ред.*

6. В полученном от компании BitcoinVanityGen.com письме щелкните на ссылке [click here](#).

На странице сайта компании вам будут предоставлены новый красивый адрес и закрытый ключ к нему.

7. Скопируйте свой новый адрес и его закрытый ключ и поместите эти записи на хранение в безопасное место.

Ваш новый красивый адрес и его закрытый ключ понадобятся вам в следующем подразделе.



ВНИМАНИЕ!

Никогда и никому не передавайте свои закрытые ключи! Храните открытые и закрытые ключи в безопасном месте (лучше раздельно). Открытый ключ вам будет нужен для получения или отправки биткойнов. (Свой открытый ключ вы можете указывать или предоставлять где угодно и сколько угодно раз.) Только *закрытый* ключ является истинным ключом к вашим биткойнам. Если вы утратите этот ключ (случайно или в результате хищения), то потеряете свою связанную с этим ключом криптовалюту *навсегда*.



ЗАПОМНИ!

Мир криптовалют беспощаден и не прощает забывчивости или ошибок. Свою деятельность в нем начинайте с небольших сумм, пока будете изучать, как все это работает, и учиться правильным приемам.

Пересылаем красивый адрес

В этом разделе вы узнаете, как передать свой новый красивый адрес в созданный ранее биткойн-кошелек. Такая передача позволяет управлять своим адресом, а также легко отправлять и получать биткойны. Чтобы подготовить процедуру, выполните следующие действия.

1. Войдите в свой биткойн-кошелек на сайте [Blockchain.info](#).

(Читайте раздел “Создаем второй биткойн-кошелек” выше в этой главе.)

2. На странице сайта перейдите в раздел Настройки⇒Адреса.

На рис. 3.1 показан исходный вид страницы этого раздела.

3. На странице этого раздела щелкните на ссылке Импортировать адреса.

Откроется диалоговое окно Импортировать существующий адрес Bitcoin.

4. Введите в верхнее поле свой красивый адрес и щелкните на кнопке Импортировать.

Для завершения операции щелкните в открывшемся окне предупреждения на кнопке ОК.

Вы только что создали в своем кошельке биткойн-адрес, который позволит каждому, кто будет отправлять или получать у вас биткойны, видеть ваш *красивый* адрес.

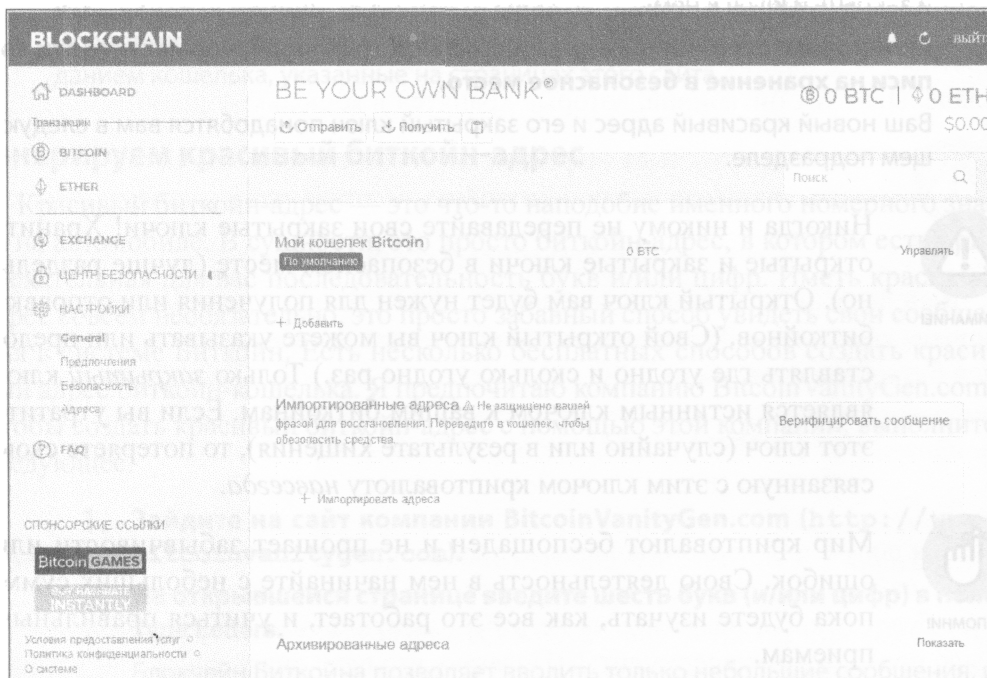


Рис. 3.1. Управление адресами кошелька

Делаем запись в блокчейне биткойна

Теперь, когда у вас есть два биткойн-кошелька, у вас появилась возможность ввести информацию в блокчейн Биткойна. Вы можете сделать это, переслав некоторую сумму биткойнов с одного кошелька на другой. Вот как это выполняется. (Детали приведенной ниже последовательности действий могут различаться в зависимости от типа используемого вами кошелька, но в целом общая идея остается неизменной.)

1. **Откройте свой биткойн-кошелек — тот, в который ранее было положена некоторая сумма денег.**

(Читайте раздел “Создаем первый биткойн-кошелек” выше в этой главе.) На открывшейся странице вам будет предложено указать получателя.

2. **Найдите на этой странице свой красивый биткойн-адрес, скопируйте его и вставьте в поле адреса получателя.**
3. **Укажите сумму биткойнов, которую вы хотите перевести, и щелкните на кнопке Отправить.**

Поздравляю! Вы только что отправили в блокчейн-сеть свое первое долговременное, необратимое и неизменяемое сообщение! Можно с уверенностью сказать, что вы навсегда вписали его в историю Биткойна.



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

Как правило, подтверждение биткойн-транзакции поступает примерно через десять минут, однако иногда его можно ожидать несколько часов. Чем больше сумма транзакции, тем дольше придется ждать ее подтверждения. Неподтвержденная транзакция еще не записана в блокчейн окончательно и все еще может быть обращена.

Читаем запись в блокчейне биткойна

В предыдущем разделе было показано, как создать небольшую постоянную запись в блокчейне Биткойна. Данные в блокчейн-цепи Биткойна не зашифрованы, поскольку они требуют подтверждения полными узлами. А это означает, что вам не составит труда найти ту запись, которая была создана вами при чтении предыдущего раздела.



СОВЕТ

Если вы только что совершили транзакцию по перемещению средств между двумя вашими кошельками, подождите минут 10–15, прежде чем выполнять следующие действия.

1. **Зайдите на сайт Blockchain.info (<http://www.blockchain.info>).**
2. **В поле задания критерия поиска (внизу справа) введите свой красивый адрес и щелкните на кнопке Search или нажмите <Enter>.**

Откроется страница с информацией о выполненной вами ранее транзакции.

Вот и все, что требуется сделать, чтобы найти свою транзакцию и прочитать информацию, которую вы встроили в свой красивый адрес.

Смарт-контракты на базе биткойна

Смарт-контракт — это автономная программа, которая может принимать финансовые решения. В мире блокчейна смарт-контракты — тема очень острая, поскольку они одновременно восхитительны и пугающи в отношении тех последствий, которые могут вызвать в функционировании мировой экономики.

Говоря упрощенно, смарт-контракт представляет собой обычный письменный договор, который был переведен в программный код, сформулированный в виде последовательности сложных операторов “если то”. Смарт-контракт способен

самостоятельно проверять выполнение договорных условий, которые были указаны при заключении данного контракта, и осуществляется это посредством извлечения проверенных данных из внешних источников. Смарт-контракты могут также самостоятельно выполнять требуемые функции при наступлении даты платежа или указанных событий других типов. Они могут быть построены вокруг множества различных идей и по своей природе вовсе необязательно быть финансовыми. Важно, что смарт-контракты способны выполнять все это, оставаясь надежно защищенными от внешнего вмешательства или контроля.

Блокчейн-технология стала той основой, на которой смогла возникнуть и воплотиться в жизнь идея смарт-контрактов. Их привлекательность вызвана тем, что они предоставляют такой уровень неизменности и защиты от искажений, который ранее обеспечивался только бумагой, чернилами и доверенными органами. Смарт-контракты представляют собой настоящее революционное средство в отношении того, как можно вести дела. Они гарантируют, что соглашение будет выполнено именно так, как оно записано. И для этого не потребуются никаких дополнительных внешних усилий — сама цепь блокчейна выступает здесь в качестве посредника и одновременно приводящего в исполнение органа.

Смарт-контракты представляют собой большой шаг вперед, поскольку, когда машины начинают обеспечивать выполнение контрактов, отменить их становится очень трудно или даже невозможно. Это замечание выводит на передний план важный аспект данных инструментов, который нельзя игнорировать, и по этой причине мое первое правило в отношении смарт-контрактов звучит так: *“Тот, кто контролирует данные, тот контролирует и контракт”*. Все смарт-контракты полагаются на внешние источники данных, чтобы принять верное решение и осуществить платеж соответствующей стороне.



ВНИМАНИЕ!

Хотя смарт-контракты являются новой революционной технологией, они все еще не способны оценивать *намерения* сторон, заключающих контракт. Юридические контракты в нашем обществе возлагают на людей интерпретацию того, что имеют в виду стороны, заключающие контракт. Компьютеры, по крайней мере сейчас, могут понимать только программный код, но никак не намерения сторон.

Создаем первое смарт-обязательство

Смарт-обязательство (*smart bond*) — это тип смарт-контракта, который может самостоятельно обеспечивать хранение и реализацию некоего объекта ценности, отслеживая при этом платежи в различных валютах с учетом данных по их курсам, полученным из соответствующих источников. В настоящее время существует уже множество типов смарт-контрактов и каждый день появляются все новые и новые.

Чтобы создать свое первое смарт-обязательство, выполните следующее.

1. **Зайдите на сайт компании SmartContract (<http://www.smartcontract.com>).**
2. **На открывшейся странице щелкните на кнопке Sign Up (справа сверху).**
Откроется страница Sign Up (Зарегистрироваться).
3. **На этой странице введите в соответствующие поля свой адрес электронной почты и выбранный пароль. Щелкните на кнопке Create an Account.**
После подтверждения введенного пароля компания SmartContract отправит вам по указанному адресу письмо со ссылкой для подтверждения реальности этого почтового адреса.
4. **Откройте полученное от компании SmartContract письмо и щелкните в нем на ссылке для подтверждения своей учетной записи и входа в нее.**
На сайте компании SmartContract вам будет предложено указать имя пользователя и юридическое название организации.
5. **Далее на сайте компании SmartContract откроется страница работы со смарт-контрактами. Щелкните на кнопке Create Contract.**
6. **На странице создания контрактов перейдите на вкладку Smart Bond, как показано на рис. 3.2.**

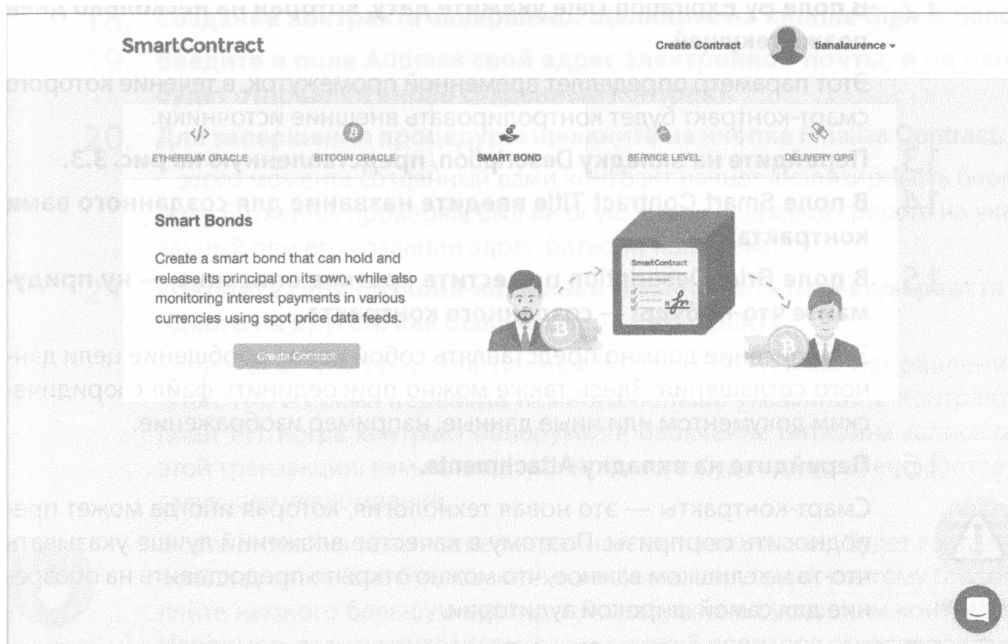


Рис. 3.2. Вкладка Smart Bond на странице сайта SmartContract

7. Щелкните на кнопке Create Contract.

Теперь все готово для ввода первой команды “Если то”.

8. Откройте вкладку Smart Terms.

Смарт-контракты анализируют внешние источники данных, чтобы получить подтверждение о выполнении условий контракта и запустить процедуру осуществления платежа. На этой вкладке вы должны указать те условия, при которых будет запущена процедура выполнения обязательств вашего смарт-контракта.

9. Выберите вариант Performance Monitoring.

Вариант Performance monitoring (Отслеживание выполнения) предполагает отслеживание смарт-контрактом того факта, что некоторое действие во внешней среде было выполнено. В нашем случае это будет перевод средств с одного счета на другой.

10. В поле If Payment To введите один из биткойн-адресов (тех, которые были созданы вами при чтении предыдущих разделов этой главы).

11. В поле Is укажите небольшую сумму (в долларовом эквиваленте), которую вы могли бы перевести с одного своего биткойн-адреса на другой.

12. В поле By Expiration Date укажите дату, которая на несколько дней позже текущей.

Этот параметр определяет временной промежуток, в течение которого смарт-контракт будет контролировать внешние источники.

13. Перейдите на вкладку Description, представленную на рис. 3.3.

14. В поле Smart Contract Title введите название для созданного вами контракта.

15. В поле Brief Description поместите краткое описание — ну придумайте что-нибудь! — созданного контракта.

Это описание должно представлять собой некое обобщение цели данного соглашения. Здесь также можно присоединить файл с юридическим документом или иные данные, например изображение.

16. Перейдите на вкладку Attachments.

Смарт-контракты — это новая технология, которая иногда может преподносить сюрпризы. Поэтому в качестве вложений лучше указывать что-то не слишком важное, что можно открыто предоставить на обозрение для самой широкой аудитории.

17. Щелкните на кнопке Attach Documents.

Вы можете вложить в смарт-контракт либо PDF-файл, либо файл изображения.



ВНИМАНИЕ!

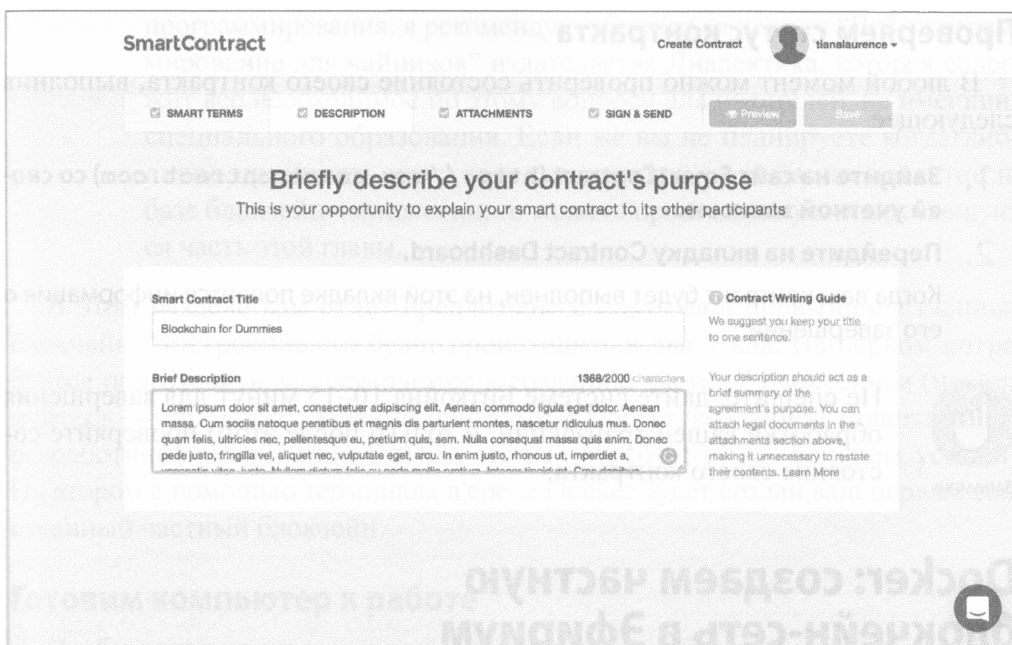


Рис. 3.3. Вкладка *Description* на странице сайта *SmartContract*

18. **Создание контракта завершено. Щелкните на кнопке Sign & Send.**
19. **Введите в поле Address свой адрес электронной почты, и на него будет отправлен вновь созданный контракт.**
20. **Для завершения процедуры щелкните на кнопке Finalize Contract.**
21. **Откройте свои биткойн-кошельки и выполните перевод средств с одного на другой, как было указано в контракте.**

С этого момента созданный вами контракт начнет анализировать блокчейн Биткойна, проверяя, был ли осуществлен перевод средств на указанный при его создании адрес биткойн-кошелька.

Убедитесь, что средства переводятся в требуемом направлении (этап 10), а сумма перевода немного больше указанной в контракте (этап 11). Когда контракт обнаружит в блокчейне Биткойна запись об этой транзакции, вам по электронной почте будет отправлено соответствующее уведомление.

В сети Биткойна за выполнение данной транзакции с вас будет взята небольшая плата (она будет вычтена из суммы перевода), поэтому отправляйте немного большую сумму, чем требуется по условиям контракта. Например, если в контракте указана сумма 5 долларов, то перевод лучше сделать на сумму 5,15 доллара, что позволит исключить возможные несоответствия.



ЗАПОМНИ!

Проверяем статус контракта

В любой момент можно проверить состояние своего контракта, выполнив следующее.

1. **Зайдите на сайт SmartContract (<http://www.smartcontract.com>) со своей учетной записью.**
2. **Перейдите на вкладку Contract Dashboard.**

Когда ваш контракт будет выполнен, на этой вкладке появится информация о его завершении.



ЗАПОМНИ!

Не спешите, дайте системе Биткойна 10–15 минут для завершения обработки вашей транзакции, и только после этого проверяйте состояние своего контракта.

Docker: создаем частную блокчейн-сеть в Эфириум

Частные блокчейны совмещают в себе как все достоинства закрытых частных баз данных, так и уровень защищенности, свойственный блокчейнам. Этот подход становится еще более привлекательным по двум следующим причинам.

- » Частные блокчейны — отличный инструмент для разработчиков, поскольку позволяет им протестировать свои решения без использования криптовалюты. При этом все найденные ими решения будут по-прежнему оставаться конфиденциальными, поскольку данные в блокчейне недоступны для широкой публики.
- » Большие организации могут зарабатывать на защищенности и неизменности данных, обеспечиваемых блокчейн-технологией, поскольку транзакции в частных блокчейнах остаются невидимыми для посторонних, в отличие от полной открытости, которая характерна для традиционных блокчейнов.



СОВЕТ

В этой книге в большинстве случаев предполагается, что вы, ее читатель, впервые сталкиваетесь с блокчейн-технологией и не имеете каких-либо навыков в программировании. Однако материал этого раздела требует определенных знаний о веб-сервисе GitHub, программе Docker и использовании режима терминала на вашем компьютере. Если вам требуется быстро освежить в памяти основы

программирования, я рекомендую обратиться к книге “Веб-программирование для чайников” издательства Диалектика, которая содержит все необходимое по этому вопросу для читателей, не имеющих специального образования. Если же вы не планируете когда-либо лично принимать участие в технической реализации проектов на базе блокчейн-технологии, то можете просто пропустить оставшуюся часть этой главы.

В этом разделе вам будет предложено создать ваш первый собственный блокчейн. Построение его будет происходить в два этапа. На первом потребуется подготовить ваш компьютер к созданию частных блокчейнов (не волнуйтесь — при использовании программы Docker, созданной талантливыми разработчиками компании GitHub, это не потребует от вас больших усилий). На втором с помощью терминала в среде Docker будет создан ваш первый собственный частный блокчейн.

Готовим компьютер к работе

Чтобы подготовиться к осуществлению данного блокчейн-проекта, необходимо загрузить на свой компьютер некоторое программное обеспечение. Начните с пакета Docker Toolbox. Чтобы загрузить ту его версию, которая соответствует вашей операционной системе, зайдите на сайт <http://www.docker.com/toolbox>.

Далее следует загрузить пакет GitHub Desktop, который можно найти по адресу <http://desktop.github.com>. После установки пакета GitHub Desktop создайте свою учетную запись в веб-сервисе GitHub, зайдя на сайт <http://www.github.com> и щелкнув на ссылке Sign Up (вверху справа). Введите имя пользователя, адрес электронной почты и пароль, а затем щелкните на кнопке Create an account.

Теперь необходимо выделить место для хранения данных вашего блокчейна. Создайте на компьютере папку с названием `ethereum`. В дальнейшем она будет использоваться для размещения репозитория (хранилища информации) и других файлов. Для завершения процедуры подготовки выполните следующее.

1. **Откройте приложение GitHub Desktop.**
2. **Войдите в приложение GitHub Desktop на своем компьютере, воспользовавшись учетной записью, созданной ранее на сайте GitHub.**
3. **Откройте браузер и перейдите по ссылке <https://www.github.com/Cargemini-AIE/ethereum-docker>.**

Откроется страница, представленная на рис. 3.4.

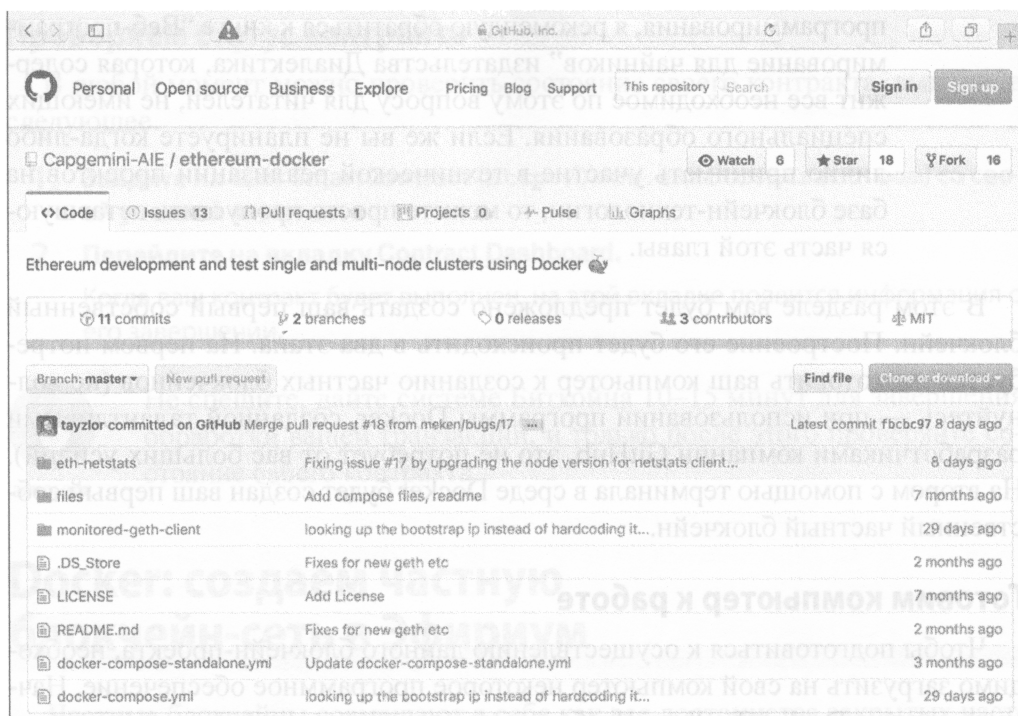


Рис. 3.4. Откройте эту страницу на сайте GitHub

4. На этой странице щелкните на кнопке **Clone or Download** (справа по центру). Вам будет предоставлен выбор: **Open in Desktop** (Открыть на рабочем столе) или **Download Zip** (Загрузить zip-архив), как показано на рис. 3.5.
5. Выберите вариант **Open in Desktop** (Открыть на рабочем столе). Приложение GitHub Desktop будет закрыто и открыто заново.
6. В окне приложения **GitHub Desktop** выберите папку нашего проекта **ethereum** и щелкните на кнопке **Clone**.

В результате клонирования с сайта GitHub будет скопирована информация, необходимая для создания у вас на компьютере собственной блокчейн-цепи. Далее для построения собственного закрытого блокчейна достаточно выполнить действия из следующего подраздела.

Создаем собственный блокчейн

Теперь пришло время воспользоваться бесплатным инструментом **Docker Quick Start Terminal** для развертывания вашего личного блокчейн-проекта. Этот инструмент предоставляет доступ к виртуальной машине, что позволит сократить время, необходимое для настройки и отладки вашей системы. В конечном

результате будет создана стабильная среда окружения для вашего блокчейна, и вам не придется беспокоиться о настройке самого вашего компьютера. Итак, выполните следующее.

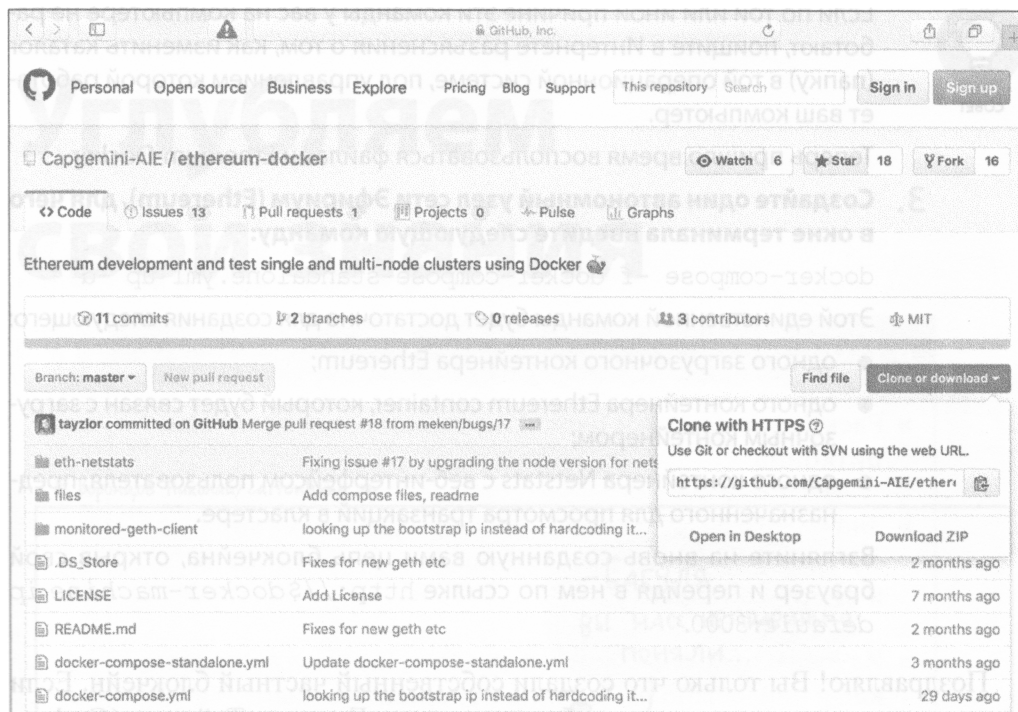


Рис. 3.5. Выберите вариант Open in Desktop

1. **Запустите на своем компьютере приложение Docker, воспользовавшись пиктограммой Docker Quick Start Terminal.**



СОВЕТ

Пиктограмма Docker Quick Start Terminal будет либо на рабочем столе, либо в меню Пуск вместе с прочими приложениями, установленными на вашем компьютере.

Приложение Docker откроет окно терминала (командное окно) которым вы будете пользоваться при создании собственного частного блокчейна.

2. **В окне терминала перейдите в папку (каталог) `ethereum`.**

Все создаваемые в процессе развертывания новой блокчейн-цепи файлы должны быть сохранены в том же месте, куда были помещены файлы, полученные в предыдущем разделе. Для того чтобы в окне терминала перейти в другой каталог, необходимо выдать соответствующую команду. Если ваш компьютер работает под управлением Mac OS или Linux, введите следующую команду:

```
cd ~ /Desktop/ethereum/ethereum-docker/
```



СОВЕТ

Если ваш ПК работает под управлением Windows, команда должна быть такой:

```
cd ~ \Desktop\ethereum\ethereum-docker\
```

Если по той или иной причине эти команды у вас на компьютере не работают, поищите в Интернете разъяснения о том, как изменить каталог (папку) в той операционной системе, под управлением которой работает ваш компьютер.

Теперь пришло время воспользоваться файлами Ethereum-Docker.

3. Создайте один автономный узел сети Эфириум (Ethereum), для чего в окне терминала введите следующую команду:

```
docker-compose -f docker-compose-standalone.yml up -d
```

Этой единственной команды будет достаточно для создания следующего:

- одного загрузочного контейнера Ethereum;
- одного контейнера Ethereum container, который будет связан с загрузочным контейнером;
- одного контейнера Netstats с веб-интерфейсом пользователя, предназначенного для просмотра транзакций в кластере.

Взгляните на вновь созданную вами цепь блокчейна, открыв свой браузер и перейдя в нем по ссылке `http://$docker-machine ip default:3000`.³

Поздравляю! Вы только что создали собственный частный блокчейн. Если это вас тронуло, скажите слово благодарности Грехему Тейлору (Graham Taylor) и Эндрю Донгу (Andrew Dong), которые потратили массу времени на создание интегрированной среды Ethereum-Docker.

³ `docker-machine ip default` — IP-адрес виртуальной машины приложения Docker, присвоенный ей по умолчанию.

Часть II

Углубляем свои знания

© Воронцов Николай/cartonbank.ru



В ЭТОЙ ЧАСТИ...

- » Раскрываем истоки блокчейн-технологии: блокчейн Биткойна
- » Знакомимся с сетью Эфириум и углубляем знания о децентрализованных автономных организациях и смарт-контрактах
- » Изучаем основные концепции сети Ripple и выясняем, как в ней можно мгновенно совершить обмен ценностями практически любого типа
- » Даем оценку блокчейну сети Factom и его возможностям в отношении защиты данных и систем
- » Исследуем высокоскоростной блокчейн DigiByte и знакомимся с некоторыми интересными приложениями, которые были созданы в сфере технологии блокчейна



Глава 4

Знакомьтесь: блокчейн Биткойна

В ЭТОЙ ГЛАВЕ...

- » Выясняем, откуда блокчейн Биткойна берет свое начало
- » Рассеиваем некоторые мифы о Биткойне
- » Обеспечиваем безопасность использования биткойнов
- » Обсуждаем возможности майнинга в сети Биткойна
- » Создаем бумажный кошелек для хранения биткойнов

Внимание! Прочитав эту главу, вы вполне можете оказаться на крючке какой-нибудь крутой новомодной технологии. Читайте ее на свой страх и риск.

Блокчейн Биткойна наиболее явно демонстрирует все аспекты блокчейн-технологии. Это та основа, с которой сравнивают все остальные блокчейн-проекты, и та структура, в которой были разработаны практически все концепции новой технологии. Изучив основы работы блокчейна Биткойна, вы сможете лучше понимать особенности любых других технологий, которые уже существуют или впоследствии появятся в данной экосистеме.

В этой главе представлена основная информация о том, как работает блокчейн Биткойна. Здесь же даны важные рекомендации, следуя которым, вы сможете накопить личный опыт работы в системе Биткойна. Вам также предложены

практические советы, как начать работать в среде Биткойна прямо сейчас. Вы узнаете, как майнить биткойны-токены, и откроете для себя новые способы работы в системе Биткойна без покупки ее криптовалюты. Наконец я расскажу вам о том, как положить биткойны-токены в бумажный кошелек, а также о других практических способах безопасного хранения биткойнов в сети.

Краткая история блокчейна Биткойна

Проект Биткойн и концепция его блокчейна впервые были представлены в виде документа осенью 2008 года, а позднее, в 2009 году, реализованы как программное обеспечение с открытым кодом. (С оригинальным основополагающим документом Биткойна можно ознакомиться по адресу <http://www.bitcoin.org/bitcoin.pdf>, а его перевод на русский язык вы найдете по ссылке https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf.)

Автором, впервые представившим миру концепцию Биткойна в документе 2008 года, был анонимный программист (или группа программистов), опубликовавший свое творение под именем “Сатоши Накамото”. Позднее, в процессе работы над реализацией проекта Биткойна, Накамото сотрудничал со многими разработчиками из числа последователей концепции ПО. Это продолжалось вплоть до конца 2010 года, когда этот человек (или группа людей) прекратил принимать участие в проекте и передал свои полномочия другим видным разработчикам ядра Биткойна. В отношении личности Накамото было выдвинуто множество предположений и различных теорий, однако на момент написания этих строк ни одна из них так и не получила окончательного подтверждения.

Как бы там ни было, этот Накамото сумел создать невероятную, поразительную одноранговую систему платежей, позволяющую пользователям пересылать биткойны — ее токены ценности — напрямую, т.е. без участия посредника, контролирующего работу обеих сторон. В качестве такого посредника здесь выступает сама сеть, проверяющая каждую транзакцию с целью получения гарантий, что в ней нет попытки обмануть систему, потратив одни и те же биткойны дважды.

Цель Накамото заключалась в стремлении заделать широкую брешь в доверии общества к цифровым документам. И концепция блокчейна оказалась тем самым средством, которое он искал. Она позволяла успешно решить задачу византийских генералов, которая стояла перед людьми от века и обрела особую важность при работе в компьютерной сети: “Как я могу доверять полученной информации и тем, кто мне ее сообщил, если корыстные люди, злонамеренные третьи стороны и иже с ними могут в любой момент попытаться меня обмануть?” Множество энтузиастов биткойна полагают, что блокчейн-технология является как раз тем недостающим звеном, которое позволит обществу

перенеси всю свою деятельность в сеть. Она расширяет рамки доверия, записывая в открытое общедоступное пространство релевантную информацию, которую в дальнейшем нельзя будет удалить или изменить и на которую всегда можно положиться в процессе принятия сложных решений.

В блокчейнах по-новому смешано много старых технологий, которые общество использовало уже тысячи лет. Например, смешение криптографии и процедуры платежа привело к созданию криптовалюты. *Криптография* — это искусство взаимодействовать защищенным образом на глазах у любых третьих сторон. Осуществление платежей с использованием токенов, лишь *представляющих* определенную ценность, но не *обладающих* ею непосредственно, также практикуется человечеством с давних времен. Смешение же этих двух давно известных вещей приводит к получению чего-то совершенно нового — криптовалюты. Криптовалюта позволяет взять концепцию денег и перенести ее в виртуальную интерактивную среду, сохранив при этом возможность осуществлять в ней продажу ценности защищенным образом — за счет использования токена.

Технология блокчейна также включает *хеширование* (преобразование данных любого размера в короткие значения фиксированной длины). Хеширование, в свою очередь, опирается на другую достаточно давно известную технологию, называемую “дерево Меркла”. Ее суть в том, что несколько хешей последовательно сжимаются до одного хеша, и при этом сохраняется возможность проверить достоверность каждого элемента данных, который хешировался индивидуально в начале процедуры (общая ее схема представлена на рис 4.1).

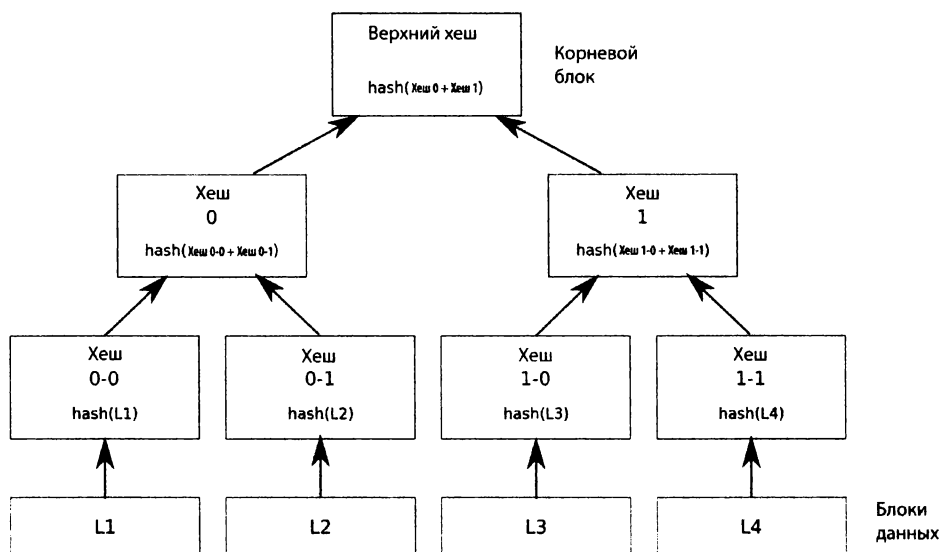


Рис. 4.1. Дерево Меркла

И наконец, любой блокчейн, безусловно, представляет собой регистрационный журнал, *реестр*, — документ, который человечество использовало для хранения финансовой и иной важной информации тысячи лет. Когда все эти старые методы объединяют в нечто единое, функционирующее в интерактивной виртуальной среде как распределенная база данных, конечный результат представляет собой нечто революционное.

Система Биткойна первоначально была разработана исключительно для поддержки ее криптовалюты — биткойна. Но очень скоро ее создатели поняли, что заложенная в ее основу технология имеет гораздо больший потенциал. Приняв это во внимание, они разработали архитектуру блокчейна Биткойна таким образом, чтобы в него можно было записывать больше чем просто сведения о перемещении его токена. Ныне блокчейн Биткойна самый старый и один из самых больших по размеру блокчейнов в мире. Его сеть включает тысячи полных узлов, на которых работает протокол Биткойна. Именно этот протокол обеспечивает создание и защиту блокчейна.



ЗАПОМНИ!

Говоря очень простыми словами, *блокчейн* представляет собой открытый реестр всех транзакций, выполненных в сети Биткойна за все время ее существования, а *полные узлы* являются компьютерами, обеспечивающими хранение этого реестра и запись в него информации. *Протокол Биткойна* — это система правил, регламентирующих, как все это должно функционировать.

Полные узлы защищают сеть Биткойна посредством майнинга ее криптовалюты. Новые токены-биткойны выдаются в качестве награды за обработку транзакций и их запись в блокчейн системы. Узлы также получают небольшую плату за подтверждение транзакций.

Любой желающий может запустить на своем компьютере протокол Биткойна и заняться майнингом его токенов. Это проект с открытым кодом, в котором приветствуется постоянный рост числа независимых участников в его сети. Чем меньше людей участвует в поддержке работы проекта, тем более централизованным он становится, а централизация ослабляет систему. То, что, в первую очередь, делает Биткойн защищенной системой, — это множество независимых полных узлов, физически распределенных по всему миру.

Наиболее успешные майнеры обладают мощными системами, которые по своей производительности могут во много раз превосходить более слабые компьютеры других майнеров. На начальном этапе развития сети можно было запускать протокол Биткойна и зарабатывать монеты на обычном персональном компьютере. Сейчас же, чтобы иметь надежду хотя бы иногда получать новые биткойны, придется заказать, запустить и обслуживать дорогое специализированное оборудование или воспользоваться облачным сервисом.

Чтобы поместить новую запись в блокчейн Биткойна, нужно отправить некоторое количество биткойнов с одного счета на другой. Когда вы отправляете новую транзакцию в систему Биткойна, сообщение о ней сразу же рассылается по всей сети. После отправки сообщения уже невозможно его изменить, поскольку это сообщение будет навсегда вписано в блокчейн Биткойна. Такая особенность требует тщательного обдумывания каждого выполняемого в сети действия и тщательного хранения своей конфиденциальной информации.

Распространение одного и того же сообщения по всей сети из тысяч узлов, а затем сохранение его навсегда в реестре движения токенов предполагает высокую оперативность. Поэтому протокол Биткойна требует, чтобы ваши сообщения были максимально короткими: действующее ограничение на их максимальный размер составляет всего 40 символов.

ОГРАНИЧЕНИЯ В СИСТЕМЕ БИТКОЙНА

Размер блоков, из которых строится блокчейн Биткойна, ограничен на уровне 1 Мбайт. Этот порог ограничивает число транзакций, которые блокчейн Биткойна может обработать в секунду, до семи. Новые блоки в блокчейне появляются в среднем каждые десять минут, но это не гарантируется.

Эти ограничения жестко прописаны в протоколе Биткойна и гарантируют, что сеть системы останется децентрализованной. В свою очередь, децентрализация является главным условием неизменности и надежной работы всей системы Биткойна. Большой размер блоков создал бы дополнительные трудности для майнеров, что могло бы иметь следствием вытеснение из сообщества полных узлов мелких операторов.

Система Биткойна имеет встроенные ограничения, которые предупреждают ее от обработки глобальных объемов денежных операций. Она также используется для защиты других типов данных и систем. Спрос на использование защищенного реестра Биткойна очень высок. На эти дополнительные осложнения ссылаются как на *раздувание Биткойна*, а их наличие замедляет работу сети и увеличивает стоимость транзакций.

На данный момент большая часть блокчейн-разработчиков лишь экспериментируют с расширением использования блокчейна Биткойна. Большинство из них еще не достигло того момента, чтобы начать масштабировать их прототипы и концепции, поэтому система Биткойна может справиться с их запросами. Появление новых блокчейн-технологий и систем также позволяет снизить нагрузку на систему Биткойна и предоставляет разработчикам более дешевые способы организовать защиту данных.

Биткойн — это живая и постоянно меняющаяся система. Сообщество разработчиков ядра Биткойна активно ищет способы улучшения системы с целью сделать ее более сильной и быстрой. Любой может внести свой вклад в протокол Биткойна, представив свои предложения на сайте его сообщества GitHub (<http://www.github.com/bitcoin>). Тем не менее сообщество ведущих разработчиков ядра Биткойна невелико. Наиболее значительный вклад был сделан Владимиром Ван-дер-Лааном (Wladimir Van Der Laan), Петером Вуйли (Pieter Wuille) и Гевинотом Андресеном (Gavin Andresen).

КАК МИР ПЕРЕВЕРНУЛСЯ: ДРАМА БИТКОЙНА

Вокруг разработки ядра Биткойна имеет место серьезный конфликт, получивший название “Гражданская война Биткойна” или “Дебаты об ограничениях на размер блока”. Это общий конфликт между сторонниками сохранения ядра биткойна в его нынешнем состоянии и желающими увеличить функциональные возможности программного обеспечения системы. Подобный конфликт кажется простым, но его последствия могут быть огромны. Неизменная природа самого Биткойна и миллиарды долларов стоимости активов, которые защищает его программное обеспечение, означают, что каждое изменение в коде должно тщательно анализироваться и обсуждаться.

Система Биткойна не только подвержена внутренним конфликтам, но и находится под интенсивным наблюдением извне. Децентрализованная природа Биткойна, которая в конечном счете способна вытеснить из общества центральные органы власти, сделала эту систему постоянной мишенью для всевозможных регулирующих органов. Появление Биткойна, кроме того, весьма приветствовалось людьми, которые хотели анонимно приобретать запрещенные товары или совершать незаконные сделки, а также перемещать денежные средства из контролируемых экономик в неконтролируемые в обход всех правительственных запретов. Эти факторы в свое время принесли Биткойну плохую репутацию и сформировали достаточно негативное отношение к нему в обществе. Однако предприниматели, которые хотели извлечь выгоду из новой технологии Биткойна, сумели вернуть к нему интерес и уважение. Были даже сделаны определенные изменения в терминологии с целью обособить программную структуру Биткойна и других криптовалют. В результате программное решение, используемое в системе поддержки криптовалют, стали называть *блокчейном*. Это смещение акцента с вызывающих споры токенов на исключительные возможности структур, обеспечивающих их существование, изменило взгляд на Биткойн как правительственных, так и коммерческих структур — от страха к восхищению.

Некоторые заблуждения в отношении Биткойна

Люди обычно с подозрением относятся ко всему новому, в особенности к тому, что им трудно понять. Поэтому вполне естественно, что биткойн — совершенно новая валюта, не похожая ни на что, что существовало прежде — вызывает у них опасения, в результате чего возникают ошибочные представления об этом предмете.

Вот некоторые из подобных заблуждений в отношении Биткойна, которые вы, возможно, уже слышали.

- » **Биткойн был взломан хакерами.** В истории Биткойна никогда не было ни одной успешной хакерской атаки на его блокчейн с целью похищения монет. Многие *централизованные* системы, работавшие с биткойнами, действительно были атакованы. И веб-сайты предоставления биткойн-кошельков, и биткойн-биржи подвергались успешным атакам вследствие плохой организации их защиты. В целях противостояния злоумышленникам Биткойн-сообщество разработало элегантные решения для безопасного хранения монет, включая шифрование кошельков, мультиподпись, офлайн-кошельки, бумажные кошельки и даже аппаратные кошельки.
- » **Биткойн используется для вымогания у людей денег.** Вследствие своей полуанонимной природы криптовалюты Биткойна может использоваться программами-вымогателями. В этой схеме хакеры пробивают брешь в какой-либо сети и держат ее в “заложниках”, пока им не выплатят требуемую сумму в биткойнах. Известны случаи, когда больничные или школьные сети становились жертвами подобных атак. Однако в отличие от наличных денег, которым преступники отдавали предпочтение ранее, в системе Биткойна их действия всегда оставляют след, который навечно записан в блокчейн и вполне может использоваться следователями.
- » **Биткойн — это финансовая пирамида.** С точки зрения майнеров Биткойна, эта система является полной противоположностью финансовой пирамиде. Биткойн-протокол спроектирован как некая “каннибалистическая гонка вооружений”. Суть в том, что появление в сети очередного нового майнера вынуждает протокол повышать сложность процедуры майнинга. С точки зрения общества, Биткойн — это рыночная система в чистом виде. Цена монет-биткойнов подвержена постоянным флуктуациям в соответствии с состоянием рынка, спросом на них и восприятием уровня их ценности.

- » **Биткойн прекратит свое существование, когда будет намайнен 21 миллион монет.** В системе Биткойна установлен лимит на количество токенов, которые могут быть выпущены. Этот лимит жестко задан в программном коде и составляет всего 21 миллион монет. Ориентировочная дата выпуска последнего биткойна — 2140 год. Никто не может предсказать, что именно произойдет в тот момент, но майнеры биткойна всегда будут получать некоторую прибыль как плату за запись транзакций в блокчейн. Кроме того, пользователи блокчейна и сама система блокчейна вынуждены будут стимулировать действия по защите сети, поскольку, если майнинг прекратится, система биткойна станет уязвимой, и в таком же состоянии окажутся данные, зафиксированные ранее в блокчейне.
- » **При достаточном количестве компьютерных мощностей можно преодолеть защиту сети Биткойна.** Данное замечание верно, но достичь этой цели невероятно сложно, в результате чего полученный выигрыш в конечном счете окажется совершенно ничтожным. Чем больше полных узлов будет функционировать в сети Биткойна, тем труднее будет осуществить подобную атаку. Сейчас, чтобы снять защиту сети, атакующему требуется количество энергии, эквивалентное тому, которое производит, например, вся Ирландия. Кстати, выгода от такой атаки будет очень невелика. Все, чего сможет достичь атакующий, — это откатить собственные транзакции. Он не сможет забрать себе чужие биткойны, подделав транзакции либо изменив владельцев монет.
- » **Вложения в Биткойн — это хорошая инвестиция.** Биткойн — это новый и интересный этап в эволюции того, как люди осуществляют торговлю ценностью. За этим проектом не стоит ни одно правительство или официальная организация. Биткойны имеют какую-то ценность только потому, что люди согласны продавать и покупать за них товары и услуги. Однако это желание людей и возможности использования биткойнов в значительной степени подвержены колебаниям. Поэтому вложения в биткойны являются нестабильной инвестицией и, следовательно, к этому вопросу следует подходить с осторожностью.

Биткойн: новый Дикий Запад

Мир Биткойна сейчас сильно напоминает первые дни эпохи Дикого Запада. В этом мире лучше подходить ко всему с осторожностью, пока не выясните для себя, кто здесь хороший парень, а кто — плохой и в каком салуне подают самое холодное пиво. Если вы окажетесь жертвой мошенничества, вам здесь никто не поможет.



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

В США токен Биткойна подпадает под категорию *товара*, согласно Закону об обмене товарами, тогда как во многих европейских странах он рассматривается как валюта, но над ним здесь не установлено никакого надзора.

В этом разделе мы обсудим три типичных вида мошенничества, преобладающих в мире криптовалют. Все они предполагают похищение ваших монет и достаточно похожи на традиционные аферы и махинации, с которыми вы, вероятно, уже сталкивались. Этот перечень не претендует на полноту, поскольку мошенники ничего не достигнут, если не будут подходить к своему делу творчески, а значит, всегда будьте настороже, манипулируя своими биткойнами! Вы не можете знать, что вас ждет за следующим углом.

Поддельные сайты

Веб-сайты, которые выглядят как биржи или сайты веб-кошельков, но являются поддельными, уже давно досаждают некоторым из ведущих веб-сайтов в мире Биткойна. Этот тип мошенничества достаточно распространен как в среде Биткойна, так и в Интернете в целом. Владельцы таких сайтов надеются сделать деньги, украв идентификационные данные и пароли пользователей либо уведя их на ложные адреса для отправки биткойнов.



СОВЕТ

Всегда дважды проверяйте URL-адреса и пользуйтесь только защищенными веб-сайтами (т.е. сайтами, адреса которых начинаются с <https://>), это позволит вам избежать проблем. Если веб-сайт или ссылки на нем кажутся вам подозрительными, проверьте, присутствует ли данный адрес в списке на сайте [Badbitcoin.org](http://www.badbitcoin.org) (<http://www.badbitcoin.org>). Список на этом сайте не является исчерпывающим, но большинство опасных сайтов в нем указано.

Нет, сначала вы!

“Отправьте мне биткойны — и я вышлю вам товар”. Скверно пахнет, правда? Мошенничества такого типа ничем не отличаются от мошенничеств с предварительным переводом денег за товар или услугу. В каждом случае некто предлагает вам купить что-то, что вы никогда не получите.

Наполовину анонимная природа Биткойна в сочетании с отсутствием возможности отменить транзакцию делают чрезвычайно затруднительными любые попытки вернуть ваши деньги. Кроме того, на данный момент не предоставляется никакой защиты биткойн-транзакций со стороны административных или правовых учреждений, поэтому на их поддержку рассчитывать не приходится, вы останетесь один на один со своей проблемой.

Мошенники могут попытаться войти к вам в доверие, предоставив поддельные идентификационные данные или даже выдав себя за других людей, которых вы можете знать. Всегда дважды проверьте любую информацию, которая поступила к вам от другой стороны совершаемой сделки.



СОВЕТ

Наилучший способ не попадаться на такие уловки — прислушиваться к своей интуиции и никогда не рисковать большей суммой, биткойнов чем та, которую вы готовы потерять. Если существует возможность проверить информацию о получателе вне сети — в реальной, а не виртуальной среде, — обязательно сделайте это.

Схемы быстрого обогащения

В мире криптовалют процветают всевозможные безумные схемы сверхбыстрого обогащения. Но есть и хорошая новость: их очень просто распознать, если знать, что искать.

Чаще всего вам будут обещать огромные доходы, и при этом в том или ином виде будут явно просматриваться попытки вербовки и идеологической обработки. Этот процесс может включать такие вещи, как обучение методам продаж, просьбы привлечь в дело ваших друзей и родственников, клятвенные заверения, что данное вложение совершенно безопасно и вы никогда не потеряете своих денег.

Подведем черту: если схема выглядит слишком хорошо, чтобы быть правдой, вероятнее всего, это просто надувательство. В любом случае внимательно присмотритесь к тому, как предлагаемые инвестиции будут генерировать внешнюю стоимость и что именно вы получите от своих инвестиций. Если вы не обнаружите ясной и разумной причины, обеспечивающей возможность получения столь высоких доходов, это мошенничество.



СОВЕТ

Прежде чем решиться на инвестиции, проконсультируйтесь у юриста и сертифицированного аудитора. Они помогут вам понять имеющиеся риски и потенциальные изменения в вашем налогообложении.

Майнинг биткойнов

Начать зарабатывать биткойны можно разными способами. Майнинг биткойнов позволяет зарабатывать эти монеты посредством участия в работе Биткойн-сети. Как правило, этот процесс реализуется с помощью специального оборудования для майнинга, очень дорогого и узкоспециализированного. На этом оборудовании будет работать программное обеспечение майнинга, обеспечивающее подключение к блокчейну Биткойна и участие в майнинговом

пуле (*mining pool*), позволяющем объединить усилия многих майнеров с целью повышения вероятности получения награды, которая затем будет распределена между всеми участниками пула.

Существует три стандартных средства, позволяющих познакомиться с процедурой майнинга в системе Биткойна.

- » **Bitcoin-QT.** Клиент майнинга Bitcoin-QT представляет собой оригинальное программное обеспечение, написанное самим Сатоши Накамото. Его можно загрузить, перейдя по ссылке <https://bitcoin.org/en/download>.
- » **CGminer.** Клиент CGminer — это один из наиболее популярных вариантов программного обеспечения для майнинга. Он относится к категории ПО с открытым кодом и имеет версии для работы под управлением Windows, Linux и OS. Загрузить его можно по адресу <http://www.github.com/ckolivas/cgminer>.
- » **Multiminerapp.** Приложение Multiminerapp представляет собой простой клиент для майнинга. Загрузить его можно по адресу <http://www.multiminerapp.com>.



ЗАПОМНИ

Система Биткойна — очень конкурентная среда, и если вы не купите специальное оборудование для майнинга, у вас просто нет шансов заработать хоть что-нибудь. В этой книге я не стану предлагать или рекомендовать вам какой-то конкретный тип такого оборудования, поскольку эта индустрия очень динамична и новые модели быстро сменяют одна другую. Могу только сказать, что за одну машину вам в среднем придется выложить от 500 до 5000 долларов. Искать такое оборудование лучше всего на сайте компании Amazon.com. У них очень большой выбор и богатый архив комментариев покупателей, который послужит вам отличным руководством для выбора.

Облачный майнинг (аренда чужих вычислительных мощностей, осуществляющих майнинг биткойнов) позволит вам начать зарабатывать биткойны в течение одного дня без необходимости загружать программное обеспечение или покупать какое-то оборудование. Достаточно будет просто выполнить следующие действия.

1. Зайдите на сайт <https://hashflare.io/panel>.



ВНИМАНИЕ!

Учтите, что доход от вложений в облачный майнинг может оказаться и величиной отрицательной. Внимательно проанализируйте все условия заключения сделки и обязательно убедитесь, что ваши инвестиции будут прибыльными, а не убыточными.

2. **Пройдите процесс регистрации.**
3. **Щелкнув на соответствующей ссылке, введите в своем профиле адрес (открытый ключ) вашего биткойн-кошелька.**

В дальнейшем это позволит вам успешно выводить заработанные майнингом средства. Если у вас еще нет собственного кошелька в системе Биткойна, обратитесь к главе 3 и выполните указанные в ней действия по его созданию.

4. **Прокрутите окно до панели SHA-256 и щелкните на кнопке Buy Now (пиктограмма в виде тележки супермаркета).**

С помощью ползунка Выберите хэшрейт уточните, на какой хешрейт (объем арендуемой мощности майнинга) вы сможете рассчитывать, исходя из предполагаемой суммы инвестиции.



СОВЕТ

Во время написания этой книги данный вариант хешрейта давал наибольший возврат на инвестиции и требовал наименьших стартовых вложений. Не пожалейте времени, чтобы лично вновь убедиться в этом, поскольку ситуация со временем может измениться.

5. **Приняв решение, щелкните на кнопке Далее, чтобы купить желаемый объем мощности майнинга.**

Откроется окно, в котором можно оформить, а затем провести процедуру инвестиции. Это позволит вам присоединиться к сети Биткойна.

6. **Перед завершением работы выберите один из предлагаемых на панели SHA-256 майнинговых пулов.**

Это позволит вам быстрее получить награду за майнинг в сравнении с майнингом в одиночку. В майнинговом пуле объединяются майнинговые мощности нескольких майнеров, а полученное вознаграждение распределяется между всеми членами пула в зависимости от их вклада.

Поздравляю! Теперь вы можете откинуться на спинку кресла и просто ждать, пока в ваш биткойн-кошелек потекут (или хотя бы начнут капать) биткойны.

Создаем первый бумажный кошелек

Бумажный биткойн-кошелек — это представленные на бумаге открытый и закрытый ключи вашего счета в системе Биткойна. Поскольку они никак не связаны с компьютерными сетями, такие кошельки — одно из наиболее надежных и безопасных средств хранения биткойнов, если, конечно, все выполнено правильно. Преимущество в данном случае состоит в том, что ваш закрытый ключ не сохраняется на каких-либо электронных носителях в цифровом виде, а значит, не может стать объектом хакерской атаки. Создать бумажный кошелек чрезвычайно просто. Достаточно лишь выполнить следующее.

1. Зайдите на сайт <http://www.bitaddress.org>.
2. В открывшемся окне некоторое время произвольно перемещайте указатель мыши, пока счетчик показателя случайности не достигнет значения 100%.

Когда это произойдет, будет сгенерирован случайно выбранный номер нового биткойн-счета, а его ключи будут предоставлены вам в открывшемся окне.

3. Щелкните в этом окне на кнопке **Paper Wallet (Бумажный кошелек)**.

Вам будет предоставлена возможность создать бумажный кошелек, который затем можно будет распечатать на принтере.

4. В поле **Addresses to Generate (Сгенерировать адресов)** введите значение 1.

За один просчет вы можете создать сразу несколько кошельков, если это требуется, но для нашего примера достаточно и одного.

5. Щелкните на кнопке **Generate (Сгенерировать)**.

На рис. 4.2 показан созданный подобным образом бумажный биткойн-кошелек.



Рис. 4.2. Бумажный биткойн-кошелек

6. Чтобы получить бумажную копию, щелкните на кнопке Print (Печатать).



ВНИМАНИЕ!

При создании и печати бумажного кошелька следите, чтобы рядом с вами не было посторонних. Это, определенно, не та работа, которую можно выполнять на общедоступном компьютере. Кроме того, убедитесь, что выбранный вами для печати принтер не подключен к вашему компьютеру через Интернет — это позволит исключить риск, что ваш закрытый ключ будет украден хакерами.



СОВЕТ

Заламинируйте свой бумажный кошелек, чтобы защитить его от повреждений.



Глава 5

Встречайте: блокчейн Эфириум

В ЭТОЙ ГЛАВЕ...

- » Узнаем, как и для чего был создан Эфириум
- » Знакомимся с Эфириум-блокчейном
- » Обсуждаем возможности взлома блокчейна
- » Начинаем работать с Эфириумом
- » Создаем децентрализованную автономную организацию

Проjekt Эфириум (Ethereum) — один из наиболее развитых и доступных блокчейнов в этой экосистеме. Он также является абсолютным лидером в блокчейн-инновациях и способах их использования. Понимать особенности этой технологии очень важно, поскольку Эфириум лидирует в поддержке смарт-контрактов и децентрализованных организаций.

В этой главе рассказывается о том, откуда появился и как развивался Эфириум, а также обсуждаются новые способы построения организаций и компаний на базе Эфириум-блокчейна. Необходимое внимание, кроме того, уделяется безопасности блокчейна Эфириума и его практическому использованию в бизнесе. Так, вы узнаете, как запустить проект и направить его в нужное русло.

И наконец в этой главе речь пойдет о том, как создать собственную децентрализованную организацию. Вы узнаете, как майнить в тестовой сети

криптовалюту, которая послужит движущей силой вашего проекта. Прочитав эту главу, вы также научитесь создавать собственные Эфириум-кошельки и осуществлять операции с этими токенами.

Знакомимся с историей появления и развития Эфириума

Описание проекта Эфириум впервые было представлено в 2013 году в основополагающем документе, написанном Виталиком Бутериным, активным членом биткойн-сообщества в качестве писателя и программиста. Бутерин видел в Биткойне исключительно большой потенциал, определяемый возможностью перемещения ценности при отсутствии центрального управляющего органа. Он внес определенный вклад в инновацию *Colored Coins* (*цветные монеты*), имеющую целью расширение способов использования Биткойна, помимо торговых операций с его собственным токеном. Бутерин полагал, что и многие другие бизнес-процессы или правительственные функции, осуществляемые при наличии централизованного органа, могут быть реализованы на основе блокчейн-структур.

В это время велись острые дебаты по поводу “раздувания” сети Биткойна за счет множества транзакций с незначительной стоимостью, поступающих от приложений, обеспечивающих себе защиту за счет эксплуатации возможностей Биткойна. Основным обсуждаемым тезисом было утверждение, что дополнительные приложения, построенные на основе Биткойн-протокола, вызовут значительные проблемы в работе сети из-за роста объема транзакций. Система Биткойна создавалась без учета потребности обработки многочисленных транзакций, генерируемых такими приложениями. Виталик, как и многие другие, полагал, что для того, чтобы строить децентрализованные приложения на основе блокчейна Биткойна, требуется либо существенная переработка его программного обеспечения, либо вообще создание совершенно нового блокчейна.

На этот момент Биткойн был уже вполне устоявшейся системой. Было очевидно, что внесение необходимых изменений в код его ядра оказалось уже за пределами реально осуществимого. Главные идеологи Блокчейна застопорили бы проведение любых изменений в работе сети. В начале 2014 года Виталик и его команда создали фонд Эфириума с целью собрать необходимые средства для построения нового блокчейна со встроенным в него языком программирования.

Начальные этапы разработки спонсировались через интерактивный крауд-фандинг, сбор средств осуществлялся в июле и августе 2014 года. Активы фонда исходно составили около 18 миллионов долларов, полученных за счет продажи токенов криптовалюты проекта, получившей название “эфир”. Все это сопровождалось ожесточенными спорами в отношении того, является ли такой

вариант краудфандинга легальным, поскольку он может расцениваться как нелицензированный выпуск ценных активов.

Однако занесение проекта в серую зону с точки зрения легальности не смогло воспрепятствовать его продвижению. Как бы там ни было, острая новизна проекта притягивала к фонду общее внимание и талантливых исполнителей. Неудовлетворенные и бесправные разработчики со всего мира собрались в этом проекте. Децентрализация рассматривалась как идеальное решение для противостояния угнетению со стороны коррумпированных центральных органов власти.

Те 18 миллионов долларов, которые были получены в результате торговли токенами, позволили основателям организации нанять большую команду разработчиков, задачей которой было создание сети Эфириума. Первая рабочая версия блокчейна сети получила название *Ethereum Frontier*; она была запущена в эксплуатацию в конце июля 2015 года. Это был базовый релиз программного обеспечения, который только технически подкованные специалисты могли использовать для построения собственных приложений.

Новая, текущая версия протокола сети, получившая название *Homestead*, была введена в эксплуатацию в марте 2016 года. Она имеет значительно более дружелюбный пользовательский интерфейс, а предлагаемым в ней шаблоном приложения может воспользоваться для своих целей практически любой человек. Помимо прочего, у проекта Эфириум есть большое сообщество преданных ему разработчиков.

Следующим планируемым релизом протокола Эфириума будет *Metropolis*. Главное отличие этой версии будет состоять в том, что приложения будут полностью разработаны и хорошо протестированы. Эти приложения также будут еще более простыми в использовании и ориентированными на более широкий рынок применения, что позволит людям даже с очень небольшими техническими познаниями не испытывать затруднений, работая с ними.

Последним планируемым этапом развития сети Эфириум будет версия *Serenity*. На этой стадии протокол блокчейна Эфириума перейдет от консенсуса типа “proof-of-work” (доказательство выполнения работы, когда майнеры соревнуются в создании очередного блока) к модели консенсуса “proof-of-stake” (доказательство доли владения). В этой модели узлы, формирующие блоки, выбираются псевдослучайно и вероятность выбора любого узла пропорциональна той доле, которую составляет принадлежащая ему сумма криптовалюты в отношении к общему ее количеству в сети. Основным преимуществом при такой замене является сокращение затрат энергии отдельными узлами в сравнении с тем, что требуется по методу “proof-of-work”. А это сделает поддержку полных узлов в сети более привлекательной для индивидуалов, что в конечном счете будет способствовать росту ее децентрализации и защищенности.

Эфириум: Всемирный компьютер с открытым кодом

Эфириум, возможно, — один из самых сложных блокчейнов из числа когда-либо созданных. У него есть собственный полнофункциональный язык программирования, позволяющий разработчикам создавать приложения любого типа. Протокол Эфириума может выполнять практически все, что возможно осуществить средствами любого обычного языка программирования, и это помимо того, что он встроен внутрь блокчейна, что само по себе дает ему дополнительные преимущества и уровень защищенности. Если вы способны представить себе какой-то программный проект, то знайте, что он может быть реализован в среде Эфириума.

Сейчас экосистема Эфириума — наилучшее место для создания децентрализованных приложений. Здесь имеется превосходная документация и предоставляется дружелюбный интерфейс, что позволяет быстро включиться в работу. Ускоренный процесс разработки, обеспечение защиты для малых приложений и предоставление приложениям возможности легко взаимодействовать одно с другим — ключевые характеристики этой системы.

Полный по Тьюрингу язык программирования — это главная особенность, которая делает блокчейн Эфириума гораздо более мощным (в сравнении с Биткойном) инструментом создания новых программ. Язык сценариев среды Эфириума (*Solidity*) позволяет создать приложение, подобное Твиттеру, с помощью лишь нескольких строк кода, обеспечивая ему при этом исключительную защищенность.

В среде Эфириума также могут быть созданы смарт-контракты, подобные тому, который вы создали в главе 3. Протокол Эфириума открыл совершенно новый класс приложений. Вы можете взять практически любой процесс в бизнесе, правительственных органах или в любой иной организации и создать его цифровое представление в блокчейне Эфириума. В настоящее время платформа Эфириума уже эксплуатируется для управления цифровыми активами (*digital assets* — новый класс активов, которые размещаются в сети и могут представлять полностью цифровой актив, подобный биткойн-токену, или являться цифровым представлением активов реального мира, например запаса кукурузного зерна), финансовыми инструментами (подобными ипотечным ценным бумагам), записями о владении имуществом (например, землей) и децентрализованными автономными организациями (DAO). Последние представляют собой новый способ организации бизнес-структур, некоммерческих, правительственных или любых других организаций, члены которых должны иметь возможность договариваться и совместно работать в общих интересах. Поддержка DAO была встроена в платформу Эфириума изначально.

Децентрализованные приложения: добро пожаловать в будущее

Наиболее революционным и вызывающим дискуссии нововведением Эфириума являются самоуправляемые и децентрализованные приложения (DAPP). Они могут управлять такими объектами, как цифровые активы и децентрализованные автономные организации (DAO).

Децентрализованные приложения были созданы взамен централизованного управления активами и организациями. Эта структура для многих оказалась очень привлекательной, поскольку давно уже известно, что абсолютная власть развращает абсолютно. Для тех, кто боится утратить контроль, внедрение структур этого типа будет иметь серьезные последствия.

Игра Etheria (<http://www.etheria.world>), подобная известной игре Minecraft, является интересным примером этой технологии в действии (рис. 5.1). Она не может быть подвергнута цензуре или удалена из сети и будет существовать столько, сколько будет существовать блокчейн Эфириума. Если в Эфириуме было что-то создано, то удалить эту структуру или организацию, даже при наличии на то веских оснований, практически невозможно.

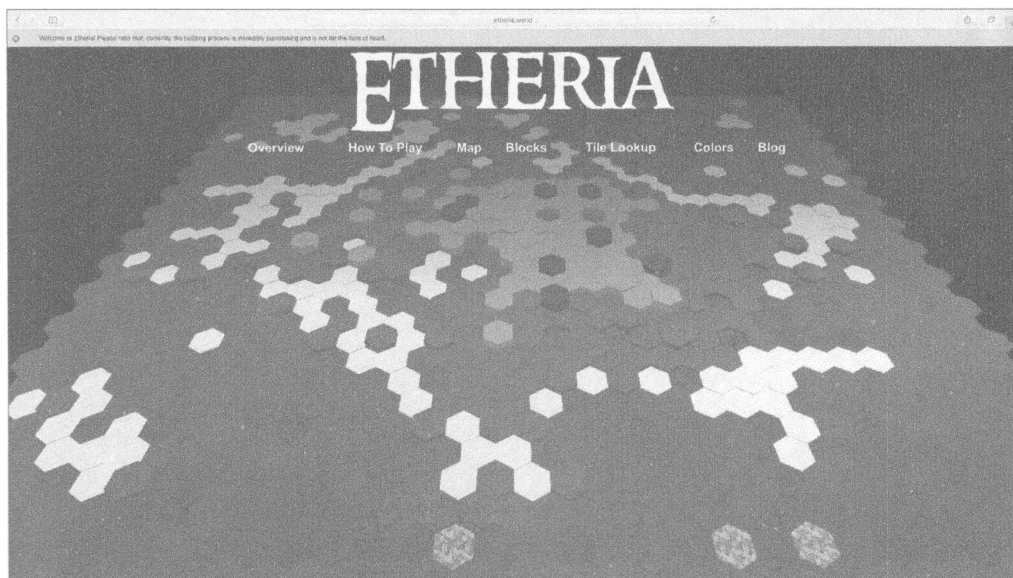


Рис. 5.1. Первая в мире бессмертная цифровая игра Etheria

Сила децентрализованных автономных организаций

Децентрализованные автономные организации (DAO) представляют собой такой тип эфириум-приложений, которые представляют в блокчейне Эфириума

виртуальную организацию. При ее создании вы можете пригласить других людей для участия в управлении данной организацией. Участники могут оставаться анонимными и никогда не встречаться в реальности, что может противоречить правилу “Знай своего клиента” (процедура, согласно которой в бизнесе осуществляется проверка подлинности клиента) и создавать проблемы с соблюдением требований защиты от отмыwania денег (законы и положения, предназначенные для воспрепятствования практике получения доходов из нелегальных источников).

Децентрализованные автономные организации были разработаны с целью сбора средств для инвестирования, но они могут предназначаться и для гражданских или некоммерческих целей. Система Эфириума предоставляет базовую среду для осуществления руководства. И уже только от организаторов проекта зависит, над чем именно будет осуществляться руководство. В среде Эфириума были созданы различные шаблоны, предназначенные для оказания помощи в процессе создания децентрализованных автономных организаций.

На рис. 5.2 показано, как организация может быть представлена в эфириум-приложении.

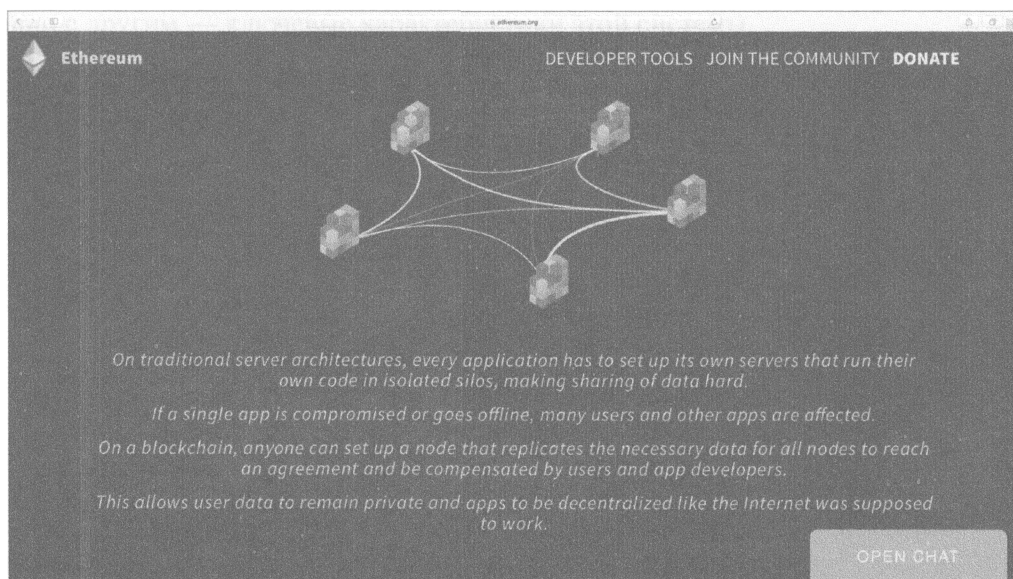


Рис. 5.2. Представление блокчейна приложения на сайте Ethereum.org

Вот основные принципы работы децентрализованных автономных организаций.

1. Группа людей готовит смарт-контракт по созданию организации и управлению ею.

2. Участники выделяют организации денежные средства и получают взамен токены, представляющие их собственность.
Эта схема работает подобно акциям компаний, но в данном случае участники получают контроль над фондами с первого дня.
3. Когда необходимая сумма собрана, организация начинает функционировать и ее члены могут начать подавать на рассмотрение предложения о том, как и на что расходовать имеющиеся средства.
4. По каждому предложению члены организации проводят голосование.
5. Для каждого предложения, когда заранее установленное для него время голосования истекло и было собрано заранее определенное количество голосов, оно либо принимается, либо отклоняется.
6. Определенные члены выступают в качестве подрядчиков для обслуживания организации.

В отличие от большинства традиционных инвестиционных инструментов, где решение об инвестировании принимает только центральное звено, члены децентрализованной автономной организации контролируют все 100% активов. По поводу всех инвестиций и прочих решений всегда проводится голосование. Такая организационная структура угрожает полным отказом от института традиционных финансовых менеджеров.

Распределенные автономные организации строятся с помощью программных инструментов и их код не может подвергаться изменениям в процессе функционирования. Привлекательность такого подхода состоит в том, что злонамеренные хакеры не смогут манипулировать фондами в традиционном смысле. Тем не менее хакеры все же могут найти способы заставить программное обеспечение функционировать непредвиденным образом и тем самым попытаться вывести средства. Неизменяемая природа программного кода распределенных организаций делает практически невозможным исправление обнаруженных в нем ошибок, когда эти организации уже функционируют в среде блокчейна Эфириума.

С БОЛЬШОЙ СИЛОЙ ПРИХОДЯТ... БОЛЬШИЕ ВОЗМОЖНОСТИ

Первая распределенная автономная организация (DAO), созданная в среде Эфириума, называлась довольно банально: "The DAO". Ее история явила яркий пример определенных опасностей, свойственных децентрализованным и автономным образованиям. Это был крупнейший в мире краудфандинговый проект — его активы составили 162 миллиона долларов, поступивших за 26 дней более чем от 11 тысяч человек. То, что эти люди считали величайшей силой своей организации, превратилось в ее величайшую слабость. В неизменяемый

программный код этой DAO были жестко вписаны правила, как эта организация управляется и как распределяются ее фонды. Такой подход позволял членам организации считать свои инвестиции надежно защищенными. И хотя программный код предварительно был тщательно проверен, некоторые имевшиеся в нем недоработки все же не были своевременно обнаружены.

Первой существенной угрозой в среде Эфириума стала хакерская атака на организацию "The DAO". Непредвиденный способ использования программного кода позволял достаточно умному клиенту выводить ее средства в свое личное распоряжение. Неизвестный пользователь сумел изъять из фондов организации эфиры на сумму около 50 миллионов долларов, прежде чем его остановили.

Сообщество Эфириума ожесточенно дебатировало о том, можно ли и нужно ли вернуть владельцам украденные эфиры. Тот, кто атаковал "The DAO", технически не выполнил ничего запрещенного и, по сути, даже не взламывал саму систему. Фундаменталисты в сообществе Эфириума считали, что программный код в том виде, в каком он был принят, является законом, а значит, не следует что-либо предпринимать с целью вернуть изъятые фонды.

Как оказалось, то, что делает Эфириум сильным, одновременно является и его величайшей слабостью. Децентрализация, неизменность и автономия в совокупности означают отсутствие центральной власти, способной быстро принимать решения о том, что следует предпринять. С другой стороны, нет и тех, кого можно было бы наказать за неправильное использование системы. В действительности в системе просто не существовало никаких подходящих случаев мер защиты клиентов. Это был *новый рубеж*, на что указывало и само название программного обеспечения (*Frontier*), используемого в тот момент в среде Эфириума.

После нескольких недель обсуждения проблемы сообщество Эфириума решило прекратить деятельность "The DAO" и создать новый вариант Эфириум-блокчейна. Этот процесс называют *хардфорк* (hard forking), когда изменения вносятся в цепочку блоков блокчейна, а не в само программное обеспечение. В результате осуществления в сети Эфириума хардфорка все выполненные хакерами транзакции были отменены. Следствием этого действия также стало разделение блокчейна Эфириума на две версии: просто Эфириум и Эфириум Классик.

Не все были согласны с принятым решением. Это сообщество продолжает и в настоящее время использовать блокчейн Эфириум Классик (Ethereum Classic). Токены сети Эфириум Классик по-прежнему находятся в обращении, но утратили большую часть своей рыночной стоимости. А рыночная стоимость токенов *нового* блокчейна Эфириума смогла превысить уровень, существовавший до момента атаки, лишь весной 2017 года.

Решение провести хардфорк потрясло мир блокчейна. Это был первый случай, когда большинство участников блокчейн-проекта осуществило изменение существующей цепочки блоков с целью возвращения похищенных средств инвесторам. Такое решение поставило под сомнение многие из принципов, которые, в первую очередь, делали технологию блокчейна столь привлекательной.

Взлом блокчейна

Блокчейн Эфириума никогда не был взломан. Хардфорк (перезапись) его блокчейна в 2016 году вследствие атаки на компанию “The DAO”, о которой подробно рассказывается во врезке “С большой силой приходят... большие возможности”, в действительности не являлся следствием *взлома* системы, хотя на этот факт часто ошибочно ссылаются именно как на взлом. Система Эфириума работает безупречно. Проблема состояла в том, что она работала слишком уж безупречно. В результате возникла необходимость перезапустить систему, когда в ней было украдено большое количество денег у большого числа ее пользователей.

Единственный способ исправить подобные нарушения в блокчейне, подобном Эфириуму, — это осуществить хардфорк (*hard fork*), который позволяет внести фундаментальные изменения в записи протокола работы системы. В результате хардфорка ранее валидные (действительные) в системе блоки и транзакции становятся недействительными. В системе Эфириума это было сделано для защиты фондов, которые были выведены неким пользователем из фондов компании “The DAO”. Ограбление этой компании концептуально является одним из крупнейших примеров извлечения выгоды из ошибок в программе.

Тем не менее в мире криптовалют действительно имело место множество жульничеств и попыток взлома. Большая часть этих атак была направлена на централизованные объекты — валютные биржи и другие сетевые приложения. Множество хакеров мечтает о краже криптовалюты, ведь она имеет реальную ценность и не так защищена, как обычные деньги, защищаемые правительствами. Анонимная природа криптовалют также делает ее привлекательной для мошенников всех видов. Поимка и наказание этих индивидуумов является трудной задачей. В ответ криптовалютное сообщество оказывает необходимое сопротивление и создает новые линии обороны для своей защиты.



ЗАПОМНИ!

Взломать одну точку несравненно проще и дешевле, чем попытаться преодолеть сопротивление децентрализованной сети. Если вам когда-либо попадутся сообщения о взломе в мире блокчейна, то, скорее всего, речь будет идти о конкретном веб-сайте или криптовалютном кошельке, который был атакован хакерами, но едва ли об атаке на всю сеть.

Познакомимся ближе со смарт-контрактами

Смарт-контракты в среде Эфириума схожи с обычными договорными соглашениями за исключением того, что не существует центральной стороны, обеспечивающей их выполнение. Протокол Эфириума “принуждает” к

выполнению смарт-контрактов, оказывая экономическое давление. Также гарантируется соблюдение всех требований, если они были указаны в блокчейне Эфириума, поскольку эта система может проверять, были ли соблюдены определенные условия. Если некоторое условие не зафиксировано в Эфириуме, гарантировать его соблюдение будет намного труднее.



ВНИМАНИЕ!

Смарт-контракты в Эфириуме пока еще не имеют юридической поддержки и, возможно, никогда не будут ее иметь по очевидной причине: вам просто не потребуются внешние органы, обеспечивающие соблюдение соглашений. Все юридические системы контролируются правительствами. На сегодняшний день именно правительства являются центральной властью — с большей или меньшей долей общественного согласия и демократических принципов. В смарт-контрактах Эфириума каждый участник имеет неотъемлемый голос.

Смарт-контракты Эфириума не предусматривают использования инструментов искусственного интеллекта. Реализацию этой исключительной возможности можно ожидать в ближайшем будущем. Но на данный момент Эфириум — это просто программное обеспечение, функционирующее на основе блокчейна.

Смарт-контракты Эфириума нельзя считать абсолютно безопасными. Атака на компанию “The DAO” — хороший пример тех угроз, которые могут иметь место в будущем. Эта технология пока еще лишь на начальном этапе своего развития, поэтому вкладывание слишком больших сумм в неотработанную до конца систему нельзя считать разумным решением. Лучше пока экспериментировать с небольшими вкладами, ожидая времени, когда все ошибки и недостатки будут выявлены и исключены из новых контрактов.

Знакомьтесь: криптовалюта “эфир”

“Эфир” — это название криптовалюты, используемой в блокчейне системы Эфириум. В прошлые века с этим названием связывали субстанцию, которая, как предполагалось, пронизывает все пространство, что делало возможным существование Вселенной. В этом смысле криптовалюта “эфир” действительно является той субстанцией, которая делает возможным существование всей системы Эфириум. Криптовалюта “эфир” стимулирует сеть защищать саму себя посредством ее майнинга с использованием протокола “proof-of-work” — доказательства выполнения работы точно так же, как майнинг биткойна стимулирует защиту сети Биткойна. Криптовалюта “эфир” необходима для выполнения любых программ в сети Эфириум. Когда она используется для выполнения контрактов в системе Эфириума, на валюту “эфир” ссылаются как на “газ” (*gas*).

Выполнение программного кода в смарт-контрактах также обходится в некоторое количество эфиров. Эта функция придает токenu дополнительную утилитарность. До тех пор, пока люди будут стремиться использовать систему Эфириум для размещения приложений и контрактов, эфир будет обладать определенной ценностью, не зависящей от спекуляций на бирже.

Взрывной рост денежного эквивалента эфира, наблюдаемый в последнее время, делает его популярным токеном для спекуляции. Он широко продается и покупается на различных биржах по всему миру. Некоторые новые хедж-фонды смотрят на эфир как на средство инвестирования. Тем не менее волатильная природа и низкая глубина рынка делают криптовалюту “эфир” рискованным вложением капитала.

Подключаемся и начинаем работать в Эфириуме

В этом разделе рассказывается, как получить доступ и начать работать в экосистеме Эфириума. Но прежде чем хоть что-нибудь создать в этой среде, необходимо завести эфириум-кошелек.



ЗАПОМНИ

В вашем кошельке будут храниться токены системы Эфириум, которые носят название *эфир* (ether). Эфир — это криптовалюта, которая потребуется вам для создания смарт-контрактов в блокчейне Эфириума. В последнем случае на них также могут ссылаться как на *gas*.

Чтобы загрузить эфириум-кошелек, потребуется определенное время, но соответствующий интерфейс интуитивно понятен, а предоставляемые по ходу процесса инструкции очень просты в выполнении.



СОВЕТ

В эфириум-кошельке вы можете выиграть тестовый эфир, что позволит вам создать тестовые контракты и организации. В этом случае вам не потребуется майнить или покупать реальные эфиры, чтобы изучить, как все здесь работает.

Майнинг эфиров

Блокчейн системы Эфириум поддерживается работой сети компьютеров, расположенных по всему миру, на которых выполняются обработка контрактов и защита сети. На эти компьютеры обычно ссылаются как на *узлы* (node) и на них осуществляется майнинг криптовалюты “эфир”.

Для лиц, обеспечивающих работу узлов, за потраченное ими время и издержки, связанные с майнингом эфира, протокол системы предусматривает вознаграждение в пять эфиров, которое выдается каждые 12 секунд. Приз выдается тому узлу, которому удалось создать последний блок, помещенный в блокчейн Эфириума.

Все новые блоки содержат список последних транзакций, выполненных в сети. Консенсус по протоколу доказательства выполнения работы (“proof-of-work”) гарантирует, что этот приз чаще будут получать те узлы, которые обладают большей вычислительной мощностью. Компьютеры меньшей мощности также могут выиграть приз, но на это потребуется больше времени. Если вы хотите попробовать свои силы в майнинге эфира, можете сделать это даже на своем домашнем компьютере, но учтите, что в этом случае для достижения успеха в майнинге блока и получения награды может потребоваться очень много времени.



ВНИМАНИЕ!

Майнинг эфира — это не самое подходящее занятие для тех, кто не имеет необходимой технической подготовки. Как минимум вам потребуется уметь работать в командной строке. Если вы не имеете представления, что такое командная строка, вам, вероятно, лучше отказаться от участия в этом процессе. В любом случае предварительно обязательно ознакомьтесь с текущими инструкциями по майнингу в сети Эфириума на сайте Ethereum GitHub (<http://github.com/ethereum>).

Получаем эфириум-кошелек

Чтобы установить и настроить собственный эфириум-кошелек, выполните следующие действия.

1. **Зайдите на сайт <http://www.ethereum.org>.**
2. **Прокрутите открывшуюся страницу и щелкните на кнопке Download (Загрузить).**

Эта кнопка находится на странице немного ниже ее начального экрана. Перед загрузкой вам потребуется подтвердить свое согласие с предупреждениями о личной ответственности и безопасности.



СОВЕТ

Убедитесь, что при загрузке эфириум-кошелька его файл будет записан на вашем компьютере в таком месте, где впоследствии вы сможете легко его найти.

3. **Распакуйте загруженный файл-архив и запустите на выполнение программу `Mist.exe`.**

4. В открывшемся окне щелкните на ссылке Use Test Network (Использовать тестовую сеть).

На этом этапе вам потребуется некоторая подготовка к майнингу первого тестового эфира. Эта процедура проще и займет меньше времени, чем настройка реального майнинга криптовалюты, но все же ее необходимо пройти.

5. Придумайте себе надежный пароль.

Не забудьте сохранить свой пароль где-нибудь в надежном месте.

6. Пройдите процедуру загрузки тестовой сети, последовательно щелкая на кнопке Next. В последнем окне щелкните на кнопке LAUNCH APPLICATION! (Запустить приложение).

Процедура загрузки сопровождается выводом серии окон, в которых вам будет предложено ознакомиться с тестовыми материалами по различным темам, связанным с возможностями системы Эфириум. В целом загрузка потребует от пятнадцати минут и более.

7. Когда загрузка завершится, закройте окно программы и вновь запустите приложение Mist.exe.

8. В окне приложения Mist откройте меню Develop (Разработка) и установите в нем флажок Start Mining (Начать майнинг).

Хотя на успешный майнинг тестовых эфиров может потребоваться немало времени, ни в коем случае не пропускайте этот этап. Вам необходимо иметь хотя бы один эфир для создания последующих проектов.

Поздравляю! Вы только что создали и настроили собственный эфириум-кошелек и заработали свой первый тестовый эфир, который вам потребуется для изучения последующих разделов этой главы.

Создаем свою первую децентрализованную автономную организацию

В будущем децентрализованные автономные организации по всему миру полностью изменят правила, по которым ведутся дела. Этот тип приложений позволяет кому угодно в любом уголке планеты создать в Сети компанию нового типа, которая будет управляться по предварительно согласованным правилам, выполнение которых впоследствии обеспечивается через сеть блокчейна. Создать такую организацию проще, чем вы думаете. В этом разделе вы узнаете, как создать свою первую тестовую организацию такого типа. В этой процедуре имеется три аспекта: создание, взаимодействие, управление.



ЗАПОМНИ!

Для успешного создания собственной тестовой децентрализованной организации предварительно необходимо создать эфириум-кошелек и запустить майнинг в тестовой сети, чтобы заработать некоторое количество тестовых эфиров (читайте предыдущий раздел).

Для создания собственной децентрализованной организации выполните следующее.

1. Зайдите на сайт <http://www.ethereum.org/dao>.
2. Прокрутите открывшуюся страницу до раздела The Code (Код) и скопируйте в буфер обмена представленный там программный код (рис. 5.3).
3. Откройте эфириум-кошелек (приложение Mist), который был создан вами ранее.

Процедура создания децентрализованной организации выполняется в окне эфириум-кошелька.

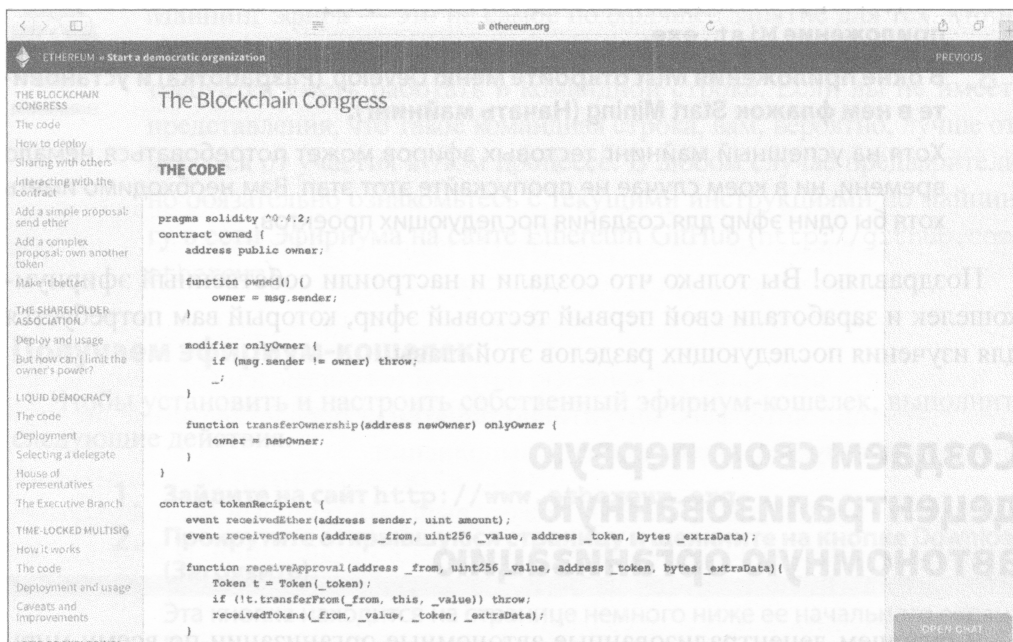


Рис. 5.3. Раздел The Code на странице сайта Ethereum

Тестовая сеть и обсуждение

Следующим этапом вашего проекта децентрализованной организации является настройка программной среды для его выполнения.

1. В окне эфириум-кошелька выберите команду меню Develop⇒Network⇒Test Net (Разработка⇒Сеть⇒Тестовая сеть).
2. Щелкните на вкладке Contracts (Контракты), а затем на ссылке Deploy Contract (Развернуть контракт).

Команда разработчиков Эфириума подготовила для начинающих несколько тестовых шаблонов для создания децентрализованных организаций.

3. Вставьте скопированный вами в предыдущем разделе программный код в область ввода Solidity.

Solidity — это название встроенного в блокчейн Эфириума языка сценариев, подобного языку JavaScript.

4. В списке Contract Picker (Выбор контракта) выберите вариант Congress.
5. Укажите значения некоторых переменных, когда вам будет предложено это сделать.

Вот возможные варианты:

- переменная *minimum quorum* (минимальный кворум) определяет для предложения количество голосов, которое оно должно получить, прежде чем будет принято;
- переменная *minutes for debate* (минуты на дебаты) задает минимальное количество времени (в минутах), которое должно пройти, прежде чем начнется выполнение;
- переменная *margin of votes* (порог голосов) количественно определяет понятие большинства при голосовании. Предложение проходит, если за него подано более 50% голосов плюс значение, указанное в этой переменной. Значение 0 означает простое большинство.

Управление и голосование

Теперь необходимо присвоить имя и определить процедуру управления вашей организацией. Необходимо задать значение переменной *minimum quorum* для предложений (сколько голосов должно получить новое предложение, прежде чем оно будет принято). Также следует определить значения переменной *margin of votes for a majority* (Сколько голосов должен получить план, прежде чем будет принят) и указать время, выделяемое на обсуждение новых планов.

1. Присвойте своей новой организации имя.
Это примерно то же самое, что дать название новой компании.
2. Для параметра Debate Times (Время дебатов) укажите значение 5 минут.
Оно определяет, как долго новое предложение будет открыто для обсуждения.
3. Оставьте значение параметра Margin of Votes for Majority (Порог голосов для большинства) равным 0.

Эта переменная определяет степень демократичности в работе организации.

4. Подтвердите стоимость своей новой организации.

У вас в кошельке уже должны быть (тестовые) эфиры, намайненные при его создании. Если, создавая кошелек, вы пропустили этот этап, вернитесь к нему сейчас. Вам потребуется совсем немного эфиров тестовой сети, чтобы создать свою децентрализованную автономную организацию.

5. Щелкните на кнопке Deploy (Развернуть) и введите свой пароль.

На развертывание новой организации может потребоваться некоторое время. Когда откроется панель управления новой организацией, прокрутите страницу вниз, где показан процесс ее формирования.

6. Щелкните на пиктограмме New (Новая) в правом верхнем углу страницы.

В результате будет сгенерирована новая уникальная пиктограмма, которая будет представлять вашу децентрализованную автономную организацию.

Поздравляю! Вы только что создали свою первую децентрализованную организацию (DAO).

Поговорим о будущем децентрализованных организаций

Концепции смарт-контрактов и децентрализованных организаций весьма многообещающи. Их исключительная демократичность и сверхрациональная природа весьма притягательны. Однако на данный момент в этой области больше потенциальных возможностей, чем реально опробованных решений. Поэтому каждый создаваемый контракт может оказаться как новаторским прорывом, так и грандиозным жульничеством или полным фиаско.

Если подходить к системе Эфириум как к новым рубежам в общественных отношениях, чем она, по сути, и является, то результаты будут более благоприятными. Сеть Эфириума имеет больше преимуществ, чем недостатков, если подходить к ней с необходимой осторожностью. Если ожидать, что все будет работать безупречно, а все участники проявят исключительную честность, то вас ждут большие потери и сильные разочарования. В Эфириуме есть своя часть потенциальных преступников, но найдутся и те, кто с искренним дружелюбием и энтузиазмом захотят, чтобы вы преуспели.

Атака на смарт-контракт в 2016 году высветила огромную важность обеспечения защищенности и тщательного предварительного анализа заключаемых контрактов. Она также продемонстрировала, что есть и такие, кто с честью борется за исправление любых возникающих проблем.

Изучение этой книги — только первый шаг; она лишь предоставит вам надежную базу для последующего углубления своих знаний об Эфириуме.

Но, как и в случае других новых технологий, система Эфириума очень быстро эволюционирует. Поэтому наилучшая практика — постоянно следить за появляющимися новыми решениями и развитием методов защиты.

В следующем разделе обсуждается несколько важных моментов, о которых не следует забывать в процессе создания новых децентрализованных организаций (DAO) и смарт-контрактов и отладки новых блокчейн-систем.

Вкладываем деньги в DAO

Не вкладывайте большие суммы в непротестированные контракты или контракты, которые не были достаточно проверены на надежность. Помните, что крупные контракты гораздо чаще становятся целью хакерских атак. Атака на “The DAO”, о которой рассказывалось во врезке “С большой силой приходят... большие возможности”) выше в этой главе, показала, что даже хорошо продуманные контракты могут иметь слабые места, остававшиеся незамеченными ранее.



ЗАПОМНИ!

Хотя смарт-контракты и блокчейн-технология позволяют вести дела с кем угодно по всей планете, учтите, что все здесь пока лишь у своей отправной точки. Можно снизить риски, работая в новой среде лишь с известными вам и доверенными партнерами.



СОВЕТ

Уровень защищенности в системе постоянно возрастает за счет выявления очередных ошибок. Всегда держаться в курсе событий — вот наилучшая практика для вас. Контролируйте суммы денег, вкладываемые в рискованные предприятия, и разворачивайте контракты без спешки и поэтапно. Эфириум — это новая технология, и зрелые решения в ней пока еще отсутствуют.

Создаем более “умные” смарт-контракты

Программирование смарт-контрактов требует совсем иных знаний и умений, чем написание обычного контракта. Здесь у вас не будет третьей стороны, которая будет следить, чтобы в конечном счете все было правильно, если на практике контракт будет реализован не совсем так, как вы планировали и ожидали. Неизменная и распределенная природа блокчейна делает чрезвычайно сложной задачу изменения нежелательного результата.



ЗАПОМНИ!

Любой ваш контракт будет иметь недостатки и может потерпеть неудачу. Старайтесь заранее расставлять в своих контрактах предохранительные клапаны, которые позволят вам предпринять необходимые ответные действия в случае обнаружения в них ошибки или

уязвимости. Смарт-контракт также должен иметь некий “выключатель”, который позволит вам “вытащить вилку из розетки” и приостановить его работу, если что-то пойдет не так, как предполагалось.



СОВЕТ

Если ваш контракт достаточно крупный, предложите всем желающим вознаграждение за найденные в нем ошибки, что будет способствовать привлечению членов сообщества к поиску уязвимостей и изъянов в вашем контракте.

Как и во многих других случаях, повышение сложности контракта всегда повышает вероятность наличия в нем ошибок и потенциальных возможностей для атаки. Стройте свои контракты логически простыми. Разрабатывайте небольшие модули, каждый из которых будет содержать один из разделов контракта. Создание контракта по такой схеме поможет вам разделить всю процедуру на отдельные этапы, простые и логически завершенные.

Ищем информацию об ошибках в системе

Не изобретайте колеса, создавая собственные варианты общеизвестных инструментов, таких, например, как генератор случайных чисел. Вместо этого пользуйтесь результатами тех работ, которые сообщество уже выполнило и которые были хорошо протестированы.



ВНИМАНИЕ!

Вы можете полностью контролировать только то, что присутствует в теле вашего контракта. Будьте осторожны с привлечением в выполняемые процедуры внешних контрактов. В них может присутствовать вредоносный код, который позволит злоумышленникам блокировать ваш контроль над происходящим.

Сообщество Эфириума ведет широко известный список обнаруженных ошибок и еще более полезную подборку советов по созданию защищенных смарт-контрактов. Они доступны на страницах сайта GitHub по адресу <https://github.com/ethereum/wiki/wiki/safety>.



Глава 6

Поговорим о блокчейне Ripple

В ЭТОЙ ГЛАВЕ...

- » Выясняем, откуда система Ripple берет свое начало
- » Знакомимся с особенностями блокчейна Ripple
- » Учимся использовать сеть Ripple

Ripple (Рипл) — это одна из самых интересных блокчейн-систем для перемещения и торговли ценностью в глобальном масштабе. Протокол Ripple допускает взаимозаменяемость активов любого типа — даже для двух несхожих активов и на неликвидных рынках. При этом все это делается по чрезвычайно низкой цене, с исключительно высокой степенью защищенности и в рекордное время. Инфраструктура системы Ripple была реализована как рабочая площадка для новых методов торговли и предоставления банковских услуг.

В этой главе обсуждаются важные особенности технологии, положенной в основу построения блокчейна Ripple, и тонкие детали того, как Ripple революционизирует банковское дело и вообще все, что связано с финансами в глобальном масштабе. Также здесь будут рассмотрены практические аспекты использования блокчейна Ripple и предоставлены конкретные советы по безопасной работе при использовании протокола Ripple.

Эта глава подготовит вас к ведению торговых операций ценностью множеством способов и в глобальном масштабе. Вы поймете, почему эта технология так важна для вашего бизнеса и как можно начать использовать ее прямо сегодня. Вы узнаете, как создать учетную запись для ведения торговых операций по протоколу Ripple и как защититься от мошенничества, работая в этой экосистеме.



СОВЕТ

Если вы не нуждаетесь в масштабных решениях на корпоративном уровне с целью освобождения от налогов или пошлин либо получения банковской лицензии, то можете пропустить эту главу, поскольку система Ripple предназначена, прежде всего, для обслуживания различных финансовых институтов.

Краткая история блокчейна Ripple

Проект Ripple старше Биткойна. В своем развитии он прошел несколько этапов, но исходная его реализация была создана канадским разработчиком Райаном Фэггером (Ryan Fugger) еще в 2004 году. Тогда он создал децентрализованную монетарную систему, которая позволяла отдельным людям или сообществам создавать собственные деньги.

Позднее к работе Райана подключились Джед Мак-Калейб (Jed McCaleb), Артур Бритто (Arthur Britto) и Дэвид Шварц (David Schwartz), создав компанию, получившую название “OpenCoin”. Их работа помогла добавить в проект больше особенностей, подобных функциям блокчейна, таких как система цифровой валюты, в которой цепь транзакций формировалась на базе консенсуса среди членов сети.

Крис Ларсен (Chris Larsen), первый руководитель высшего звена в команде Ripple, был основателем нескольких компаний, включая E-Loan и Prosper (деструктивные организации, изменившие рынок потребительского кредитования). Он присоединился к проекту Ripple в августе 2012 года и возглавлял его команду до 2016 года.

К тому времени проект Ripple вырос до крупного венчурного стартапа. В мире инвестиций он вошел в число крупнейших игроков, из числа которых можно также назвать Google Ventures и Andreessen Horowitz. По состоянию на 2016 год проект Ripple в венчурном фондировании вырос до уровня более 93 миллионов долларов. Компания Ripple также проявляет активность на политической сцене, являясь членом руководящего комитета целевой группы по ускоренным платежам Федерального резерва, а также сопредседателем рабочей группы по веб-платежам комитета W3C. Компании имеет свои офисы в Сан-Франциско, Нью-Йорке, Лондоне, Люксембурге и Сиднее. Многие из команды учредителей уже покинули Ripple и начали новые проекты.

В банковской индустрии деятельность компании Ripple была весьма разрушительной, нарушающей все существующие каноны, и на этом поприще она достигла немалых результатов. В 2015 году американская Комиссия по расследованию финансовых преступлений (FinCEN) оштрафовала Ripple на 700 тысяч долларов за нарушение Закона о секретности. Штраф был наложен за продажу токенов Ripple (криптовалюты XRP) Роджеру Веру (Roger Ver), широко известному инвестору Биткойна, без предоставления отчета о подозрительных действиях, поскольку Вер был признан виновным в продаже фейерверков на eBay. После наложения штрафа банк DBS и корпорация Oversea-Chinese Banking отказали в банковских услугах отделению Ripple в Сингапуре. Как предполагается, это произошло по той причине, что указанные банки пришли к заключению, что выдача активов в блокчейн приносит больше проблем с регулирующими органами, чем дает какой-либо выгоды. С этого момента Ripple перевел фокус своих интересов, прежде всего, на обслуживание глобальных и региональных банков.

Сегодня Ripple представляет собой глобальную финансовую структуру, которая позволяет банкам и их клиентам обмениваться ценностью. Как и в Биткойне, в протоколе Ripple существенно снижена общая стоимость расчетов, что позволяет клиентам осуществлять транзакции прямо и мгновенно. Система Ripple построена на распределенном интернет-протоколе с открытым кодом, использует блокчейн и имеет собственную криптовалюту, получившую название *ripples* (или XRP).

Распределенная финансовая технология Ripple предоставляет пользователям возможность проводить международные платежи в реальном времени непосредственно через ее сеть. Воспользовавшись системой Ripple, глобальные рынки смогут, наконец, удовлетворить свои требования к системе проведения платежей в отношении скорости ее работы, низкой стоимости транзакций и постоянной доступности в любой день и в любое время суток.

Система Ripple особенно хороша в отношении проведения платежей за границу и обмена различных видов ценности. В системе Ripple создана глобальная сеть финансовых институтов, маркет-мейкеров и клиентов. Теперь стало возможным мгновенно обменивать практически любые типы ценности в любой точке в мире. Система Ripple — это новый фундамент для *Интернета ценности* (Internet of Value). Идея, положенная в основу понятия “Интернет ценности”, заключается в том, что любые ценности, такие как деньги, машины, земля или товары, теперь могут быть представлены и использоваться в торговых сделках исключительно в Сети, без каких-либо промежуточных элементов или структур, обеспечивающих процесс. Сами протоколы, такие как протокол Ripple, обеспечивают теперь торговые операции и выполняют роль любых промежуточных структур.

Ripple: здесь все вертится вокруг доверия

Система Ripple представляет собой платформу для обмена валюты и торговых операций, построенную на основе использования блокчейна. Финансовые учреждения используют ее протокол для проведения транзакций посредством их записи в распределенный реестр Ripple. Также здесь есть возможность погашать обязательства через распределенную фондовую биржу Ripple.

В сети Ripple имеется два основных способа взаимодействия.

- » Финансисты, пользователи системы, участвуют в работе ее сети, выпуская, принимая и осуществляя торговлю активами для проведения платежей.
- » Операторы узлов участвуют в работе сети, отслеживая транзакции и приходя к консенсусу с другими узлами в сети в отношении их валидности и упорядоченности.



СОВЕТ

Термины *узел* и *компьютер* часто используют как взаимозаменяемые. В обоих случаях предполагается ссылка на вычислительное устройство и работающую на нем программу, используемую для поддержки работы сети.

Участники-финансисты должны доверять эмитентам тех активов, которые они хранят, а операторы узлов должны доверять другим узлам в своих списках доверенных узлов в том смысле, что он не сговорится между собой, чтобы заблокировать подтверждение действительных транзакций. Здесь все построено на доверии и согласованных стимулах поддерживать сотрудничество.

В системе Ripple был найден надежный способ обмена всевозможными типами ценности в ее распределенной сети. Криптовалюта системы Ripple, XRP, используется для торговли между несхожими видами ценности с низким объемом торгов или при отсутствии доверенных каналов. Между узлами, сетью и финансовыми участниками в системе Ripple была построена базовая инфраструктура, оптимизирующая существующие процедуры проведения платежей и обмена валюты в глобальном масштабе.

В этом разделе вам будут представлены основные функции, которые протокол Ripple предоставляет для банковской индустрии.

В сети Ripple обеспечиваются две критически важные функции.

- » **Она действует как общий реестр для соединения банков и платежных сетей.** Это позволяет банкам и платежным сетям проводить транзакции за пять секунд. Это также обеспечивает пользователям

постоянное соединение друг стругом, поддерживая непрерывный мониторинг потока транзакций по всей сети.

- » **Она действует как нейтральный протокол транзакций.** В системе Ripple стоимость передается на двухсторонней основе для одного и того же типа ценности. Для транзакций с различными валютами в Ripple используются источники финансирования из собственного рынка поставщиков ликвидности. Это очень важная особенность, поскольку ликвидность является главной проблемой для множества рынков.

Банки высоко оценили эту технологию, поскольку она позволяет им перейти от посредников и расчетных палат к быстрому, дешевому и менее рискованному варианту ведения дел. Банки смогли невероятно ускорить процедуру проведения платежей за границу за счет устранения необходимости в оформлении бумаг и использовании посредников.

Система Ripple также помогла банкам сократить риски и снизить операционные расходы в операциях обмена валюты, позволив им непосредственно взаимодействовать с другими банками по всему миру и предоставляя источники ликвидности из собственного открытого рынка маркет-мейкеров.

Основные преимущества, предлагаемые системой Ripple, можно кратко описать следующим образом.

- » Платежи в реальном времени
- » Полная отслеживаемость транзакций
- » Почти мгновенная сверка
- » Возможность конвертирования практически любого типа валюты, собственности или токенов

Чем система Ripple отличается от других блокчейнов

В Ripple, как и в Биткойне, используется нейтральное и децентрализованное программное обеспечение. Практически кто угодно может использовать систему Ripple как открытый стандарт для упрощения поиска контактов и взаимодействия.

Система Ripple существенно отличается от Биткойна по своей структуре и способу организации работы сети. Система Ripple находит наиболее эффективный вариант обмена, структурирует транзакции как задолженности и

использует собственную криптовалюту как механизм обмена между различными видами ценности, торговля которыми осуществляется в ее сети.

В системе Ripple все построено на доверии — в отличие от других блокчейнов, которые по большей части являются системами, где доверительные отношения практически отсутствуют. Так, в системе Биткойна любые две стороны могут отправить друг другу токены, а затем сеть проверит, действительно ли в этой транзакции ни одна из сторон не обманывает другую. Частью задачи, которая в системе Биткойна решается при записи в блокчейн очередного блока транзакций, является требование удостовериться, что каждый упоминаемый в этих транзакциях токен был потрачен лишь однажды.

Другим существенным отличием системы Ripple является тот факт, что в ней не используется консенсус по правилу доказательства выполнения работы (“proof-of-work”). Такой подход позволил команде Ripple избавиться от огромных затрат энергии, необходимых другим блокчейнам для защиты самих себя. В результате расход электроэнергии в сети Ripple оказался несравненно ниже, а скорость работы сети существенно выше, чем у традиционных блокчейнов. Больше узнать о принципах работы системы Ripple вы сможете в декларативном документе, который находится по адресу https://ripple.com/files/ripple_consensus_whitepaper.pdf. Из русскоязычных документов можно предложить веб-страницы https://ru.bitcoinwiki.org/wiki/Ripple?mobileaction=toggle_view_desktop и <https://ru.wikipedia.org/wiki/Ripple>.

Система Ripple работает совсем не так, как другие блокчейн-системы. Одно из наиболее примечательных отличий состоит в том, как в сети обеспечивается децентрализация и как в ней достигается консенсус. Подход к децентрализации в Ripple выбран очень тонкий. Любой узел по своему усмотрению может поместить любые другие узлы в свой список надежных узлов с целью отслеживания, какие транзакции эти узлы хотят подтвердить. Единственным требованием в таком подходе является обеспечение достаточного перекрытия списков проверки между всеми узлами, чтобы исключить возможность случайного перехода сети в состояние с несколькими разными консенсусами.

В системе Ripple эта ситуация контролируется за счет того, что, хотя каждый узел поддерживает собственный список проверки, он всегда включает в него определенные доверительные узлы системы Ripple. Этим и гарантируется достаточное перекрытие списков проверки. С ростом сети список доверительных узлов будет включать все больше и больше узлов от широко известных, достойных доверия и независимых учреждений по всему миру. В результате с течением времени процесс достижения консенсуса в сети Ripple будет становиться все более и более децентрализованным.

Помимо того как в системе Ripple обеспечиваются децентрализация и достижение консенсуса, есть еще несколько важных особенностей, отличающих Ripple от Биткойна.

- » **Система Ripple занимает промежуточный уровень.** Программное обеспечение системы Ripple функционирует как промежуточное звено между финансовыми инструментами и организациями. Если вы намерены использовать сеть Ripple, вам необходимо быть лицензированным поставщиком финансовых услуг либо оператором мобильных денежных сервисов.

Биткойн-протокол открыт для любого желающего использовать его именно так, причем так, как он считает нужным. Регулирующие нормативы могут меняться, но на текущий момент вам не нужна лицензия, чтобы использовать систему Биткойна.

Любой разработчик может получить и запустить на выполнение ПО системы Ripple, однако его использование может оказаться нелегальным, если у вас нет на это лицензии. Это одна из причин, по которым система Ripple ориентирована на крупные финансовые организации и их пользователей. В отличие от этого, в сети Биткойна может работать кто угодно и она удобна, прежде всего, для проведения небольших транзакций.

- » **Работа системы Ripple базируется на особом алгоритме консенсуса, а не на майнинге.** В ней используется вероятностное голосование между доверенными узлами. Этот тип консенсуса позволяет узлам прийти к соглашению и подтвердить блок транзакций в пределах пяти секунд. В системе Биткойна транзакции могут ожидать подтверждения часами.
- » **Все активы в системе Ripple, за исключением XRP (собственный токен Ripple), представлены как долговые обязательства.** В системе Биткойна, наоборот, присутствуют только аккаунты для передачи токенов Биткойна между биткойн-адресами, а ценность токена Биткойна определяется внешними рынками.
- » **Общий объем криптовалюты XRP установлен в пределах 100 000 000 000 и изменить его нельзя. Это количество токенов было создано в начале работы системы Ripple и принадлежало ей.** Затем токены XRP были распределены между владельцами компании и другими лицами.

В системе Биткойна новые токены создаются каждый раз, когда в ее блокчейн записывается новый блок. Новые токены являются наградой тем узлам, которые в процессе достижения консенсуса выиграли право создать новый блок. С течением времени количество токенов в этой сети постоянно возрастает. Протокол Биткойна построен

таким образом, что генерация новых токенов прекратится, когда их общее количество составит 21 миллион.

- » **Система Ripple защищает себя от спама и атак типа DOS (отказ в обслуживании) посредством взимания минимальной платы за транзакцию.** Стандартный сбор за транзакцию составляет 0,00001 XRP, т.е. 10 минимальных частей токена, называемых каплями (*drop*).

Протокол Ripple предусматривает увеличение размера взимаемых сборов за транзакцию, если наблюдается превышение нормального объема выполняемых транзакций. Это похоже на то, как система Биткойна защищает себя от спама, но в ней нет минимального сбора. Майнеры Биткойна, вероятно, просто проигнорируют ваши транзакции, и они не получают подтверждения в сети, за исключением одной.

- » **Для совершения операций с валютой XRP не требуется доверительный путь (trust path).** Благодаря этому становится возможным проведение финансовых операций, когда стороны не являются партнерами, доверяющими друг другу. В результате появляется возможность проводить торговые операции с ненадежными партнерами или рынками с низкой ликвидностью, включая в сделку как промежуточное звено перевод средств в валюту XRP.

С другой стороны, в системе Биткойна доверительные отношения отсутствуют изначально. Торговые операции в ней разрешены любым двум сторонам независимо от того, доверяют они друг другу или абсолютно не знакомы, но при этом торговать можно только токенами Биткойна. Что касается Ripple, то ее упомянутое выше замечательное качество позволяет клиентам заключать сделки по обмену практически чем угодно.

- » **В системе Ripple осуществляется отбор тех узлов, которые используются для защиты консенсусной системы в ее сети.** Эта система не является столь же открытой, как система Биткойна, в которой каждый может принимать полноправное участие в работе сети. А это означает, что система Ripple является в определенной степени централизованной, но с течением времени ее децентрализация постоянно возрастает.

Открываем для себя всю мощь системы Ripple

В системе Ripple уже прекращена практика открытия новых счетов клиентских кошельков на сайте Ripple Trade, портале работы с клиентами. Также по

большей части в системе Ripple уже свернули поддержку всех продуктов, предназначенных для работы с клиентами. Нагрузка, связанная с обслуживанием клиентов, оказалась слишком высокой, к тому же американская Комиссия по расследованию финансовых преступлений (FinCEN) постановила, что все участники на рынке виртуальных валют должны регистрироваться как поставщики финансовых услуг в полном соответствии с федеральным законодательством.

Выход за пределы возможностей портала работы с клиентами не помешал росту банковского сектора в сети Ripple. На настоящий момент Ripple фокусирует свои усилия на обслуживании крупных корпоративных клиентов. Банки — вот кто действительно нуждается в том, что система Ripple может предложить и в таком масштабе, который будет им выгоден.

В качестве клиента вы можете получить доступ к системе Ripple лишь через третью сторону. Поставщиком кошельков, с которыми Ripple может работать, является сайт GateHub.

В кошельке на сайте GateHub можно хранить свои активы в разных валютах. В сети Ripple прямо из своего кошелька вы сможете переводить средства, торговать золотом, серебром, криптовалютой XRP и биткойнами. В кошельке также можно следить за текущей сетевой стоимостью различных валют, учитывая колебания рынка.

На сайте GateHub вам, прежде всего, нужно будет идентифицировать себя, поэтому получение учетной записи потребует определенного времени. Когда учетная запись будет создана и активирована в сети, у вас появится возможность оценить всю мощь сети Ripple.

Для регистрации и начала работы на сайте GateHub выполните следующее.

1. **Зайдите на сайт <http://www.gatehub.net>.**
2. **Щелкните на кнопке Sign Up.**
Она находится в правом верхнем углу экрана.
3. **На открывшейся странице укажите адрес своей электронной почты и пароль, после чего щелкните на кнопке Sign Up (Зарегистрироваться).**
Обратите внимание: эта маленькая кнопка расположена под большой кнопкой SIGN IN (Войти); вам нужна именно маленькая.
4. **Сохраните предложенный вам ключ восстановления (recovery key) в надежном месте.**
5. **Проверьте свою почту. В полученном от GateHub письме щелкните на кнопке Activate account (Активировать аккаунт).**
6. **Заново войдите в систему и предоставьте необходимые данные для верификации.**

Для проведения идентификации вас могут попросить предоставить номер телефона, имя, фото и подтверждающие вашу личность документы.

После завершения идентификации вашей личности вновь созданная учетная запись будет активирована, и вам будет предоставлена возможность совершать торговые операции по протоколу Ripple. Например, вы сможете отправить на свой новый счет некоторые средства из своего биткойн-кошелька.

Чтобы создать что-нибудь свое в системе Ripple, вам необходимо быть программистом или хотя бы иметь контакт с одним из них. В системе Ripple к вашим услугам отличная документация и команда поддержки; это поможет вам увереннее приступить к данной работе.



ВНИМАНИЕ!

Система Ripple создана для быстрого перемещения денежных средств при малых накладных расходах. Эта область экономики строго регулируется законодательством. Система Ripple декларирует, что она предоставляет вам лишь свое программное обеспечение, которое позволяет решать упомянутые выше задачи. Все вопросы по выяснению и соблюдению действующих правил и законодательных норм возлагаются исключительно на вас.

Если вы еще не отказались от мысли создать собственный пользовательский проект в сети Ripple, вам будет предоставлена необходимая помощь. Наилучший способ начать такую работу — зайти на страницу для разработчиков проектов на сайте Ripple (<https://ripple.com/build/>). Если вы хотите ближе познакомиться с программным обеспечением самой сети Ripple, посетите соответствующую страницу на ее сайте GitHub: <https://github.com/ripple>.

Некоторые предупреждения относительно системы Ripple



ЗАПОМНИ!

Система Ripple, как и другие блокчейн-системы, работающие с криптовалютами, подвержена многим опасностям. Работая в мире криптовалют, всегда руководствуйтесь здравым смыслом и следуйте всем практическим рекомендациям в отношении обеспечения защиты, предложенным в этой книге. Этот мир — действительно новый “Дикий Запад”, полный возможностей и риска.



ВНИМАНИЕ!

Вот несколько возможных рисков, характерных только для системы Ripple.

- » **Неэтичные торговые операции.** Как говорилось выше, система Ripple была создана для перемещения ценностей по всему миру быстрее и дешевле, чем позволяет любая другая сеть. В структурах

Ripple присутствуют кластерные группы различных рынков. Эти рынки имеют доверенные узлы, совместно подтверждающие транзакции. Время от времени между этими группами возникают небольшие расхождения в ценах, и эти расхождения могут провоцировать незитичные торговые операции.

» **Манипулирование транзакциями.** Для сети Ripple, в частности, характерна склонность к операциям *арбитражной купли-продажи* (одновременной покупке и продаже активов на разных рынках с целью извлечения преимуществ от различия в ценах на один и тот же актив), поскольку она работает со многими валютами на множестве различных рынков, а достаточно опытный программист может манипулировать порядком выполнения транзакций. Вот две известные формы подобных манипуляций в Ripple.

- **Выгодное размещение транзакций арбитражной купли-продажи.** Извлечение преимуществ из различия в ценах между несколькими рынками прежде, чем реестр будет закрыт. Реестр закрывается каждые пять секунд, поэтому трейдеры могут применять специальные программы-боты для использования удобной ситуации на рынках. Эти программы-боты выпускают комбинацию совпадающих сделок, которые извлекают выгоду из небольшого дисбаланса между рынками, одновременно обеспечивая размещение этих транзакций на оптимальных позициях в реестре. Трейдеры извлекают выгоду, пользуясь различиями в ценах на рынках.

- **Опережение больших сделок.** Структура работы и задержки в протоколе достижения консенсуса системы Ripple подвергают сеть опасности нового типа опережения больших сделок. Это возможно из-за того, что каждый узел в сети рассылает транзакции другим доверенным узлам. На протяжении этого времени программы-боты могут мониторить все транзакции в поисках возможности вставить новую транзакцию перед большой сделкой.

Бот будет искать возможность скупить исходные предложения, выбранные для выполнения большого заказа, а затем перепродать их прежнему владельцу. Одновременно бот переставит транзакции в реестре таким образом, чтобы предпринятая манипуляция оказалась возможной. Конечным результатом всех этих действий будет то, что исходный владелец получит меньшую сумму за проведенную торговую операцию.

Узнать больше о подобных махинациях можно на веб-странице <http://availableimagination.com/exploiting-ripple-transaction-ordering-for-fun-and-profit/>.



СОВЕТ

В системе Ripple прилагают большие усилия для исключения попадания различных ботов и программ-эксплоитов в ее сеть. Программистам открыто предлагается зарабатывать деньги, отыскивая ошибки в протоколах, вылавливая эксплоиты и выявляя вредоносное программное обеспечение. Очень желательно, чтобы две упомянутые выше проблемы были устранены в ближайшее время.



Глава 7

Новый подход: блокчейн Factom

В ЭТОЙ ГЛАВЕ...

- » Создаем записи в блокчейне Factom
- » Разбираемся в структуре цепочки блокчейна
- » Выясняем, как в блокчейне обеспечивается подлинность
- » Знакомимся с блокчейном Factom в действии

Блокчейн Factom — это мощный инструмент, который поднимает блокчейн-технологию до отраслевого уровня. Он отличается от других открытых блокчейнов и обладает собственными уникальными свойствами, делающими эту систему просто идеальной для публикации потоков данных и построения защищенных систем. Система Factom опирается на собственную корпорацию, Factom, Inc., которая возглавляет ее разработку и создает инструменты и приложения, работающие поверх ее протокола.

Программное обеспечение блокчейна Factom встроено в систему, которая обуславливает подлинность, а затем обеспечивает ее защиту как для людей, так и для фактов, обстоятельств или имущества. Она, кроме того, обеспечивает интеграцию и связывание мостами с другими блокчейнами, что осуществляется на основе все той же блокчейн-технологии. Связи с другими блокчейнами

повышают защищенность системы Factom и в то же время позволяют этим блокчейнам взаимодействовать между собой.

В этой главе объясняется, как работает система Factom, обсуждаются ее уникальные свойства и предоставляются простые инструкции, которые помогут вам начать работать с этой системой. Прочитав эту главу, вы сможете разобраться во многих важнейших концепциях блокчейна Factom и в тех технологиях, которые были положены в его основу, а также понять, какие дополнительные преимущества эта система способна предоставить вашим собственным блокчейн-проектам.

Наверное, самое время упомянуть, что я, автор этой книги, была сооснователем, а сейчас являюсь директором по маркетингу в корпорации Factom, Inc. И хотя в этой книге я всегда стремилась сохранять максимальную объективность, сдерживать мой энтузиазм в отношении системы Factom мне, возможно, удавалось не всегда.

Вопрос доверия

Блокчейн-технология по самой своей сути позволяет различным сущностям кооперироваться и сотрудничать без необходимости доверять защищенности данных или бизнес-процессов друг друга. Исторически некий доверенный посредник или отраслевой консорциум обеспечивал необходимый уровень доверия, но это всегда было связано с высокими дополнительными расходами и просто смещало доверие с контрагентов на третью сторону. Блокчейн-технология переносит доверие с контрагентов на сеть из распределенных бесстрастных третьих сторон и делает это исключительно математическими методами.

Корпорация Factom, Inc. — это компания, которая на основе блокчейн-технологии создает программное обеспечение для открытой системы блокчейна Factom. Программы Factom, предназначенные для сохранения записей, обеспечивают исключительно высокий уровень защищенности посредством шифрования сохраняемых данных и включения в блокчейн системы Factom их криптографически уникального хеш-кода (можно сказать, “отпечатка пальца”), как показано на рис. 7.1. В качестве дополнительной меры по усилению защиты сети каждые 10 минут хеш-код *всего* блокчейна Factom записывается в несколько других открытых блокчейнов. Эта функция дополнительной защиты отличает систему Factom от большинства других открытых блокчейнов.

Концепция протокола системы была впервые представлена в основополагающем документе, опубликованном в 2014 году, и имела целью масштабирование возможностей системы Биткойна. Поскольку к тому времени различные децентрализованные приложения уже начали обеспечивать себе защиту,

используя исключительные возможности системы Биткойна, выяснилось, что ввод данных в этот блокчейн оказался делом непомерно дорогостоящим, а сама система Биткойна столкнулась с серьезными затруднениями, вызванными необходимостью обработки множества дополнительных транзакций. Говоря метафорически, невозможно поместить 10 фунтов данных в 5-фунтовый пакет Биткойна.



Рис. 7.1. Структура блокчейна системы Factom

Протокол системы Factom был разработан с целью снять ограничения по стоимости и объему данных, свойственные другим блокчейнам. Главная цель состояла в обеспечении защиты данных и систем. Именно по этой причине систему Factom часто характеризуют как *инструмент публикации*. Она предоставляет пользователю возможность записать данные в собственный реестр за очень небольшую плату. Объем помещаемых в запись данных ограничен на уровне 10 Кбайт, стоимость транзакции фиксирована и невелика, а объем выполняемых транзакций может быть существенно больше в сравнении с блокчейнами, использующими консенсус по правилу “proof-of-work”.

Важной для понимания концепцией является то, что блокчейн системы Factom строится на слоях и цепочках. Слои имеют отношение к тому, как данные структурируются. Чтобы получить криптографическое доказательство того, что любые хранимые данные были записаны в систему именно в среде Factom, используется дерево Меркла. Криптографическое доказательство, называемое *корнем хеш-дерева* (Merkle root — 32 случайных символа, которые представляют все хеш-дерево определенных данных), помещается в другой

открытый блокчейн, по структуре подобный блокчейну системы Эфириум. Это дополнительный уровень защиты, отсутствующий в других блокчейнах.



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

Дерево Меркла — это математическая древовидная структура, создаваемая посредством хеширования пар фрагментов данных, после чего полученные хеши вновь попарно хешируются, и так до тех пор, пока не будет получен единственный хеш всех исходных данных, называемый корнем хеш-дерева (Merkle root). Этот криптографический метод доказательства получил свое название от имени Ральфа Меркла, который предложил его в 1979 году.

Организация данных в виде цепочек способствует их масштабируемости. Цепочки позволяют приложениям извлекать из блокчейна Factom только ту информацию, которая им нужна, без необходимости загружать весь набор данных. Эта схема работает очень просто: вы можете записать свои данные в уже существующую в системе цепочку либо создать новую цепочку. Идентификатор выбранной вами цепочки далее будет использоваться в последующих вводимых записях данных, а также как средство отслеживания данных, представляющих для вас интерес.

Назначение блокчейна Factom: публикация чего угодно

Система Factom — это платформа для ввода и последующего надежного хранения информации. С самого начала она проектировалась как инструмент публикации и подтверждения юридической силы любых данных. Все прочие приложения в данной системе построены вокруг этой простой функциональности. Система Factom позволяет обрабатывать транзакции с размером записываемых данных до 10 Кбайт; более крупные объемы информации необходимо предварительно специальным образом структурировать и вводить в виде серии транзакций. В качестве альтернативы можно также опубликовать в системе хеш, представляющий определенные данные.

Поскольку протокол Factom является ПО с открытым кодом, система функционирует как открытая общедоступная площадка. Это то место, где каждый желающий может ввести любые данные, и блокчейн Factom обеспечит им необходимую защиту и гарантию неизменности. Не стоит удивляться тому, что некоторые пытались опубликовать здесь непристойный контент, однако лимит на объем вводимых за одну транзакцию данных не позволил им опубликовать слишком много. Попадание спама в систему сдерживается тем, что за каждый вводимый блок с пользователя взимается небольшая плата. Поэтому, если кому-то захочется записать в блокчейн что-то непристойное, это будет стоить ему денег.

Криптовалютой в сети системы Factom является *Factoid*, название которого сейчас чаще всего сокращают до “FCT”. В децентрализованной системе должен быть предусмотрен определенный механизм вознаграждения ее активных участников. Исходя из этого положения, закрытая система требует от активных участников кооперации в долгосрочном создании ценности в ее сети. Валюту FCT можно продавать и покупать, как и любую другую из более чем 700 криптовалют, присутствующих на этом рынке. В конечном счете именно FCT используется для приобретения кредита на ввод данных в сети Factom.

Стоимость процедуры записи в блокчейн фиксирована, тогда как стоимость криптовалюты FCT подвержена колебаниям. Когда стоимость FCT растет, пользователь просто может за один токен купить больше кредитов на ввод. Такой подход разделяет пользователей системы и рынок торговцев ее токенами, позволяя выдерживать фиксированный уровень цен для одних, не мешая при этом другим спекулировать FCT на свободных рынках. Подобная функциональность была встроена еще в исходный релиз ПО Factom с целью позволить строго регулируемым законодательством отраслям и правительственным организациям использовать блокчейн-технологии, не “пачкая руки” использованием токенов, торгуемых на свободных биржах.

На начало 2017 года в сети Factom ежедневно проводилось до 40 тысяч транзакций ввода данных. Среди них присутствовала такая информация, как показатели индекса Russell 3000 Index и запись сведений о ценах альткойнов на текущий день. Эти записи могут использоваться как справочник исторических данных, как входные данные для смарт-контрактов или же как доказательство исторических сведений.

Сегодня сохранение данных и доступ к ним везде и всюду в большинстве случаев — задача уже решенная. Резервные копии любых данных на компьютерах могут дублироваться и архивироваться в необходимых масштабах. Однако большой проблемой остается определение того, что документ после создания не подвергался какой-либо ревизии, особенно при обмене информацией между разными организациями. Если система управления документооборотом реализована на основе блокчейн-технологии, каждая организация будет иметь гарантию того, что она пользуется той же самой версией документа, что и ее партнеры.

Стимулы к объединению

Многие блокчейны, такие как Биткойн и Эфириум, используют консенсус по типу “proof-of-work”. В блокчейнах такого типа алгоритм консенсуса определяет, как в сети блокчейна достигается соглашение по поводу записи новых данных в систему. Цель достижения консенсуса — удостовериться, что новые

данные являются действительными, а не поддельными. Открытые блокчейны нуждаются в жесткой системе достижения консенсуса, поскольку кто угодно может добавлять новые данные в блокчейн. Их механизм консенсуса представляет собой набор правил, которые определяют, что именно делает блок данных действительным и чему сеть должна доверять.

Консенсус типа “proof-of-work” имеет много характеристик, которые делают его весьма притягательным. Однако его использование часто требует внушительных капиталовложений в специализированную компьютерную технику и значительных затрат электроэнергии (чем дешевле она будет, тем лучше). А это означает, что единственным условием для присоединения к блокчейн-системе как элемента ее управления является необходимость расходовать электроэнергию на подходящем случае компьютере. Это также означает, что для переписывания истории системы должно быть вновь потрачено эквивалентное количество электроэнергии. Связанные с этим затраты делают искажение исторических данных делом просто невыгодным, а значит, маловероятным.

Алгоритм типа “proof-of-work” обеспечивает превосходную защиту блокчейна. С другой стороны, он требует огромных затрат энергии и является весьма дорогостоящим в эксплуатации. Это каннибалистическая гонка вооружений, в которой выигрывает более быстродействующий компьютер, а каждый дополнительный гигахеш-манипулятор, добавленный в сеть, лишь увеличивает сложность работы.

Чем больше данных содержит каждый блок, тем сложнее удостовериться в его действительности. Системам с консенсусом типа “proof-of-work”, подобным Биткойну, также необходимо работать с полным блокчейном для проверки действительности любого отдельного элемента данных в системе. Для того чтобы внешние узлы в сети Биткойна могли подтвердить выполненную вами транзакцию, им необходимо загрузить на свои компьютеры биткойн-блокчейн во всем его объеме. На настоящий момент на это может потребоваться до нескольких дней.

В системе Factom отказались от поиска ответа на вопрос “Является ли введенный элемент данных действительным?” Вместо этого здесь выполняется проверка “Был ли введенный элемент данных оплачен?” Сами пользователи системы являются теми, кто осуществляет проверку действительности введенного элемента данных. В системе Factom данные также структурируются в виде подцепей, которые могут индивидуально сканироваться для подтверждения действительности любых вводимых данных без необходимости загружать весь блокчейн системы.

На рис. 7.2 представлена диаграмма, поясняющая особенности построения структуры цепочек системы Factom.

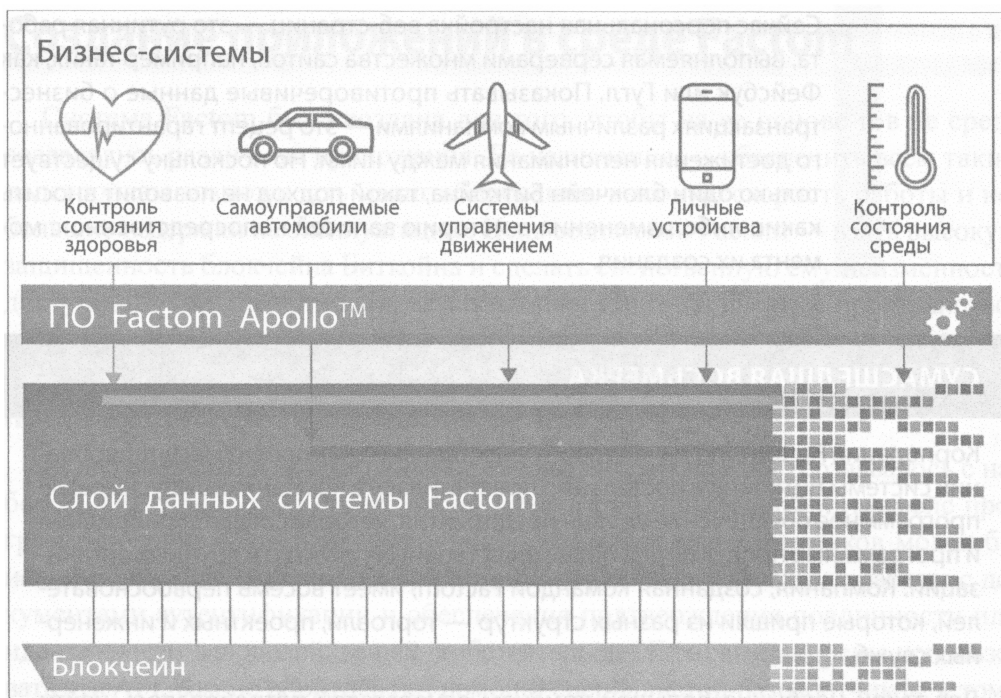


Рис. 7.2. Структура цепочек в системе Factom

Данные в блокчейне Factom были структурированы подобным образом специально для удобства реализации коммерческих приложений, поскольку членам одного отраслевого сообщества в этом случае не потребуется загружать и обрабатывать все прочие ненужные им данные от прочих сообществ. Например, чтобы убедиться, что все документы, связанные с займом, были приняты во внимание, не нужно будет также загружать сведения о колебании курса валют на бирже за многие годы.

Для защиты своей сети от разрушения данных блокчейн Factom также выводит некоторую информацию во внешний мир. Каждые несколько минут в системе создается небольшой якорный блок, записываемый в блокчейны Биткойна и Эфириума. Этим в системе достигаются две важные цели.

- » Первое и самое важное — этот подход предотвращает незаметное переписывание истории со стороны серверов, формирующих блокчейн системы Factom. Поскольку эти серверы не могут контролировать блокчейны Биткойна или Эфириума, любая запись, внесенная ими в блокчейн системы, навсегда останется неизменной.
- » Такой подход также не позволяет серверам системы Factom предоставлять разным пользователям различные версии ее блокчейна.

Сейчас персональная настройка веб-страниц — это рутинная работа, выполняемая серверами множества сайтов, например таких, как Фейсбук или Гугл. Показывать противоречивые данные о бизнес-транзакциях различным компаниями — это рецепт гарантированного достижения непонимания между ними. Но поскольку существует только один блокчейн Биткойна, такой подход не позволит вносить какие-либо изменения в историю записей непосредственно с момента их создания.

СУМАСШЕДШАЯ ВОСЬМЕРКА

Корпорация Factom, Inc. начала свое существование как проект масштабирования системы Биткойна и постепенно превратилась в компанию, выпускающую программное обеспечение уровня предприятия, которая создает приложения и программные продукты для правительственных структур и крупных организаций. Компания, созданная командой Factom, имеет восемь первооснователей, которые пришли из разных структур — торговли, проектных и инженерных служб.

Для такой необычно большой команды основателей потребовалось найти новый подход к управлению, распределению ответственности и капитала. Команда выбрала *холакратию* (holacracy), систему управления, очень напоминающую те децентрализованные сети, которые она намеревалась строить. Управленческие функции и право на принятие решений были распределены между менеджерами. Необходимый консенсус достигается еженедельно на общем собрании менеджеров продолжительностью 45 минут.

Штаб-квартира компании находится в городе Остин, штат Техас, при этом в ней реализуются глобальные проекты, включающие механизмы подтверждения подлинности, управления документооборотом, работы с недвижимостью и поддержку концепции Интернета вещей (Internet of Things — IoT). В каждом случае система Factom используется для записи информации и организации ее совместного использования. Корпорация поддерживает партнерские отношения с компанией Smarttrac, производителем радиочастотных идентификаторов (RFID) и различных решений для IoT, предназначенных для защиты документов о происхождении (документов, подобных свидетельству о рождении, на основании которых люди затем получают другие документы — идентификационные коды, водительские права и проч.) и о предотвращении кражи свидетельств подтверждения личности.

Создание приложений в среде Factom

Система Factom была создана для того, чтобы на ее основе и в ее среде создавались различные приложения. Ее назначение — обеспечить всем таким надстройкам возможность масштабирования, высокую скорость работы и небольшие издержки на эксплуатацию. Цель создателей Factom — взять высокую защищенность блокчейна Биткойна и сделать свойственную ему неизменность доступной в большей степени, чем позволяет его ограниченное пространство.

Аутентификация документов и обеспечение подлинности с использованием API

В системе Factom ее программное обеспечение изначально создавалось с набором API (*Application Programming Interface* — прикладной интерфейс программирования), которые команды программистов-разработчиков могли бы использовать для построения приложений, предназначенных для работы с документами аутентификации и обеспечения подтверждения подлинности или идентичности для людей, вещей и обстоятельств. Если вы намерены использовать эти API, вам не обойтись без помощи специалистов-разработчиков, к тому же они ориентированы на создание приложений масштаба предприятия, что нельзя считать идеальным в случае относительно небольших проектов.

Для широкой публики Factom предлагает два решения.

- » **Apollo.** Продукт Apollo представляет собой решение для публикации и аутентификации документов, позволяющее вводить в блокчейн системы Factom большие объемы данных, а затем ссылаться на них при необходимости получения исторических подтверждений. Например, это решение может быть идеальным вариантом для фиксации в блокчейне архивных данных с ваших веб-сайтов или обновлений используемых вами протоколов.
- » **Iris.** Продукт Iris является платформой для создания свидетельств идентичности или подлинности. На ее основе был развернут проект соответствующей поддержки Интернета вещей, осуществляемый Департаментом внутренней безопасности. Для записи и управления данными в нем также используется платформа Apollo.

Вы можете использовать эти API без необходимости создавать собственный блокчейн или использовать криптовалютные кошельки. Они существенно упрощают процессы разработки и являются идеальным вариантом для тех, кто стремится избежать какой-либо активности в “серой” (с точки зрения властей) зоне, в которую все еще попадает любая криптовалюта.

Знакомимся с криптовалютой Factoid: необычный токен

Система Factom использует совершенно уникальный по своим свойствам токен ценности, получивший название *Factoid* (или FCT). Это цифровая ценность, которой торгуют на некоторых биржах. Однако FCT не является настоящей валютой в том смысле, как это понимается для Биткойна. Токены FCT могут быть конвертированы их владельцем во “входные кредиты” (*entry credits*, ECs), непереводимые жетоны, которые используются исключительно для получения права на запись данных в сети Factom. Эта транзакция необратима и ее нельзя отменить. После такой конвертации токены Factoid как бы сгорают и навсегда выводятся из оборота.

Рыночная стоимость токенов FCT колеблется в зависимости от спекуляций на бирже и уровня использования, тогда как входные кредиты имеют стабильную стоимость, которая поддерживается на уровне 0,001 доллара США. Это делает размер платы, взимаемой за ввод данных в сеть, четко предсказуемым.

В самом начале работы команда корпорации выставила некоторое количество токенов на продажу с целью сбора средств на реализацию проекта Factom посредством краудфандинга. На данный момент сеть Factom еще не достигла полной федерации из 32 узлов, как это было задекларировано в основополагающем документе системы. Когда полная федерация в 32 узла будет собрана, в системе начнется генерация новых токенов (FCT), которые будут выдаваться как вознаграждение федеральным узлам и узлам аудита.

Федеральные узлы — это узлы, которые выбраны сетью для поддержания консенсуса и проверки транзакций. Узлы аудита проверяют честность этих узлов и могут лишить любой из них статуса федерального, если он будет замечен в нарушении одного из правил сети или отключится от нее, перейдя в режим офлайн.

Выпуск новых токенов FCT для вознаграждения серверов в сочетании с гашением уже выпущенных токенов пользователями представляет собой процесс переноса стоимости. Его результатом является то, что, в сущности, именно пользователи оплачивают работу серверов.

Привязывание приложений

Появление технологии блокчейна открыло дорогу новым продуктам и услугам. Сам по себе блокчейн служит лишь основой, тем уровнем, на котором старые технологии либо обретают вторую жизнь, либо заменяются новыми. Каждый блокчейн может иметь собственные уникальные свойства, которые сделают его идеальной основой для приложений определенного типа.

Блокчейн Factom особенно хорош для защиты информации, но у него все же есть ограничения: предельный размер входного блока, а также тот факт, что чем больше вводится информации, тем дороже это обходится. Можно считать,

что система Factom является идеальной в случае хранения больших файлов в структурах типа “облако” с размещением в блокчейне Factom лишь указателей на них, которые и будут использоваться в ваших приложениях для доступа к требуемым файлам.

Проект Factom в основном используется как система для управления документами, данными, а также для обеспечения подлинности и подтверждения идентичности. Блокчейн Factom интегрирован с другими блокчейнами и его можно использовать как авторитетный источник в своих смарт-контрактах.

Помещение информации в систему Factom

Проект Factom был создан разработчиками для разработчиков. Он предполагает использование специального программного терминала и требует загрузки специального ПО как для использования кошелька, так и для записи ваших данных в блокчейн системы.

Команда разработчиков Factom ставила своей главной целью создание, прежде всего, надежной и устойчивой системы. Они подготовили документацию, в которой вы найдете подробное описание и инструкции, необходимые для прохождения всей процедуры. Кроме того, в Сети веб-сервис GitHub выступает как общедоступное хранилище всего ПО с открытым кодом системы Factom и позволяет не только ознакомиться с ним, но и внести свой вклад в его разработку. Командой были приложены немалые усилия, чтобы сделать платформу Factom более дружественной к индивидуальным пользователям, но здесь все еще есть над чем работать.



СОВЕТ

Приложение FreeFactomizer является одним из моих любимых из числа созданных на платформе Factom ее почитателями. Оно очень простое в использовании и позволяет проверять основные функциональные возможности системы Factom без необходимости быть разработчиком, открывать терминал или писать какой-либо программный код. Это приложение создает хеш из данных, которые вы введете в текстовое поле или загрузите в виде файла. Затем оно собирает хеши документов, введенных в систему другими пользователями, и каждые десять минут компонует все эти хеши в один блок, записываемый в блокчейн Factom, а пользователю предоставляется возможность получить доказательство существования этого документа.



ЗАПОМНИ!

Приложение FreeFactomizer является бесплатным сервисом, предоставляемым индивидуальным лицом. Поддержка работы этого сервиса требует определенных средств, поэтому в будущем он может оказаться недоступным. Кроме того, по этому приложению не предоставляется гарантий какого-либо типа.

Чтобы воспользоваться приложением FreeFactomizer, выполните следующие действия.

1. Зайдите на сайт <http://www.freefactomizer.com>.

На рис. 7.3 представлена главная страница этого сайта.

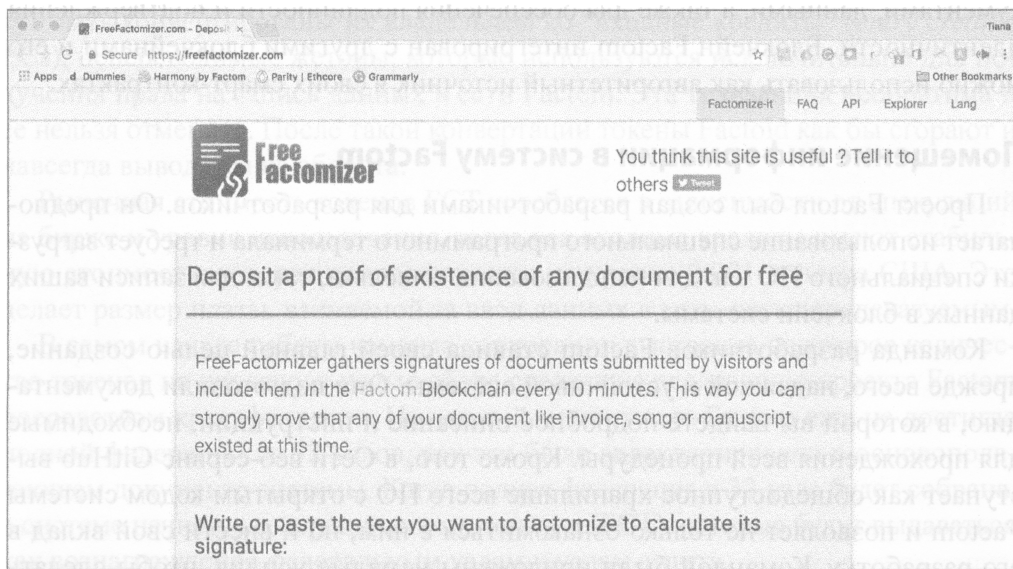


Рис. 7.3. Приложение FreeFactomizer — отличное средство опробовать на практике работу блокчейна Factom

2. Загрузите на сайт документ, который будет подвергнут хешированию.

Выберите документ, не имеющий особого значения, т.е. не содержащий личной или конфиденциальной информации, поскольку этим сервисом не предоставляется никаких гарантий или защиты.

3. Щелкните на кнопке FACTOMIZE THIS SIGNATURE.

Вам будет предоставлена оценка, сколько времени следует подождать, пока эти данные будут записаны в блокчейн Factom.

4. Дождитесь, когда блок с вашими данными будет записан в блокчейн.

На это потребуется максимум 10 минут. Чтобы проверить завершение записи, через некоторое время в окне приложения вновь щелкните на ссылке check again. Когда ввод данных будет осуществлен, в ответ на щелчок вам будет предоставлена информация о результатах записи и дана ссылка для проверки ее результатов.

5. Проверьте запись данных, воспользовавшись программой Factom Explore, поисковым инструментом базы данных Factom, позволяющим просматривать информацию в ней.

Другой, более простой способ — попробовать вновь записать эти же данные в систему. В результате такой попытки вы получите уведомление ->Signature already registered. Это означает, что указанные данные уже присутствуют в блокчейне Factom.

Поздравляю! Вы только что записали копию своих данных в систему Factom и на практике узнали, как она работает.

Повышение прозрачности в ипотечной индустрии

Служба управления документами Harmony, работающая с использованием технологии блокчейна, является первым коммерческим продуктом корпорации Factom. Она ориентирована на ипотечную индустрию, организации которой предоставляют клиентам займы на постройку домов.

Приложение Factom Harmony, общая структура базы данных которого представлена на рис. 7.4, в процессе работы получает графические образы различных документов, используемых банками, и помещает их в блокчейн-реестр, предназначенный для хранения этих документов. Создание блоков входных данных и манипулирование ими осуществляется в реальном времени по ходу процедуры предоставления ипотечного займа. Как только данные будут защищены в блокчейне Factom, становятся доступными в прозрачном режиме соответствующие метаданные, указывающие на конфиденциальные сведения о соглашениях, достигнутых между двумя доверенными сторонами.

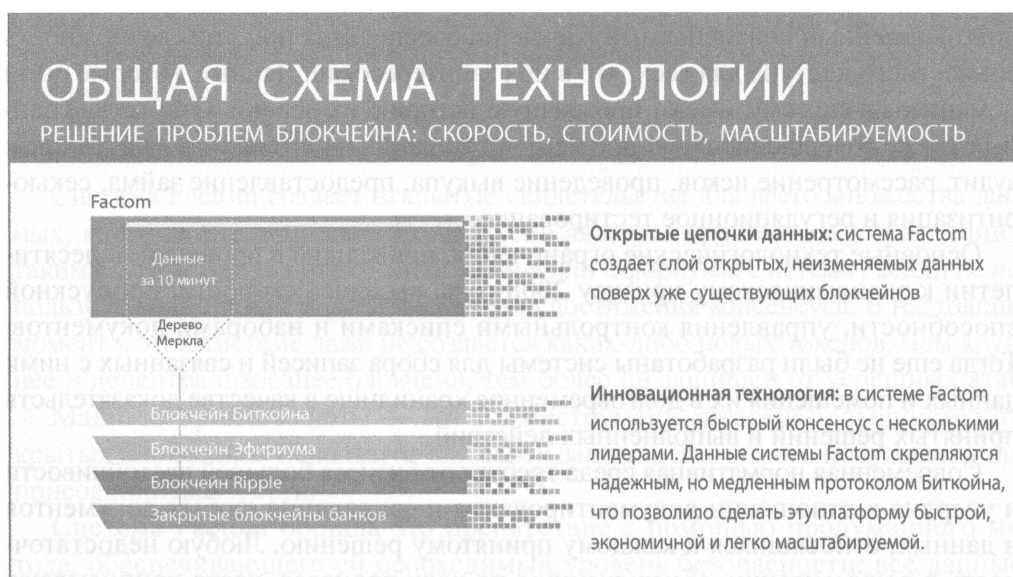


Рис. 7.4. Технология Harmony в системе Factom

Говоря простыми словами, сервис Harmony от корпорации Factom представляет собой каталог документов, построенный на основе системы обработки изображений. И это представляет собой радикальное улучшение в сравнении с ранее существовавшими системами, поскольку клиенты, которые еще долгие годы будут связаны обязательствами с банком, могут быть уверены, что образы подписанных ими и сохраненных в системе бумаг навсегда останутся идентичными тем документам, на основании которых был выдан займ. Получателям ипотечных займов больше не нужно доверять щепетильности и добропорядочности многих посредников, обеспечивавших заключение сделки между ними и заимодавцами.

Корпорация Factom надеется на получение части стоимости, высвобождающейся за счет исключения расходов, связанных со сбором и верификацией документов. Банки и другие кредиторы сейчас тратят огромное количество времени на проведение аудита, а ведь сверку записей можно осуществить, воспользовавшись всего лишь корректным набором записей и данных, сохраненных в блокчейне Factom. Это гораздо проще, особенно в тех случаях, когда несколько держателей токенов координируют свои действия, совместно работая с документами о займах, поступившими из различных источников.

Защита данных в блокчейне: цифровой регистр

Приложение Harmony корпорации Factom (см. предыдущий раздел) предоставляет пользователям возможность сохранять определенные данные и документы, необходимые для принятия решений и достижения соглашений, в долговременный неизменяемый блокчейн, обеспечивая при этом возможность совместного доступа для всех, кто в них заинтересован. Данные, которые были помещены в систему, имеют прозрачную историю их версий. Отсутствие данных также совершенно очевидно. Все это желательно в таких процедурах, как аудит, рассмотрение исков, проведение выкупа, предоставление займа, секьюритизация и регуляционное тестирование.

Основные технологические ограничения, приведшие в прошедшем десятилетии к экономическому кризису 2008 года, касались скорости, пропускной способности, управления контрольными списками и наборами документов. Тогда еще не были разработаны системы для сбора записей и связанных с ними данных и помещения их в долговременное хранилище в качестве доказательств принятых решений и выполненных действий.

Современная нормативная среда требует от бизнеса большей настойчивости и усердия в отношении документирования и сохранения любых документов и данных, относящихся к каждому принятому решению. Любую недостаточность в документации, обнаруженную по ходу процесса, часто приписывают злему умыслу, не оставляя другой стороне возможности обосновать достоверность данных и принятых на их основе решений.

Как сервис Harmony взаимодействует с системой Factom

Технологическое решение системы Factom представляет собой комбинацию блокчейн-технологии, цифровых сигнатур и набора криптографических функций, разработанных Национальным институтом стандартов и технологий США (NIST). Серии точек данных с криптографической защитой записываются в другие блокчейны, что обеспечивает пользователям возможность сохранять данные и документы для использования в будущем. В результате этого процесса создается электронный каталог файлов, которые в любое время могут быть считаны и проверены любой уполномоченной стороной.

В системе Factom на основе криптографического протокола SHA-256 генерируется хеш каждого документа и файла данных, которые затем сохраняются в блокчейне системы. Этот хеш обеспечивает криптографическую защиту, гарантирующую, что файл никогда не сможет быть изменен или заменен другим.



ЗАПОМНИ

Хеш представляет собой уникальный “отпечаток пальца” для набора данных, однозначно представляющий содержимое этого файла, но без риска, что эти данные могут быть раскрыты.

Вместе с хешем каждого документа и файла данных, связанного с записью, служба Harmony дополнительно генерирует и сохраняет набор ключевых точек метаданных. В метаданных документы и файлы данных ассоциируются и связываются с использованием аналогичных криптографических инструментов. Эти метаданные вместе с хешами файлов затем записываются в блокчейн системы Factom.

Использование блокчейна как открытого свидетельства

Система Factom создает открытые свидетельства для всего множества данных, которые она защищает. Ее блокчейн является крошечным в сравнении с такими гигантами, как блокчейн Биткойна или Эфириума. Система Factom не использует майнинг как элемент механизма достижения консенсуса. В настоящий момент в этой системе даже не создается каких-либо новых токенов. Чем крупнее и децентрализованнее блокчейн, тем более он защищен от успешных атак.

Майнинг криптовалюты — вот тот инструмент, который большинство открытых блокчейнов использует для своей защиты. Это то, что побуждает узлы присоединиться к сети.

Система Factom обошла это препятствие с помощью продуманного метода, обеспечивающего ей необходимый уровень безопасности: все данные, помещаемые в блокчейн Factom, автоматически связываются с блокчейнами Биткойна и Эфириума. Эта процедура осуществляется каждые десять минут с

использованием механизма хеширования. Весь набор существующих данных подвергается хешированию с получением одного уникального хеша, представляющего весь блокчейн системы Factom.

Проверка физических документов: dLoc и Factom

Компания Smartrac, мировой лидер в разработке, производстве и продаже RFID-транспондеров, вкладышей, предламинированных и полужаконченных карт, является партнером корпорации Factom. Результатом этого партнерства стала разработка нового способа защиты физических объектов с помощью блокчейна. Этот продукт и соответствующий ему сервис получили название “dLoc”. Изделие dLoc было разработано в виде стикера, который можно наклеить практически на что угодно. Особенно удобно им пользоваться в случае бумажных документов, подобных свидетельству о рождении или сертификату аутентичности.

Технология dLoc представляет собой сквозную систему управления безопасностью документов, в которой используется специальное программное и аппаратное обеспечение. Изделие компании Smartrac для технологии dLoc представляет собой клейкий стикер, на котором размещен трансподер класса NFC (коммуникатор ближней идентификации) со встроенным чипом. Этот стикер наклеивается на документ или другой предмет, для которого затем организуется защита с использованием блокчейна Factom.



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

Протокол NFC регламентирует установку соединения между двумя электронными приборами, когда их подносят один к другому на определенное расстояние.

Комбинация облачного программного обеспечения с технологическими решениями системы Factom позволяет создать долговременное и фактически неизменяемое свидетельство идентичности практически для чего угодно. Люди, имеющие необходимый уровень допуска, могут получить доступ к данным и проверить достоверность физического документа с помощью мобильного приложения сервиса dLoc.

Также технология dLoc позволяет агентствам-эмитентам или другим организациям превратить свои обычные документы в цифровые объекты, которые легко можно поместить в уже существующие цифровые системы, что создает мост над пропастью, существующей между миром реальным физическим и виртуальным цифровым. Данный подход может применяться к самому широкому диапазону документов — от свидетельств о рождении, документов о праве собственности на землю до судебных и медицинских записей.

Технология dLoc представляет собой первую практическую систему аутентификации документов, которая использует блокчейн системы Factom для решения проблемы целостности данных, устраняя разрыв между физическим и цифровым мирами. Это первое надежное средство защиты информации, помещенной в документы на бумажной основе, посредством создания ее цифрового образа, сохраняемого с использованием блокчейн-технологии. Технология dLoc — это решение проблемы аутентификации данных и документов, которое может найти широкое применение как в открытых, общедоступных, так и в закрытых, частных секторах, т.е. практически везде, где широко используются бумажные документы.



ЗАПОМНИ

Технология dLoc не исключает возможности мошенничества. Люди остаются людьми и всегда будут искать способы обойти закон, обмануть или украсть. Данная технология лишь делает мошенничество намного более сложной и дорогостоящей задачей. Сегодня кто угодно может купить новый идентифицирующий документ или подделать товары практически где угодно. И в некоторых случаях эти подделки будут фактически неотличимы от аутентичных документов или товаров.

Технология dLoc была создана как средство распространения уникального свойства неизменяемости технологии блокчейна на физические объекты и документы. Одновременно была создана система, способная известить вас, что была предпринята попытка подделать принадлежащее вам свидетельство идентичности, а также предоставляющая возможность предпринять по этому поводу те или иные действия.



Глава 8

Майнинг по-новому: DigiByte

В ЭТОЙ ГЛАВЕ...

- » Знакомимся с DigiByte
- » Запускаем майнинг на платформе DigiByte
- » Играем за токены

Система DigiByte представляет собой блокчейн, владеющий собственным игровым пространством. Это уникальная система, которая отлично работает с многими интересными приложениями, от компьютерных игр до систем управления документооборотом. Команда разработчиков проекта DigiByte нашла верный баланс между скоростью, доступностью и широтой функциональных возможностей созданного ею блокчейна.

Еще один уникальный аспект построения блокчейна DigiByte состоит в том, что в нем используются пять независимых алгоритмов, каждый из которых применяется для создания 20% новых блоков. Это очень интересный подход, поскольку в большинстве блокчейнов все узлы работают по одному алгоритму и только самые быстрые из них выигрывают токены.

Каждый из пяти алгоритмов блокчейна DigiByte включает свой вариант майнинга, что делает протокол системы DigiByte привлекательным для большего числа пользователей, а значит, способствует децентрализации системы. Результатом использования такого сложного протокола является также тот

факт, что в случае атаки на систему атакующему потребуется получить контроль приблизительно над 60% всего хешрейта сети, чтобы вызвать в ее работе какие-либо проблемы. Это означает получение контроля по меньшей мере над 93% узлов, работающих по одному алгоритму, и над 51% узлов, работающих по остальным четырем алгоритмам. Для сравнения: в системе Биткойна атака будет удачной, если удастся получить контроль над 51% полных узлов, что делает угрозу “атака 51%” главной концептуальной слабостью блокчейна Биткойна. Если более 51% всех майнеров в системе Биткойна попадут под контроль одной группы, она сможет манипулировать блокчейном Биткойна по своему усмотрению, что скомпрометирует всю систему в целом. В результате ее токены утратят свою ценность, а защита данных в сети будет нарушена.

В этой главе речь пойдет о практическом применении и возможном будущем системы DigiByte и ее блокчейна, а также будет представлено популярное объяснение возможных методов использования этой технологии.

Знакомимся с DigiByte: быстрый блокчейн

Система DigiByte, также известная благодаря своей криптовалюте как DGB, представляет собой блокчейн, ориентированный на проведение платежей, предоставление защиты и поддержку компьютерных игр. Штаб-квартира компании, основателем которой является Джаред К. Тейт, находится в Гонконге. До этого Тейт несколько лет принимал активное участие в работе сообщества Биткойна. Разочаровавшись в разработке ядра Биткойна, в 2014 году он запустил проект DigiByte и нашел источники финансирования для расширения своей работы в области проведения платежей и торговли.

Команда проекта DigiByte выполнила отличную работу, результаты которой сейчас используются во многих проектах. В настоящее время система DigiByte позволяет обрабатывать до 300 транзакций в секунду. Для сравнения: в системе Биткойна возможна обработка до семи транзакций в секунду. В своем проекте команда поставила много захватывающих целей, в том числе — к 2021 году достичь по скорости обработки транзакций уровня системы Visa.

Система DigiByte является одной из наиболее широко распространенных сетей, более чем с 8 тысячами узлов в 82 странах мира. Она работает подобно Биткойну в том смысле, что ее можно использовать для перемещения ценности между двумя сторонами, осуществляемого с высокой скоростью при очень небольших издержках. Она также предоставляет те же функциональные возможности, что и система Биткойна в том смысле, что обеспечивает защиту для небольшого объема информации, записываемого в ее блокчейн. Этот механизм позволит вам защитить свои данные, документы и контракты, причем с большей скоростью работы, чем в системе Биткойна.

Группа по расширению доступности системы DigiByte хорошо поработала над тем, чтобы сделать этот проект более привлекательным и даже занимательным. Она предлагала призы за проведение компьютерных игр на этой платформе и вела в Твиттере веселые репортажи о них. Проект DigiByte имеет свой хостинг на сайте GitHub и является проектом с открытым кодом, работающим под лицензией MIT.

Подразделение DigiByte Gaming, входящее в состав команды DigiByte, создало платформу, на которой криптовалюта используется в игровом пространстве с целью продвижения нового типа цифровой рекламы. Эта платформа имеет постоянно растущую базу пользователей, уже превысившую 10 тысяч человек, и представляет собой форму разрешительного маркетинга, где проведение компаний и стимулирование привлечения внимания к брендам организуется с использованием криптовалютных призов и вознаграждений. Возможность осуществлять защищенные микроплатежи вне каких-либо границ придает данному типу маркетинговой платформы очень интересные конкурентные преимущества.

Проведение рекламных кампаний без учета каких-либо границ позволяет им охватывать более широкую аудиторию. Использование криптовалюты также позволяет таким компаниям осуществлять выплаты и предлагать призы практически любого размера кому угодно в мире. Будет интересно наблюдать за тем, как маркетинг в системе DigiByte начнет выходить за рамки игровой индустрии.

Майнинг в системе DigiByte

В системе DigiByte для обработки транзакций используются пять алгоритмов майнинга. На каждый алгоритм приходится около 20% всех блоков, создаваемых в сети. Данный подход делает блокчейн системы DigiByte уникальным и отличающимся от всех прочих.

Команда системы DigiByte понимала, что можно будет достичь значительных преимуществ, если на создаваемой ими платформе допустить одновременное использование нескольких типов майнинга. В системах, использующих единственный алгоритм, выигрыш всегда будет доставаться только узлам с самым быстрым оборудованием, созданным с использованием новейших технологий. А это приводит к своеобразной “каннибалистической” гонке вооружений в борьбе за скорость и новые технологии. Тогда как в системе DigiByte, позволяющей всем ее различным алгоритмам с равным успехом выигрывать право создать блок и получить в награду токены, такое гарантированное равновесие открывает путь к большему количеству и разнообразию ее участников.

Вот краткий обзор всей пятерки алгоритмов, используемых в блокчейне системы DigiByte.

- » **SHA-256** (<https://dgb-sha.theblocksfactory.com>). Для майнинга в сети DigiByte с использованием алгоритма SHA-256 необходимо иметь ASIC-оборудование.
- » **Scrypt** (<https://dgb-scrypt.theblocksfactory.com>). Для майнинга в сети DigiByte с использованием алгоритма Scrypt можно использовать ASIC- либо GPU-оборудование.
- » **Qubit** (<http://dgb-qubit.theblocksfactory.com>). Для майнинга в сети DigiByte с использованием алгоритма Qubit необходимо GPU-оборудование.
- » **Skein** (<http://dgb-skein.theblocksfactory.com>). Для майнинга в сети DigiByte с использованием алгоритма Skein необходимо GPU-оборудование.
- » **Groestl** (<http://dgb-groestl.theblocksfactory.com>). Для майнинга в сети DigiByte с использованием алгоритма Groestl необходимо GPU-оборудование.

Использование в системе DigiByte многих алгоритмов привлекает к майнингу в ней гораздо большее количество индивидуальных участников — просто за счет снижения финансового барьера для успешного входа в сеть. Повышение децентрализации сети, которое является прямым результатом разнообразия применяемых алгоритмов, послужило причиной появления многих интересных способов использования сети. Так, майнеры криптовалюты все чаще переориентируют свое устаревшее оборудование майнинга биткойнов на работу в сети DigiByte, где оно все еще может оказаться полезным.

В этом разделе я расскажу вам, как можно приобрести несколько токенов системы DigiByte, известных как DGB. Вы можете намайнить эту криптовалюту, а затем использовать ее.



СОВЕТ

Если у вас есть устаревшее оборудование для майнинга биткойнов, можете с успехом использовать его для майнинга DGB.

Прежде чем приступить к майнингу криптовалюты DGB, следует просчитать, будет ли это занятие экономически оправданным, т.е. принесет ли оно хоть какую-то прибыль. Выполните следующие действия.

1. Зайдите на сайт <http://www.coinwarz.com/calculators>.

На этом сайте вы найдете калькулятор, который позволит оценить время окупания затрат на майнинг множества различных криптовалют.

Общий вид страницы калькулятора стоимости и вероятности успеха для криптовалюты DGB на сайте CoinWarz представлен на рис. 8.1.

Рис. 8.1. Калькулятор расходов и возможной прибыли от майнинга

2. В поле **Pool Fees %** введите значение 3.

Это высшая оценка платы за участие в майнинговом пуле. Чаще всего реальная плата будет находиться в диапазоне от 0,5% до 3%.

3. В поле **Hardware Costs (USD)** введите значение 500.

Стоимость специализированного оборудования для майнинга меняется в широких пределах. Хорошей оценкой среднего значения этой стоимости будет значение 500.

4. В поле **Hash Rate (KH/s)** введите значение 470000.

Это примерная оценка того, насколько быстро ваше оборудование будет вычислять хеши, заданная в килохешах в секунду (KH/s). Иначе говоря, это оценка того, сколько тысяч хешей будет вычислено вашим оборудованием за одну секунду. Чем выше этот показатель (хешрейт) майнинга в каком-либо конкретном блокчейне, тем труднее майнить принадлежащий ему тип криптовалюты.

Вы можете также встретить обозначения “мегахешей в секунду” (MH/s), что означает 1 миллион хешей, вычисленных за секунду; “гигахешей в секунду” (GH/s), что означает 1 миллиард хешей, вычисленных за секунду; “терахешей в секунду” (TH/s), что означает 1 триллион хешей, вычисленных в секунду; и “петахешей в секунду” (PH/s), что означает 1 квадриллион хешей, вычисленных в секунду.

5. Щелкните на кнопке **Calculate**.

В окне калькулятора будет выведена информация о том, во что обойдется, какую прибыль и за какой период времени вы сможете получить в результате майнинга данной криптовалюты при указанных значениях исходных данных.



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

Когда система Биткойна только начала свою работу, для майнинга вполне можно было использовать обыкновенный настольный компьютер. Однако довольно скоро, в связи с ростом общего объема хешрейта в блокчейне Биткойна, обычному настольному компьютеру, чтобы удержаться в майнинге “на плаву”, требовалось максимально использовать уже все имеющиеся у него ресурсы.

Когда хешрейт блокчейна достиг уровня гигахешей, вычислительных возможностей среднего компьютера стало совершенно недостаточно, хотя даже этот уровень хешрейта оказался совершенно недоступным для многих майнеров. Поддержка такого уровня вычислений требовала очень больших объемов энергии, значительных затрат времени и других ресурсов, чтобы удерживать майнинг биткойнов на уровне минимальной доходности. Однако, поскольку блокчейн системы DigiByte предусматривает использование пяти разных алгоритмов, у вас все еще имеется возможность использовать нормальный компьютер для зарабатывания ее токенов.

Со временем майнеры биткойнов выяснили, что для проведения майнинга этой криптовалюты можно приспособить графический процессор (GPU) на видеокарте обычного компьютера. Использование GPU в этом процессе позволило майнерам более чем в 50 раз увеличить его скорость, при этом графический процессор потребляет меньше энергии, а значит, майнинг обходится дешевле.

В 2011 году начали появляться майнинговые фермы. На них использовалось специальное оборудование, получившее название “Программируемая пользователем вентильная матрица” или FPGA. Эти устройства подключались к компьютеру через USB-порт и расходовали гораздо меньше электроэнергии, чем в случае майнинга с использованием обычного ПК или видеокарт.

Но развитие оборудования для майнинга не стоит на месте. Сейчас наилучшим оборудованием для этих целей являются АСИК-майнеры, в которых используются интегральные схемы, разработанные специально для проведения подобных вычислений (ASIC — Application-Specific Integrated Circuit). АСИК-майнеры обеспечивают майнинг с невероятной скоростью вычисления хешей и, по моему личному опыту, являются весьма шумными аппаратами. Если вы решите приобрести такое устройство, не пожалейте времени и внимательно почитайте обзоры и отзывы. Кроме того, обязательно убедитесь, что его использование будет для вас экономически выгодным и окупится за приемлемое время, а также удостоверьтесь, что устройства данного типа совместимы с протоколом той криптовалюты, которую вы собираетесь майнить.

Подписывание документов в сервисе DiguSign системы DigiByte

Сервис DiguSign, созданный командой DigiByte, представляет собой интересную альтернативу для традиционных облачных хранилищ и служб электронной подписи. Сервис DiguSign обеспечивает основную функциональность этих приложений, добавляя к ней неизменяемость и прозрачный контроль, характерные для блокчейн-технологии. Он позволяет ставить цифровую подпись на документы, а затем защищать их средствами блокчейна системы DigiByte.

Команда DigiByte полагает, что сервис DiguSign станет очень ценным инструментом для юристов, служб предоставления медицинских услуг и в финансовых кругах, где очень важно хранить четкую историческую последовательность того, какие именно документы были представлены, когда и кому.



СОВЕТ

Вам может быть предоставлена возможность связать свою учетную запись в службе DiguSign со своими учетными записями в облачных хранилищах, таких как Google Docs, Dropbox или OneDrive. А до этого момента каждый документ вам придется по отдельности загружать в среду DiguSign. Служба DiguSign имеет бесплатную пробную версию, которая позволяет создать три бесплатных документа или контракта, занесенных в блокчейн системы DigiByte.

Служба DiguSign пока находится в стадии раннего тестирования, но уже предоставляет своим пользователям возможность хранить, неофициально нотариально заверять и придавать юридическую силу цифровым документам.



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

Служба DiguSign публикует SHA256-хеш вашего документа, помещая его в виде транзакции в блокчейн DigiByte. В дальнейшем эта транзакция защищается средствами блокчейна системы DigiByte.

Для создания учетной записи в службе DiguSign выполните следующие действия.

1. **Зайдите на сайт <http://www.digusign.com> и щелкните на кнопке GET STARTED HERE для создания собственной учетной записи в службе DiguSign.**

Для этого на открывшемся экране вам потребуется щелкнуть на ссылке Sign Up! (внизу), а затем в новом окне указать адрес электронной почты, желаемые никнейм и пароль. На почту придет письмо для подтверждения вашей учетной записи, после чего вы сможете зайти в службу DiguSign со своей вновь созданной учетной записью.

2. Загрузите пробный документ в службу DigiSign.

Вам будет предоставлена возможность создать документ или воспользоваться шаблоном контракта.

3. Выберите вариант документа, который хотите создать.

4. Введите все требуемые подписи и заполните прочие поля, которые потребуются при создании выбранного вами типа документа.

5. Введите адреса электронной почты тех людей, которые, по вашему мнению, должны будут подписать этот документ.

6. Щелкните на ссылке Secure Final Version option.

Когда все указанные вами лица подпишут этот документ, вам нужно будет отправить его окончательную версию в блокчейн системы DigiByte, просто щелкнув на кнопке Secure Final Version.

Вы только что создали новый неизменный “отпечаток пальца” вашего документа, сослаться на который сможете в любое время.

Зарабатываем токены DigiByte играя

В команде DigiByte обратили внимание на благосклонное отношение игровых сообществ к цифровым токенам и задумались над тем, чтобы приобщить их к блокчейн-технологии. Для геймеров вполне естественно использовать цифровые валюты в игровом процессе, поэтому команда DigiByte решила, что будет достаточно просто организовать использование их криптовалютного токена в качестве средства стимулирования с целью привлечения пользователей.

В системе DigiByte была реализована возможность зарабатывать токены DGB в процессе игры в такие игры, как Counter Strike, League of Legends и World of Warcraft. При этом награды предоставляются через механизм спонсирования игровых компаний, не предусматривающий использования вычислительных мощностей пользователей для майнинга криптовалюты.

Команда DigiByte реализовала интересную возможность для игровых компаний — создавать дополнительные модели стимулирования с целью привлечения новых игроков и сохранения уже существующих. Ею также был найден оригинальный способ, позволяющий игрокам превращать полученные ими в цифровом мире призы в реальные деньги, которые можно потратить в физическом мире.

Заработать токены DigiByte можно на игровом сайте этой системы. Каждый день компания DigiByte предлагает несколько квестов, прохождение которых позволяет заработать то, что на этом игровом сайте называют *XP*. Заработанные

вами баллы XP затем переводятся в токены DigiByte в соответствии с установленным на этот день курсом. В результате у вас появляется возможность играть в World of Warcraft или любую другую из предлагаемых игр, расплачиваясь за это токенами DigiByte.

Помимо этого, вы можете обменивать токены DGB на биткойны, воспользовавшись услугами любой криптовалютной биржи, например Bitfinex.com. А дальше не составит проблемы превратить биткойны в любую другую валюту, в том числе наличную. Конечно, предложенный вариант включает несколько этапов, но это понятный и довольно занимательный способ получения вознаграждения или оплаты!

Начать зарабатывать токены DigiByte посредством игры исключительно просто. Вам не нужно будет заниматься майнингом, вам даже не придется открывать окно командной строки! Просто выполните следующие действия.

1. Зайдите на сайт <http://www.digibytegaming.com>.

2. Создайте для себя новую учетную запись.

Сайт DigiByte допускает использование учетных записей социальных сетей, что делает процесс настройки более быстрым и простым.

3. Подтвердите свою новую учетную запись.

Проверьте указанный при регистрации почтовый адрес и в поступившем на него письме воспользуйтесь ссылкой для подтверждения своей учетной записи.

4. Зайдите на сайт <http://www.battle.net>.

Здесь вы можете создать себе профиль для подключения только что созданной учетной записи DigiByte. Этот профиль будет функционировать как мост между игровой площадкой World of Warcraft и системой DigiByte.

5. Установите на своем компьютере игру World of Warcraft.

Если вы уже играли в эту игру, на этом этапе просто воспользуйтесь своим игровым ключом.

6. Вернитесь на сайт <http://www.digibytegaming.com>.

7. Выберите вариант World of Warcraft.

8. Подключитесь к своей учетной записи на сайте Battle.net.

9. Запустите приложение World of Warcraft и начните играть.

Ну вот и все. Теперь вы зарабатываете токены DigiByte, просто играя!

Часть III

Мощные блокчейн- платформы

© Борогас Виктор/cartonbank.ru



В ЭТОЙ ЧАСТИ...

- » Познакомьтесь с Hyperledger — крупнейшим консорциумом, созданным специально для продвижения блокчейн-технологии в деловом мире, и оцените выгоды и воздействие, которые он может оказать на вашу индустрию или организацию
- » Узнайте об усилиях, направляемых корпорацией Microsoft на развитие блокчейн-технологии, и об основных инструментах, которые предлагаются в ее сети заинтересованным пользователям
- » Оцените проект Bluemix корпорации IBM и последствия, которых можно ожидать от объединения блокчейн-технологии с искусственным интеллектом



Глава 9

Консорциум Hyperledger: ведущая сила блокчейн-технологии

В ЭТОЙ ГЛАВЕ...

- » Знакомимся с тремя ключевыми проектами консорциума Hyperledger
- » Раскрываем возможности смарт-контрактов Chaincode
- » Изучаем Sumeragi — новый алгоритм консенсуса
- » Углубляемся в детали алгоритма консенсуса PoET

Консорциум Hyperledger — это сообщество разработчиков программного обеспечения и энтузиастов блокчейн-технологии, цель которого заключается в разработке отраслевых стандартов для блокчейн-приложений и платформ. Работа этого сообщества очень важна, поскольку это ведущая группа в вопросах превращения блокчейн-индустрии в ведущее направление отрасли и принятия ее коммерческими кругами в полном масштабе. Консорциум

Hyperledger предоставляет “безопасную” платформу для развертывания проектов масштаба предприятия.

Эта организация и ее уникальные проекты растут и развиваются с каждым днем. На момент написания этих строк в ней состояло более ста компаний-членов и несколько проектов уже находилось в стадии разработки. Среди нескольких первых проектов можно упомянуть Explorer, веб-приложение для просмотра и уточнения содержимого блоков, а также Fabric, не требующая настройки программа-построитель для создания блокчейн-приложений. Также в работе находятся проекты Iroha и Sawtooth, представляющие собой модульные блокчейн-платформы.

В этой главе будут подробно рассмотрены три ключевых проекта консорциума Hyperledger, работа над которыми идет полным ходом. Также вы получите полное представление о будущем коммерческих блокчейнов и о том, чем они станут для вашей компании и индустрии. Это знание поможет вам принять правильное решение в ходе анализа, какие технологии следует использовать в своих проектах, а каких лучше избегать, чтобы исключить излишние затраты времени и ресурсов.

Знакомимся с Hyperledger: мечты о гипербудущем

В конце 2015 года консорциум Linux Foundation сформировал проект Hyperledger, направленный на развитие среды разработки приложений распределенных реестров масштаба предприятия. Этим решением предполагалось сфокусировать внимание блокчейн-сообщества на создании надежных, ориентированных на конкретные отрасли систем из приложений, платформ и оборудования с целью поддержки бизнес-процессов и бизнеса в целом.

Консорциум Linux Foundation обратил внимание на существование множества различных групп, работающих над развитием блокчейн-технологии при полном отсутствии координирующего их действия органа управления. В результате усилия многих независимых групп были направлены на достижение одинаковых целей, что вынуждало каждую группу вновь решать одни и те же задачи. Создатели проекта знали по собственному опыту, что для того, чтобы эта технология смогла полностью раскрыть свой огромный потенциал, просто необходимо придерживаться стратегии совместной разработки приложений с открытым кодом.

Проект Hyperledger возглавляет исполнительный директор Брайан Белендорф, обладающий огромным опытом, накопленным за десятилетия, прошедшие с момента основания им фонда Apache Foundation и последующего

образования консорциума Linux Foundation. Кроме того, он является технологическим директором Всемирного экономического форума (ВЭФ) в Давосе, поэтому совсем не удивительно, что проект Hyperledger был очень хорошо принят. Многие ведущие игроки в бизнесе и промышленности присоединились к этому проекту, включая корпорации Accenture, Cisco, Fujitsu Limited, IBM, Intel, J.P. Morgan и Wells Fargo. Также он привлек внимание многих ведущих блокчейн-организаций.

Консорциум R3, поддерживающий банковскую индустрию, передал проекту Hyperledger свое архитектурное решение для финансовых транзакций, а компания Digital Asset предоставила свои стандарты и определенные программные решения для приложений масштаба предприятия. Корпорация Factom предоставила в распоряжение консорциума некоторые свои разработки масштаба предприятия, а также часть своих разработчиков. Корпорация IBM и многие другие организации тоже передали в распоряжение проекта свои программные и прочие ресурсы.

Технические руководящие комитеты консорциума Hyperledger призваны обеспечить надежность и широкие возможности для взаимодействия между этими различными технологиями. Можно надеяться, что межотраслевое сотрудничество на платформе с открытым кодом даст блокчейн-технологии значительные преимущества и принесет миллиарды в ее экономическую ценность, распределив при этом издержки на исследования и разработку между многими организациями.

В проектах Hyperledger выявляются важные функции и требования, отсутствующие на данный момент в экосистеме блокчейн-технологии, и принимаются решения, направленные на устранение возникших проблем. Здесь также поощряется разработка межотраслевых открытых стандартов в отношении распределенных реестров, а разработчикам предоставляются широкие возможности внести свой вклад в создание более совершенных блокчейн-систем.

Рабочая процедура проекта Hyperledger похожа на ту, которая принята в консорциуме Linux Foundation. Все поступающие предложения анализируются и обсуждаются, а принятые направляются в разработку. Когда проект достигает стабильного состояния, он считается завершенным и переводится в активное состояние. На сегодняшний момент все проекты консорциума Hyperledger¹ находятся в стадии предложений либо в стадии разработки. Каждый из проектов возглавляется крупной корпорацией или стартапом. Например, проект Fabric возглавляет корпорация IBM, проект Sawtooth — корпорация Intel, а во главе проекта Iroha стоит стартап Soramitsu.

¹ Все, кроме одного: проект Hyperledger Fabric 1.0 был признан достаточно надежным и передан как завершенный в активное использование в июле 2017 года. — *Примеч. ред.*

В своих проектах консорциум Hyperledger, как и многие другие проекты с открытым кодом, использует сайты GitHub (<http://www.github.com/hyperledger>) и Slack (<https://slack.hyperledger.org>) для предоставления широкой общественности контакта с командой разработчиков, работающей над каждым отдельным проектом. Эти площадки — лучшее место для получения последних обновлений и проверки, какой прогресс за прошедшее время был достигнут в ходе разработки каждого из этих проектов.

Сосредоточимся на приложении Fabric

Первым проектом консорциума Hyperledger, достигшим стадии разработки, был проект Fabric, представляющий собой блокчейн-платформу с правами доступа. Он работает так же, как и большинство прочих блокчейнов, в том смысле, что в нем создается и хранится реестр цифровых событий. Эти события представляются как транзакции, совместный доступ к которым предоставляется различным участникам. Запись транзакций осуществляется без использования криптовалюты. Наилучшим источником информации об этом проекте является документ https://trustindigitallife.eu/wp-content/uploads/2016/07/marko_vukolic.pdf.

Все транзакции являются защищенными, закрытыми и конфиденциальными. Блокчейн в Fabric может быть обновлен только по достижении консенсуса между участниками. Помещенную в него запись уже никогда нельзя будет изменить.

Платформа Fabric представляет собой решение для предприятий, заинтересованных в возможности масштабирования своих процессов с соблюдением всех правил, установленных регулируемыми органами. Все участники должны зарегистрировать свои доказательства идентичности в службе контроля членов, чтобы получить доступ к системе. В блокчейне Fabric транзакции формируются с производными сертификатами, которые не связаны непосредственно с владеющими участниками, тем самым обеспечивая анонимность в сети. Кроме того, содержимое каждой транзакции шифруется, чем гарантируется, что увидеть его сможет только установленный круг участников.

Платформа Fabric имеет модульную архитектуру. В свой проект вы сможете добавить или изъять определенные компоненты, реализуя тем самым необходимые спецификации его протокола. Контейнерная технология этой платформы позволяет использовать большинство основных языков для разработки смарт-контрактов.

Напротив, в работе системы Биткойна каждый может принять участие анонимно, и ее сообщество всегда находится в поисках способов, позволяющих

оказывать сопротивление цензуре и проявлять активность тем, кто был лишен гражданских прав. Также система Биткойна была разработана преимущественно с целью перемещения и защиты ее криптовалютного токена. По этой причине сравнение лучших решений в системах Биткойна и Fabric может иметь мало смысла.

Создание собственной системы в среде Fabric

Множество усилий было приложено к тому, чтобы сделать платформу Fabric более доступной для широкой публики, но она по-прежнему во всей полноте доступна для понимания лишь тем, кто достаточно технически подкован.

Консорциум Hyperledger предоставил несколько детальных описаний вариантов использования этой технологической платформы. В ближайшем будущем платформу Fabric можно будет использовать и для разработки различных иных приложений с интуитивным пользовательским интерфейсом, помимо тех, которые были представлены в упомянутых выше описаниях. Но в любом случае при создании собственных приложений вам не обойтись без привлечения к работе квалифицированных разработчиков.

Работа с контрактами типа Chaincode

На платформе Hyperledger Fabric контракты между двумя сторонами могут быть переведены в код с использованием технологии Chaincode. Технология Chaincode — это версия смарт-контрактов системы Эфириум от концерна Hyperledger. Данная технология автоматизирует выполнение соглашения, зафиксированного в контракте, таким способом, которому могут доверять обе договаривающиеся стороны.

Технология Chaincode является полной по Тьюрингу, как и смарт-контракты Эфириума. В данный момент для создания chaincode-контракта вам потребуется помощь программиста на языке Java. Команда Fabric разработала некоторые типовые варианты сценариев, например манипуляции цифровыми валютами или отправка текстовых сообщений, включив их создаваемую систему как элементы ядра среды разработки. Команда Fabric также предусмотрела другие интересные сценарии бизнес-манипуляций, работа над которыми еще не была завершена на момент написания этой книги, но которые, без сомнения, уже будут реализованы, когда вы будете ее читать.

Проекты консорциума Hyperledger еще находятся на довольно ранней стадии разработки, отставая примерно на два года от результатов работы разработчиков системы Эфириум. Однако каждый из проектов поддерживается действительно серьезной командой и обеспечен необходимыми ресурсами.

- » **Бизнес-контракты.** В Hyperledger решено обеспечить поддержку как открытых, так и закрытых контрактов. Закрытые контракты заключаются между двумя и более сторонами и содержат конфиденциальную информацию. Открытые контракты доступны для просмотра всем желающим, кто не пожалеет времени на их поиск в блокчейне Hyperledger. Например, можно использовать открытый контракт, чтобы сделать публичное предложение о продаже некоего продукта или, наоборот, воспользоваться им с целью запросить предложения по контракту.

Подготовка таких контрактов является более сложной задачей в сравнении с традиционными контрактами, поскольку здесь отсутствуют арбитр и третья сторона, обеспечивающая точное соблюдение всех условий. Кроме того, необходима аутентификация лиц, участвующих в контракте. Плюс большинство контрактов являются уникальными и не поддаются стандартизации. Чем сложнее контракт, тем в больших местах он может быть искажен в отношении его исходных намерений. Команда консорциума Hyperledger работает над созданием системы управления контрактами, обеспечивающей повышение масштабируемости возможностей контрактов Chaincode.

- » **Цепочки поставок для производства.** Управление цепочками поставок является превосходным объектом для применения блокчейн-схем и по этой причине детально исследовалось в проекте Fabric. Компании, занимающиеся окончательной сборкой готовых изделий, получают возможность управлять поставками всех компонентов и материалов, необходимых для выпуска их продукции. Эта функция проекта обеспечивает возможность своевременно реагировать на спрос и при необходимости отслеживать происхождение каждого компонента вплоть до его оригинального изготовителя. В случае возврата продукта можно будет легко найти виновника брака; кроме того, обеспечивается возможность запросить сведения об аутентичности каждого элемента до его использования.

Пока проект Fabric нуждается в дополнительных усилиях разработчиков для данного сценария, поскольку здесь требуется обеспечить легкую доступность данных для всех участников цепи поставок. Команда Fabric работает над стандартным протоколом, позволяющим каждому участнику в сети цепочек поставок вводить и отслеживать информацию о номерных компонентах, которые производятся и используются для изготовления конкретной продукции.

Когда работа будет закончена, новая функциональность позволит проводить глубокий поиск сведений о производстве каждого продукта, причем в любое время. При этом допускается десять и более

уровней углубления в производство любого из изделий. Потребители смогут установить происхождение любого произведенного товара, который, в свою очередь, состоит из других компонентов и материалов, происхождение которых также может быть установлено. Такая возможность способна оказать интересное социальное воздействие на потребление.

- » **Ценные бумаги и активы.** Ценные бумаги и активы — это как раз то, что идеально подходит для блокчейн-технологии, поскольку в этом случае можно будет автоматизировать многие функции, которые в обычном мире выполняются третьей стороной. Платформа Fabric позволит всем держателям ценных бумаг иметь прямой доступ к этим активам, их структуре и истории, обходясь без посредников, которые сейчас владеют этой информацией. Платформа Fabric также позволит повысить скорость проведения расчетов по активам, приблизив его к реальному времени.
- » **Прямая связь.** В будущем платформу Fabric можно также будет использовать как площадку, на которой компании смогут размещать свои публичные заявления и предложения. Например, если компания хочет увеличить свои фонды и ей необходимо известить всех держателей акций о конкретных деталях своего предложения в реальном времени, она сможет это сделать. Как и децентрализованные автономные организации (DAO) в системе Эфириум, держатели акций смогут принять решение и привести его в исполнение. Процесс принятия решения и его утверждение будут происходить в реальном времени. Все это сделает процедуру обсуждения и голосования существенно более простой и быстрой.
- » **Взаимодействие активов.** В будущем платформа Fabric, возможно, получит такие же функциональные возможности, какие имеются в системе Ripple (см. главу 6). Можно представить такой вариант использования платформы, когда компании смогут проводить обмен своих активов на малоликвидных рынках, сопоставляя требования между многими сторонами. Вместо того чтобы заниматься урегулированием рыночных ограничений при прямой торговле между двумя сторонами, сеть блокчейна обеспечит соединение покупателей с продавцами и поможет найти лучшее соответствие среди активов многих видов. В будущем среда Hyperledger вероятно, будет весьма привлекательной для торговли деривативами. Узнать больше по этой теме можно из документа

http://events.linuxfoundation.org/sites/events/files/slides/TradingDerivatives_LinuxCon_2016.pdf.

Исследуем проект Iroha

Проект Iroha консорциума Hyperledger построен на результатах работы, выполненной в проекте Fabric. Он предназначен для расширения функциональности платформ Fabric, Sawtooth Lake и других проектов, осуществляемых под эгидой консорциума Hyperledger. В сообществе Hyperledger проект Iroha был переведен в стадию разработки прежде всего по той причине, что другие проекты не включают каких-либо проектов инфраструктуры, написанных на языке C++. Отсутствие проектов на языке C++ сильно ограничивает круг людей, которые могут получить преимущества от использования платформ консорциума Hyperledger, а также количество разработчиков, которые могли бы внести свой вклад в его проекты.

Кроме того, на данный момент большинство разработок блокчейнов было выполнено на самом низком уровне инфраструктуры и практически не было проведено каких-либо работ по созданию приложений пользовательского интерфейса или мобильных приложений. В консорциуме Hyperledger считают, что приложение Iroha просто необходимо для широкой популяризации блокчейн-технологии. Этот проект заполняет существующий пробел, позволяя привлечь к работе больше специалистов-программистов и предоставляя необходимые библиотеки разработчикам интерфейсов пользователя для мобильных устройств.

На момент написания этих строк проект Iroha был еще совсем новым и не был интегрирован с платформами Fabric и Sawtooth Lake. В консорциуме Hyperledger планировалось в ближайшем будущем расширить его функциональность для обеспечения работы с блокчейнами других проектов. Библиотеки проекта Iroha для iOS, Android и JavaScript предоставляют вспомогательные функции, такие как добавление цифровой подписи к транзакциям. Они будут очень полезны при разработке коммерческих приложений, позволяя добавить новые уровни защищенности и бизнес-модели, реализовать которые можно только на основе блокчейн-технологии.

Знакомьтесь: Sumeragi, новый алгоритм консенсуса

Все блокчейны включают подсистему, которая позволяет узлам сначала договориться о единой версии истинного состояния, а затем записать это одобренное всеми истинное состояние в реестр. Достигнутое всеми соглашение здесь называют *консенсусом*.

Достижение консенсуса — это сложный процесс. Подробное обсуждение всех нюансов того, как и на каких принципах в сети достигается консенсус, выходит далеко за рамки этой книги. К тому же это совершенно излишне и едва ли потребуется вам как бизнес-профессионалу. Действительно важным

для вас будет лишь понимание того, как выбор того или иного варианта механизма консенсуса отразится на том, что вы сможете делать в среде этого блокчейна. Я выделила описание консенсуса проекта Iroha, получившего название “Sumeragi”, в отдельный раздел лишь потому, что он очень сильно отличается от методов достижения консенсуса в традиционных блокчейнах.

Вот несколько ключевых положений, которые делают консенсус Sumeragi таким особенным.

- » В консенсусе Sumeragi не используется криптовалюта.
- » Узлы, которые начинают свое участие в консенсусе, добавляются в систему службами контроля членов платформы Fabric. С течением времени узлы создают себе репутацию на основании того, как они взаимодействовали с реестром. Для этого используется блокчейн разрешений, формируемый известными субъектами системы.
- » Новые записи добавляются в реестр уникальным образом. Первый узел, который начал процедуру консенсуса, называемый *лидером*, распространяет запись среди группы других узлов, после чего эти узлы осуществляют проверку записи. Если проверка завершилась неудачно, первый узел через заранее установленный промежуток времени вновь повторяет рассылку записи. Элемент рассылки записей напоминает то, как работает консенсус в системе Ripple.

В зависимости от того, как вы собираетесь использовать блокчейн, пакет Iroha может быть для вас хорошим или плохим выбором. Если вас беспокоит проблема изменения данных, пакет Iroha может оказаться не самым лучшим вариантом. В этом случае вам лучше подобрать такой вариант блокчейна, в котором гарантируется защита от манипуляции данными. Если вас беспокоит вопрос о возможности арбитража со стороны других участников сети, пакет Iroha вновь является не самым лучшим выбором — здесь необходимы дальнейшие исследования. Но если вы хотите знать всех игроков в своем блокчейне, пакет Iroha, скорее всего, — именно то, что вам нужно.

Разработка мобильных приложений



СОВЕТ

Пропустите этот раздел, если вы не принадлежите к сообществу разработчиков приложений.

Пакет Iroha создавался для разработчиков мобильных и веб-приложений с целью предоставить в их распоряжение всю мощь систем консорциума Hyperledger. Команда проекта Iroha понимала, что построение распределенного реестра будет совершенно бесполезно, если не будет приложений, позволяющих им пользоваться.

Пакет Iroha пополняет арсенал разработчиков следующими инкапсулированными компонентами на языке C++.

- » Библиотека консенсуса Sumeragi
- » Библиотека цифровой подписи Ed25519
- » Хеш-библиотека SHA-3
- » Библиотека сериализации транзакций Iroha
- » Библиотека рассылки P2P
- » Библиотека серверного API
- » Библиотека iOS
- » Библиотека Android
- » Библиотека JavaScript
- » Эксплорер блокчейна/пакет визуализации данных

Одним из важнейших препятствий в развитии блокчейн-индустрии являлась необходимость сделать системы дружелюбными по отношению к их пользователям. В проекте Iroha были созданы библиотеки ПО с открытым кодом для iOS, Android и JavaScript и реализованы общие функции API, удобные для вызова. Проект еще не завершен, но Iroha — это отличный ресурс, за состоянием которого необходимо следить, работая над бизнес-приложениями.

Блокчейн-платформа Sawtooth Lake

Проект Sawtooth Lake, возглавляемый корпорацией Intel, является еще одной платформой с распределенным реестром в консорциуме Hyperledger. Его цель — создание мощной модульной платформы для построения новых распределенных блокчейн-реестров уровня компании.



ВНИМАНИЕ!

На момент написания этих строк текущий релиз платформы включал программное обеспечение, которое только *имитировало* консенсус. Оно не предоставляло никакой защиты для создаваемых на его основе проектов, а значит, могло использоваться только для целей тестирования продуктов и проверки новых идей.

В платформе Sawtooth Lake не используется криптовалюта. Защита в ней обеспечивается за счет разрешения бизнес-приложениям создавать собственные блокчейны. Эти поддерживаемые бизнес-приложениями частные блокчейны затем распределяют бремя вычислений, необходимых для работы сети. В документации проекта Sawtooth Lake утверждается, что такой тип настройки будет гарантировать универсальное соглашение о состоянии разделяемого реестра.

В платформе Sawtooth Lake были взяты базовые модели блокчейнов, но при этом их поставили с ног на голову. Большинство блокчейнов имеют следующие три элемента.

- » Разделяемая запись текущего состояния блокчейна
- » Способ ввода новых данных
- » Способ достижения соглашения по этим данным

В платформе Sawtooth Lake первые два элемента слиты в сигнальный процесс, получивший название *transaction family* (семейство транзакций). Эта модель лучше в использовании в тех случаях, когда все участвующие стороны получают взаимную выгоду от корректной записи данных.

Разработчики корпорации Intel обеспечили созданному ими ПО достаточную гибкость, чтобы вмещать пользовательские семейства транзакций, отражающие уникальные требования каждого бизнеса. Эта платформа также имеет три встроенных шаблона для построения цифровых активов.

- » **EndPointRegistry.** Место для записи элементов в блокчейн
- » **IntegerKey.** Разделяемый реестр, используемый для управления цепями поставок.
- » **MarketPlace.** Торговая блокчейн-платформа для покупки, продажи и котировки цифровых активов.

Алгоритм консенсуса платформы: Proof of Elapsed Time

Алгоритм консенсуса платформы Sawtooth Lake получил название “Proof of Elapsed Time” (PoET — “доказательство прошедшего времени”). Он был разработан для выполнения в защищенной области центрального процессора вашего компьютера, называемой “trusted execution environment” (TEE — “доверительная среда выполнения”). Алгоритм PoET использует защищенность области TEE для вставки в транзакцию меток времени с целью доказательства, что время прошло.

Другие алгоритмы консенсуса также имеют определенный элемент, который можно уподобить метке времени. Способ, которым гарантируется, что записи не подвергались изменению, состоит в их открытом публиковании в блокчейне, — как доказательство того, что он не изменялся. Открытый реестр действует как общедоступное свидетельство, которое любой может просмотреть и проверить. Этот подход похож на публикацию в газете объявления как доказательства того, что нечто произошло.

Алгоритм PoET также имеет систему выбора узла, которая работает немного иначе, чем в других блокчейнах, использующих алгоритм консенсуса “proof-of-work”. Узел в нем случайным образом выбирается из пула проверяющих

узлов. Для узла вероятность быть выбранным возрастает пропорционально объему обработки ресурсов разделяемого реестра, который этот узел взял на себя. При этом могут быть приняты меры для предотвращения ситуации, когда узлы “разыгрывают” систему или пытаются повредить ее реестр.

Развертывание среды разработки Sawtooth

Корпорация Intel подготовила комплект превосходной документации и справочных материалов, который доступен по адресу <https://intelledger.github.io/tutorial.html>. Здесь подробно описывается процесс установки виртуальной среды разработки блокчейна, причем в качестве примера используется блокчейн для игры в крестики-нолики. Чтобы эта документация была для вас полезной, необходимо иметь определенное представление о таких инструментах, как Vagrant и VirtualBox.



Глава 10

Используем Microsoft Azure

В ЭТОЙ ГЛАВЕ...

- » Создание новых приложений
- » Связывание существующих систем
- » Проверка подлинности новых систем
- » Развертывание частного Эфириума

В этой главе вам предлагаются краткий обзор интересных инноваций, которые реализованы на платформе облачного сервиса Azure корпорации Microsoft, а также рекомендации по использованию этих новых возможностей создания продуктов и служб для повышения эффективности своего бизнеса.

Материал этой главы поможет вам успешно конкурировать, плодотворно сотрудничать и эффективно обслуживать клиентов в самых широких, вплоть до глобальных, масштабах. Блокчейн-технология открывает совершенно новые рынки и меняет сложившиеся бизнес-модели. Корпорация Microsoft прикладывает максимум усилий, чтобы сделать эту технологию доступной и привлекательной для традиционного бизнеса.

В этой главе также рассказывается об инновационных блокчейн-мостах, которые могут быть построены с целью получения возможности соединять

и масштабировать уже существующие у вас системы. Вы узнаете, как можно развернуть собственный блокчейн в облачном сервисе Azure, и получите рекомендации относительно того, как в своем бизнесе сделать помещаемые в блокчейн-системы транзакции безопасными и не вызывающими споров.

Bletchley: модульная блокчейн-“материя”

Проект Bletchley имеет целью предоставление архитектурных строительных блоков корпоративным клиентам в пределах *консорциума блокчейн-экосистемы* (“консорциум” — новое название для блокчейнов, доступ к которым имеет лишь ограниченный круг участников). Блокчейн-платформа проекта Bletchley, получившая название *Fabric* (материал, ткань), опирается на сервис Azure, облачную вычислительную платформу от Microsoft. Проект Bletchley предусматривает следующее.

- » Цифровое свидетельство идентичности
- » Управление закрытыми ключами
- » Конфиденциальность клиентов
- » Защита данных
- » Администрирование операций
- » Системная совместимость

В проекте Bletchley сервис Azure обеспечивает для блокчейна облачный уровень, выступающий как платформа, для которой могут быть созданы и на которой будут выполняться приложения. Она будет доступна в 24 регионах в глобальном масштабе. Сервис Azure распространит свои традиционные преимущества — совместимость любых систем, обширный портфель сертификатов соответствия и защита на уровне предприятия, — на различные блокчейны. Корпорация Microsoft ставит своей целью упростить для существующих клиентов быструю адаптацию к блокчейн-технологии, особенно в строго контролируемых властями секторах, таких как здравоохранение, финансовые институты или государственные службы и учреждения.

На рис. 10.1 представлена структурная схема одного из продуктов проекта Bletchley — Blockstack Core v14, — реализующего новый децентрализованный “Интернет” без серверов, т.е. сетевое пространство, в котором пользователи размещают свои данные и приложения, выполняющиеся на их собственных виртуальных машинах, не нуждаясь в услугах серверов.

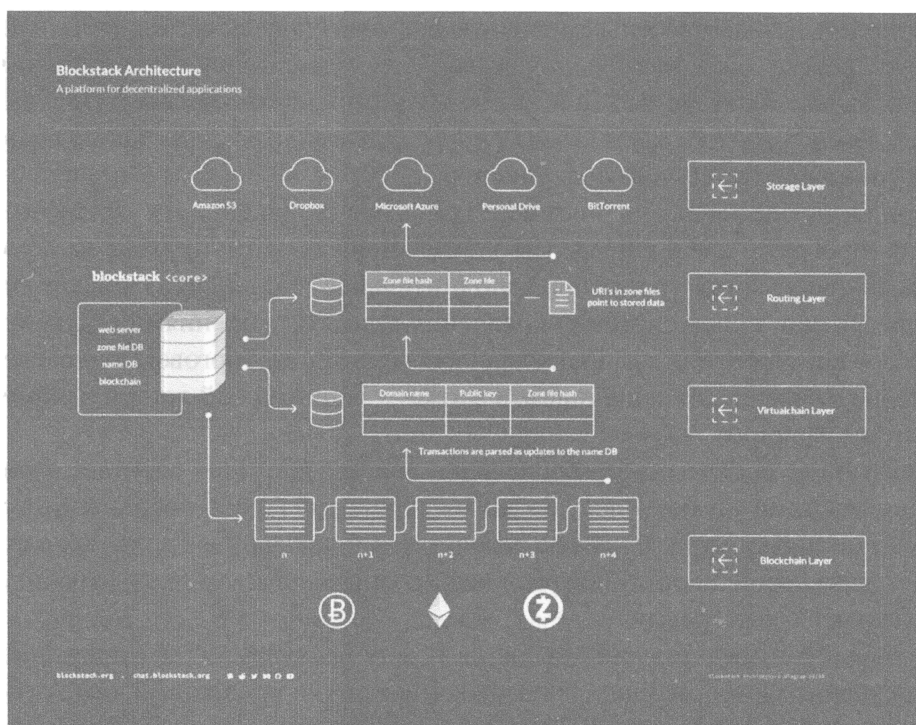


Рис. 10.1. Архитектура приложения Blockstack Core v14

Сервис Azure будет работать с несколькими различными блокчейн-протоколами. Все они являются частью проекта Hyperledger и основаны на модели отслеживания неизрасходованных транзакций (UTXO — unspent transaction output). Это означает, что платформа в среде Azure не будет использовать криптовалюты и за счет этого может быть более привлекательной для корпоративных клиентов. Также предусматривается интеграция с более сложными протоколами, включая Эфириум, в которых для обеспечения защиты сети используется криптовалюта.

Криплеты для шифрования и аутентификации

Проект Bletchley строится на двух основных элементах.

- » **Связующее программное обеспечение** (Blockchain middleware). Под этим понимаются облачное хранилище, контроль и обеспечение идентичности, аналитика, машинное обучение.
- » **Криплеты** (Cryptlet). Код, выполняющийся в безопасном контейнере и обеспечивающий совместимость и взаимодействие между сервисом Microsoft Azure, экосистемой проекта Bletchley и технологиями пользователей.

Криплеты создаются как компоненты вне кода блокчейна, могут быть написаны на любом языке, выполняются в защищенных контейнерах и осуществляют все взаимодействия по защищенным каналам. Криплеты могут использоваться в смарт-контрактах и UTXO-системах, когда необходима дополнительная функциональность или информация.

Криплеты обеспечивают мост через разрыв в защищенности между выполнением программ вне и в пределах блокчейн-экосистемы, приходя на помощь в тех случаях, когда требуется дополнительная защищенная информация. Они обеспечат вашей системе управления взаимоотношениями с клиентами (CRM — customer relationship management) или вашей торговой площадке соединение с облачным хранилищем, а затем — защищенный доступ, например, к системе Эфириум.

Связующее программное обеспечение проекта Bletchley работает в тандеме с криплетами и уже существующими сервисами Azure, подобными Active Directory или Key Vault, а также с экосистемами других блокчейн-технологий, представляя собой законченное решение, гарантирующее надежную работу вашей блокчейн-интеграции.

В табл. 10.1 представлены различия между оракулами (так принято называть источники информации для смарт-контрактов) и криплетами, как это было представлено на конференции Devcon 2 по проекту Bletchley.

Таблица 10.1. Криплеты и оракулы: сходства и различия

	Криплет	Оракул
Верификация требований	Требуется доверительная верификация с доверенным узлом (по каналам HTTPS) с использованием доверительного ключа криплета и доверительной анклавной подписи	Требуется доверительная, но неформальная верификация
Инфраструктура	Стандартная инфраструктура. Аппаратная изоляция и аттестация достигаются через анклав, доступные во всем мире в среде Azure. Программная среда для разработки ПО криплетов проекта Bletchley (Utility и Contract) общедоступна и позволяет быстро приступить к созданию и использованию криплетов	Настраиваемая инфраструктура. Написание ПО и его развертывание могут выполняться по отдельности. Установление доверия сложно осуществимо. Оракулы зависят от используемой платформы, а существующая на данный момент документация весьма фрагментарна

	Криплет	Оракул
Использование разработчиками	Допускается использование многих языков программирования, тип используемой в системе блокчейн-технологии безразличен	Привязан к используемому блокчейну, выбор языков программирования ограничен
Доступность торговой площадки	Для публикации и предоставления информации доступна торговая площадка	Нет общедоступной торговой площадки для публикации и предоставления информации

Криплеты создаются разработчиками и продаются на торговой площадке проекта Bletchley. В них предлагается множество различных наборов функций, которые могут быть полезны при построении распределенных приложений, использующих блокчейн-реестры. Этот рынок растет в соответствии с увеличением спроса со стороны пользователей, нуждающихся в определенной функциональности, такой как защищенное выполнение, интеграция, конфиденциальность, функции управления, совместимость и полный набор служб обработки данных.

Криплеты типа **Utility** и **Contract**, функция **CryptoDelegate**

В проекте Bletchley существует два типа криплетов.

- » **Utility.** Криплеты класса **Utility** обеспечивают шифрование, запись отметок времени, доступ к внешним данным и аутентификацию. Они делают транзакции более наполненными и надежными.
- » **Contract.** Криплеты класса **Contract** представляют собой инструменты полного делегирования. Они могут выполнять функции автономных агентов или ботов. Они обеспечивают всю ту логику выполнения, которая обычно осуществляется смарт-контрактами, но действуют вне экосистемы блокчейна.

Криплеты класса **Contract** привязываются к смарт-контрактам и создаются, когда соответствующий смарт-контракт публикуется. Они работают параллельно с вашей виртуальной машиной и обеспечивают большую производительность в сравнении с обычными смарт-контрактами, встроенными непосредственно в блокчейн, поскольку им не требуется никакой криптовалюты для выполнения. Этот класс криплетов наиболее привлекателен для пользователей блокчейнов, не использующих криптовалюту, когда информация в блокчейне и смарт-контракты подписываются доверенными сторонами.

На рис. 10.2 представлена схема взаимосвязей между контейнером криплета, защищенным каналом коммуникации и смарт-контрактом.

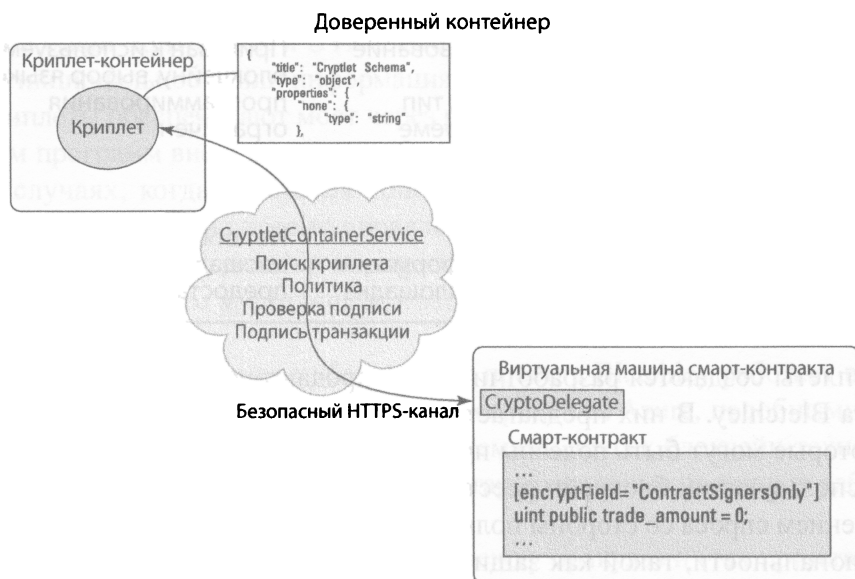


Рис. 10.2. Взаимодействие криплета в контейнере и смарт-контракта

Функция `CryptoDelegate`, выполняемая в виртуальной машине смарт-контракта (см. рис. 10.2), обеспечивает ей возможность взаимодействия с криплетами обоих классов — `Utility` и `Contract`. Эта функция действует как адаптер, обеспечивая виртуальной машине смарт-контракта своего рода “зацепки” для внешней функциональности, позволяющие ей из кода смарт-контракта обратиться к криплету, который, в свою очередь, создает защищенную и аутентичную оболочку для транзакций.

Создание приложений в экосистеме Microsoft Azure

Сервис Azure представляет собой цифровую экосистему и платформу для облачных вычислений. Он позволяет организациям устанавливать в облаке прямое соединение с их партнерами и приложениями SaaS¹. Такое решение позво-

¹ SaaS (software as a service — программное обеспечение как услуга) — это одна из форм облачных вычислений, при которой подписчикам предоставляется готовое прикладное программное обеспечение, полностью обслуживаемое поставщиком. Доступ к этому ПО обычно предоставляется через мобильное приложение или веб-браузер. — *Примеч. ред.*

ляет организациям передавать свои и получать ответные данные надежным и защищенным образом.

Облачная платформа Azure от Microsoft является второй по размеру инфраструктурой, используемой как платформа услуг IaaS. Это надежные и безопасные “небеса” для ваших облачных вычислений и хранилищ данных. В системе Azure имеется сервис, получивший название “ExpressRoute” и предоставляющий потребителям способ прямого подключения к ее облачным сервисам. А это, в свою очередь, позволяет избежать проблем с производительностью и безопасностью, столь характерных для открытого Интернета.

В 2015 году корпорация Microsoft приняла решение расширить экосистему сервиса Azure в направлении интеграции с блокчейн-системой Эфириум и поддержки решений проекта Hyperledger. Первая законченная разработка предлагается потребителям под названием “Azure Blockchain” и представляет собой службу, поддержку которой обеспечивает система Эфириум. Для создания приложений клиентам в системе Эфириум предоставляется полная по Тьюрингу среда разработки блокчейн-решений. Корпорация Microsoft предполагает разработку новых предложений, построенных на основе блокчейн-технологии и проектов консорциума Hyperledger. Она также расширяет торговую площадку Azure, намереваясь со временем преобразовать ее в портал для клиентов сервиса Azure.

Расширение от Microsoft для сервиса Azure, получившее название “Azure Stack” и предназначенное для предоставления инфраструктуры и платформы как услуги (IaaS), включает шаблоны быстрого запуска Azure (Azure Quickstart Templates). С помощью приложения Azure Resource Manager эти шаблоны обеспечивают разворачивание различных ресурсов Azure с целью сократить объем выполняемых работ. Приложение Azure Resource Manager позволяет клиентам работать с их бизнес-ресурсами как с группой. Оно позволяет скоординированно разворачивать, удалять или обновлять все ресурсы в отдельном решении посредством единственной операции.

Шаблоны быстрого запуска Azure могут работать в различных операционных средах, таких как разработка, установка и тестирование. Благодаря приложению Azure Resource Manager клиенты получают необходимые функциональные возможности для маркировки, аудита и защиты ресурсов. Эти функции помогают клиентам управлять своими ресурсами после их развертывания.

Вкладом корпорации Microsoft в проекты консорциума Bletchley является ее блокчейн-архитектура, соединенная с уже устоявшимися корпоративными технологиями, которые эта корпорация предлагает своим клиентам. В результате сервис Azure превратился в платформу поддержки блокчейн-технологии и соответствующую торговую площадку.

Экосистема консорциума Bletchley основана на подходе, выбранном корпорацией Microsoft для того, чтобы сделать блокчейн-технологии и сети

распределенных реестров доступными для самой широкой аудитории, одновременно обеспечив их высокую защищенность и эффективность. Главная цель Microsoft — оказать помощь своим клиентам в создании аутентичных решений их актуальных бизнес-проблем.

ВЫБИРАЕМ ШАБЛОН

Шаблоны быстрого запуска — это инструмент, который был разработан с целью упростить пользователям проекта Bletchley задачу развертывания закрытой блокчейн-группы. Сейчас существует уже порядка дюжины блокчейн-шаблонов, которые позволяют быстро разворачивать блокчейн-приложения в среде Azure. В будущем подобных шаблонов будет доступно, безусловно, больше.

Закрытая версия системы Эфириум является одним из наилучших решений для автоматизации всей процедуры. Этот шаблон предоставляет пошаговую процедуру, по ходу выполнения которой вы сможете выбрать членов создаваемого консорциума, определить количество узлов сети, которое будет в распоряжении каждого участника, а затем географически распределить эти узлы, используя облачный сервис Azure для повышения устойчивости системы.

Начинаем работу с Chain в Azure

Технология Chain, предоставляющая доступ к решениям блокчейн-технологии, доступна в виде среды разработки Chain Core Developer Edition на платформе Azure. Приложение Chain Core Developer Edition является ПО с открытым кодом и представляет собой бесплатную версию платформы распределенного реестра корпоративного уровня. Оно позволит вам выпускать, а также перемещать цифровые активы в авторизованных блокчейн-сетях.

Воспользовавшись тестовой сетью этой платформы, ваши разработчики смогут присоединиться к существующей или запустить собственную блокчейн-сеть, получить доступ к учебным материалам и технической документации, а также создать собственные финансовые приложения. Также они смогут запустить их собственные прототипы в тестовой сети Chain или создать их собственную личную сеть в облачном сервисе Azure.

Установка среды программирования Chain

Среда программирования Chain Core Developer Edition включает примеры кода, набор средств разработки (SDK) для языка Java и руководства для

начинающих. Кроме того, она поставляется с аналитической панелью и инсталляторами для платформ Linux, Mac и Windows.

Для установки на своем компьютере среды разработчика Chain Core Developer Edition выполните следующие действия.

1. **Зайдите на страницу установки приложения:** <https://chain.com/docs/core/get-started/install>.
2. **Выберите вариант для своей операционной системы.**
3. **Щелкните на кнопке Download.**
4. **Откройте программу Chain.**
5. **Запустите установщик Chain Core installer.**

Технология Chain имеет собственный набор средств разработки (SDK), предоставляющий разработчикам инструменты создания ПО, позволяющие создавать блокчейн-приложения и активы.

Создание собственной закрытой сети

В облачном сервисе Azure можно создать собственную закрытую блокчейн-сеть консорциума Эфириум. Вы вполне сможете сделать это самостоятельно, не обращая за помощью к профессиональным разработчикам. Просто выполните следующие действия.

1. **Создайте новую или воспользуйтесь существующей учетной записью в Azure для входа в эту систему.**

У вас будет возможность воспользоваться бесплатной пробной версией и вариантом поэтапной оплаты, что очень упрощает задачу попробовать, как это работает в облачном сервисе Azure.

2. **Откройте в браузере страницу <https://goo.gl/Ixu5of>.**
3. **Щелкните на кнопке Deploy to Azure.**



ВНИМАНИЕ!

Шаблоны приложения Azure Resource Manager были созданы в личном порядке членами сообщества Azure. Корпорация Microsoft не дает никаких гарантий в отношении их защищенности, совместимости или производительности.

4. **Заполните предложенную форму.**
5. **Щелкните на кнопке Purchase.**

Поздравляю! Теперь у вас есть собственная закрытая блокчейн-сеть консорциума Эфириум.

Использование финансовых служб Chain в Azure

Технология Chain реализована как ПО с открытым кодом в виде бесплатной платформы для разработчиков. Она включает тестовую сеть, работа которой поддерживается корпорацией, платформу Chain и платформу Initiative for Cryptocurrencies and Contracts (Инициатива по криптовалютам и контрактам), сокращенно — “3CI”. В настоящее время 3CI является платформой, развернутой на платформе Chain, которая предоставляет разработчикам решения блокчейн-технологии и реализована в виде среды разработки Chain Core Developer Edition.

Эта платформа позволяет выпускать и перемещать цифровые активы в авторизированной блокчейн-сети. В ее создании принимали участие многие ведущие финансовые компании и команда разработчиков проекта Chain. С помощью среды разработки Chain Core можно разрабатывать различные финансовые приложения.

На этой платформе планируется реализовать многие инновационные продукты. В их число входят платежные системы, банковские решения, страхование и рынки капитала. Кроме того, корпорация Visa установила партнерские отношения с командой Chain с целью разработки защищенной, быстрой и простой в использовании системы обработки платежей B2Bin (business-to-business), способной охватить весь мир.

Развертывание блокчейн-инструментов в Azure

Облачный сервис Azure включает и несколько других полезных реализаций блокчейн-технологии, а также инструментов, которые могут оказаться вам полезными. В этом разделе речь пойдет о четырех основных блокчейн-инструментах и проектах, включая реализацию в Azure доступа к системе Эфириум, проект Cortana (аналитический инструмент, использующий машинное обучение), инструмент визуализации данных в среде Azure Power BI и инструмент Active Directory (AD) этого облачного сервиса. Последние три не являются непосредственно блокчейн-приложениями, но могут использоваться в любых блокчейн-проектах на платформе Azure.

В этом разделе вы найдете рекомендации в отношении того, что можно создать на платформе Azure и какие имеются инструменты, позволяющие сделать свои проекты успешными.

Использование Эфириума в Azure

В настоящее время блокчейн системы Эфириум уже доступен на платформе Microsoft Azure в качестве сервиса. Эта инициатива была предложена компанией ConsenSys и корпорацией Microsoft как партнерское решение. Этот уже

реализованный проект получил название “Solidity” и позволяет желающим начать построение собственных децентрализованных приложений в среде системы Эфириум. Более подробную информацию вы найдете на странице <https://marketplace.visualstudio.com/items?itemName=ConsensSys.Solidity>.

Использование блокчейна системы Эфириум как службы (EaaS) позволяет корпоративным разработчикам и клиентам создавать в облачном сервисе блокчейн-среду, которая может быть развернута буквально одним щелчком мышью.

При развертывании блокчейна Эфириум на платформе Azure вам изначально предложат два инструмента.

- » **BlockApps.** Это полужакрытая или закрытая блокчейн-среда в системе Эфириум.
- » **Ether.Camp.** Встроенная среда разработчика.

Вариант BlockApps также может быть развернут как открытая среда в системе Эфириум. Все эти инструменты обеспечивают быструю разработку приложений на основе смарт-контрактов.

Эфириум — это гибкая открытая система, которая может быть настроена так, чтобы соответствовать различным нуждам отдельных пользователей. Подробно о системе Эфириум рассказывается в главе 5.

Cortana: аналитический инструмент машинного обучения

Сервис Cortana — это мощный аналитический инструмент, использующий методы машинного обучения и развернутый в облачном хранилище. Этот полностью управляемый облачный сервис предоставляет пользователям возможность легко и быстро создавать, настраивать и совместно использовать прогностические аналитические решения, обеспечивающие их создателям много преимуществ.

Воспользовавшись аналитической информацией, предоставленной службой Cortana Intelligence, вы сможете предпринять необходимые действия раньше, чем ваши конкуренты, опираясь на предсказания о предстоящем развитии событий. Это гибкое и быстродействующее программное обеспечение позволит вам уверенно принимать быстрые решения, соответствующие вашим конкретным нуждам.

Помимо прочего, аналитический инструмент Cortana learning является надежным, защищенным и масштабируемым. Он предоставляет ценные сведения, безотносительно к сложности и объему исходных данных. И, самое главное, сервис Cortana позволяет взаимодействовать со смарт-агентами, что позволит вам стать ближе с вашими клиентам более естественным, практическим и полезным образом. Инструмент Cortana Intelligence Suite будет полезен

в различных секторах экономики, включая производство, финансовые службы, розничную торговлю и здравоохранение.

Визуализация данных посредством Power BI

Инструмент Power BI, предложенный корпорацией Microsoft, представляет собой мощный сервис, развернутый в облачной системе Azure. Он работает со всеми новейшими сервисами и инструментами бизнес-аналитики от Microsoft. Этот инструмент поможет тем, кто занят анализом данных, визуализировать свои результаты и делиться идеями, возникшими в результате изучения данных их организаций.

Курс обучения визуализации в Power BI, доступный в системе бесплатного онлайн-обучения edX, является частью программы профессиональной сертификации в науке о данных от Microsoft. Эта облачная служба быстро набирает популярность среди профессионалов в области науки о данных.

Инструмент Power BI помогает получить доступ и визуализировать свои данные. Изучающие курс визуализации в Power BI учатся тому, как получить доступ, импортировать, преобразовать и графически представить имеющиеся данные для бизнес-исследований. Кроме того, в этом курсе объясняется, как создавать аналитические панели и предоставлять их в распоряжение бизнес-пользователей на мобильных устройствах и в Интернете.

Управление доступом в Azure с использованием Active Directory

Служба Azure Active Directory (AD) представляет собой решение для организации широкого доступа и управления свидетельствами подлинности. Она предоставляет широкий набор функциональных возможностей, позволяющих контролировать доступ к облачной среде и находящимся в ней внутренним ресурсам и приложениям. К последней категории относятся различные сетевые сервисы от Microsoft, такие как Office 365, а также многочисленные SaaS-приложения от сторонних разработчиков.

Одним из важнейших свойств службы Azure AD является то, что вы можете управлять доступом к ее ресурсам. Эти ресурсы могут быть во внешних каталогах, как в случае приложений программного обеспечения как услуги (SaaS), внутренних ресурсов или сайтов SharePoint и служб сервиса Azure, либо во внутренних каталогах, как в случае разрешений на манипулирование объектами посредством ролей каталога.



Глава 11

Выясняем возможности платформы IBM Bluemix

В ЭТОЙ ГЛАВЕ...

- » Знакомимся с блокчейн-приложениями искусственного интеллекта
- » Строим собственную среду IBM Fabric
- » Создаем смарт-контракты
- » Разворачиваем решения для Интернета вещей

В этой главе рассказывается об инициативах корпорации IBM в отношении блокчейн-технологий. В частности, в IBM было принято решение связать данные технологии с другими новаторскими технологиями этой корпорации, такими как Bluemix (полномасштабная платформа для построения приложений, предоставляемая как сервис (PaaS — Platform as a Service)) и Watson (платформа, представляющая собой интегрированную вычислительную среду, подобную суперкомпьютеру).

Блокчейн-технология позволяет организовать практически беспрепятственный обмен ценностью, а искусственный интеллект обеспечивает ускорение анализа значительных объемов данных. Слияние этих двух новаторских решений может привести к изменению самой парадигмы и оказать существенное влияние на те методы, которыми сейчас ведется бизнес и осуществляется защита связанных между собой электронных устройств.

Если в сферу ваших интересов входит Интернет вещей (IoT), здравоохранение, задачи организации хранения и транспортировки или решение проблем логистики, вам будет полезна информация, которую вы получите, прочитав эту главу. Также, если вы предприниматель и хотели бы узнать больше о новых возможностях, возникающих за счет интеграции искусственного интеллекта и технологии блокчейна на платформе создания масштабируемых приложений, эта глава, безусловно, будет для вас полезна.

Бизнес-блокчейны в среде Bluemix

В настоящее время корпорация IBM предлагает решения блокчейн-технологии, интегрированные с ее традиционными разработками, такими как платформа Bluemix. По своей сути Bluemix является реализованной по облачной технологии платформой PaaS с открытыми стандартами, предназначенной для создания и управления приложениями, которую в IBM интегрировали с пакетом блокчейн-решений от Hyperledger — консорциума, входящего в состав Linux Foundation и имеющего целью всемерное развитие и популяризацию блокчейн-технологии.

Вам следует быть готовыми к быстрым и фундаментальным изменениям в блокчейн-инициативах от IBM. Эта технология еще совершенно новая и проходит лишь начальный этап своего развития как в корпорации IBM, так и в консорциуме Hyperledger.

У консорциума Hyperledger в стадии разработки находится несколько различных подпроектов. На момент написания этих строк в IBM использовали платформу Fabric, но вполне вероятно, что платформа Bluemix будет открыта и для других решений. Проект Fabric имеет открытый код и в консорциуме Hyperledger пока находится в стадии активной разработки. Он еще не совсем готов для коммерческих целей — по крайней мере так было на момент написания этих строк.

Вы можете начать тестировать Fabric в среде Bluemix, воспользовавшись версией ПО Hyperledger Fabric v0.6. Однако в IBM предупреждают о необходимости воздержаться от проведения реальных транзакций с активами, используя ПО Fabric версии v0.6 или более ранних.

Ваша собственная изолированная среда

Платформа Bluemix — это новейшее решение в облачных технологиях, предлагаемое корпорацией IBM. Это реализация открытой облачной архитектуры IBM, построенная на платформе Cloud Foundry, представляющей собой реализацию концепции PaaS с открытым кодом.

Платформа Bluemix позволяет сначала быстро и просто создавать собственные приложения, а затем разворачивать их и управлять ими. Платформа Bluemix предлагает сервисы корпоративного уровня, которые можно интегрировать с приложениями без необходимости знать, как их следует устанавливать или настраивать в этой среде.

На рис. 11.1 показано, как на этой платформе увязываются различные аспекты блокчейна и элементы системы от IBM. Подробнее об этом можно прочитать на странице <https://goo.gl/12Q6no>.

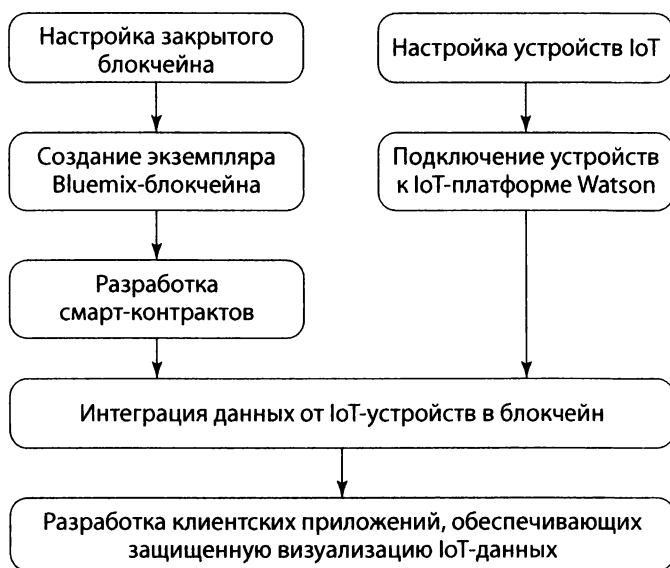


Рис. 11.1. Слияние IBM-платформ Bluemix и Watson для работы с Интернетом вещей (IoT)

Платформа IBM Bluemix предоставляет следующие четыре основных элемента.

- » Вычислительную инфраструктуру, основанную на архитектурных решениях, необходимых для ваших приложений.
- » Возможность разворачивать приложения в открытом облаке Bluemix либо в выделенном облаке.

- » Предоставление основных инструментов, таких как редакторы или компоновщики кода.
- » Доступ в разделе сервисов к инструментам с открытым кодом от сторонних разработчиков.

Как видите, на платформе Bluemix вам предоставляется все, что необходимо для создания собственных приложений. А в настоящее время у вас уже даже имеется возможность протестировать инфраструктуры, создаваемые на основе блокчейн-технологии.

Также в системе существует сервис, предназначенный для интеграции ваших приложений с блокчейном Bluemix. Сообщается, что в этом случае возможны две модели оплаты. Бесплатная учетная запись предоставит в ваше распоряжение все, что требуется для тестирования имеющихся у вас идей. Вы получите четыре узла-участника и право подписи транзакций, а также информационную панель с журналами, элементами управления и доступом к API. Также в вашем распоряжении будет несколько примеров приложений с открытым кодом, с которыми можно будет экспериментировать. Корпоративный план предполагает ежемесячную оплату в размере 10 тысяч долларов и предлагает более высокий уровень защищенности и быстродействия по сравнению с бесплатным вариантом.

Примеры использования Bluemix

Из пионеров использования технологий Bluemix и Hyperledger Fabric следует упомянуть двух интереснейших представителей.

- » **Wanxiang.** Крупнейшая китайская компания, выпускающая автомобильные комплектующие Wanxiang, сотрудничает с корпорацией IBM в вопросе развертывания закрытого корпоративного блокчейна. В этой компании возникла идея внедрить права собственности в такие вещи, как электроавтомобили. Целью является сокращение издержек потребителей на лизинг оборудования. Компания Wanxiang намеревается использовать блокчейн-технологии для отслеживания сроков службы компонентов и восстановления использованных батарей. Платформа Bluemix возьмет на себя заботу обо всем остальном.
- » **КУСКИ.** Стартап КУСКИ, работающий в сфере финансовых технологий, использует интеграцию в блокчейн IBM как новый способ реализовать правило “знай своего клиента” (KYC) для компаний, которые оказывают брокерские услуги. Связанные с этим требованием расходы весьма обременительны и являются ограничивающим фактором для банков и других финансовых служб. Правила

КУС предназначены для предотвращения отмыwania денег и незаконной торговли, а также как одна из мер борьбы с терроризмом. Усилиями стартапа КУСК! была создана платформа для проведения видеоконференций и предоставления зашифрованных документов. Ее назначение — обеспечить брокерам возможность работать и проводить аутентификацию клиентов, с которыми они лично не встречались.

В корпорации IBM также были созданы три простых блокчейн-приложения, которыми можно воспользоваться, чтобы на практике опробовать работу ее блокчейн-сети.

- » **Marbles.** Это приложение, которое демонстрирует передачу стеклянных шариков между двумя пользователями. Его назначение — помочь вам понять, как в блокчейне осуществляется перемещение активов.
- » **Commercial Paper.** Приложение Commercial Paper (коммерческие бумаги) представляет собой торговую блокчейн-сеть, реализованную в блокчейн-реестре корпорации IBM. Вам предоставляется возможность создавать новые коммерческие бумаги, которые затем можно будет выставлять на продажу, а также покупать и продавать бумаги других торговцев и проводить аудит состояния сети.
- » **Car Lease.** Приложение Car Lease во многом напоминает приложение Marbles. Оно создано, чтобы предоставить вам возможность манипулировать активами. Активы в блокчейне можно создавать, обновлять и передавать. Приложение также позволяет наблюдать за событиями в сети с третьей стороны.

Умный блокчейн в системе Watson

Суперкомпьютерная платформа Watson корпорации IBM также доступна на платформе Bluemix. Платформа Watson представляет собой компьютерную самообучающуюся вычислительную систему искусственного интеллекта, способную анализировать структурированные и, что еще более впечатляет, неструктурированные данные с невероятной скоростью.



ВНИМАНИЕ!

Эта технология все еще находится в стадии разработки, и пользователи неоднократно высказывали сомнения в ее истинных способностях распознавать неструктурированный письменный язык.

Система Watson способна дать ответ на вопросы, заданные ей обычным языком, и продолжает свое обучение по мере получения новой информации.

Последствия слияния этой технологии с блокчейн-технологией просто поражают. Одна из первых реализаций такого единения имела место в экосистеме Интернета вещей (IoT). Здесь существует жесткая необходимость защиты данных, поступающих от подобных устройств, а также потребность сделать полученную информацию действенной и понятной.

Когнитивные вычисления в среде Watson имитируют процессы мышления человека и осуществляются с использованием протокола MQTT. Как и в случае мышления человека, их интенсивность растет с течением времени. Эти самообучающиеся системы используют методы добычи данных, распознавания шаблонов и распознавания естественного языка для имитации методов работы нашего мозга. Платформа Watson позволяет проводить расчеты со скоростью более 80 терафлоп/с (один терафлоп/с — это триллион, т.е. 10^{12} , операций с плавающей точкой в секунду). Чтобы было понятнее, такая скорость расчетов позволяет повторить (а в некоторых случаях и превзойти) способность отвечать на вопросы человека с хорошей реакцией и высоким уровнем трудоспособности. Супервычислитель платформы Watson способен делать это, обращаясь к 90 серверам, на которых размещено комбинированное хранилище данных, содержащее более 200 миллионов страниц информации, которую он обрабатывает, руководствуясь 6 миллионам логических правил. Суперкомпьютер Watson по размеру равен примерно 10 холодильникам, но его размеры постепенно уменьшаются, а скорость работы возрастает. На рис. 11.2 представлено, как платформа Watson связана с различными аспектами блокчейна и других подсистем корпорации IBM. Подробнее об этом рассказывается на странице <https://goo.gl/12Q6no>.

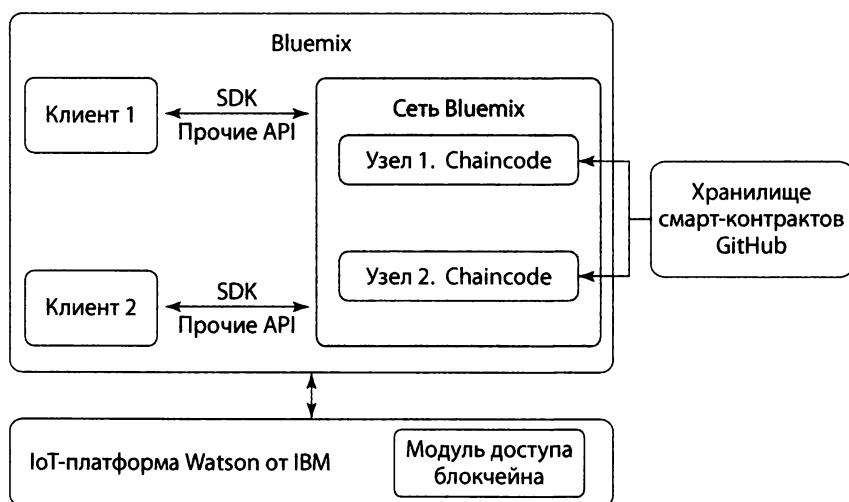


Рис. 11.2. Интеграция клиентов, узлов и платформы Watson в сервисе Bluemix от IBM

Все эти потрясающие возможности корпорация IBM применяет к потокам данных из Интернета вещей (IoT), которые затем используются для реализации функций смарт-контрактов Chaincode. Технология Chaincode — это система построения смарт-контрактов консорциума Hyperledger. Ниже поясняется, как блокчейн-сервис на платформе Watson работает с IoT-устройствами.

- » Данные из IoT-устройств отправляются в закрытый блокчейн-реестр пользователя для включения в транзакции, оформляемые в виде защищенных от несанкционированного доступа записей с временной отметкой.
- » Партнеры и провайдеры сторонних услуг также могут получать доступ к IoT-данным или же предоставлять их без необходимости централизованного контроля и управления.
- » Все стороны могут подписывать и проверять данные, что снижает возможность их оспаривания и гарантирует, что каждый партнер будет нести ответственность за свои индивидуальные действия.

Это очень простая реализация, которая не использует в полном объеме те преимущества, которые обеспечивают все функциональные и прочие возможности платформы Watson. Способность вычислительной среды этой платформы обучаться и вносить предложения, а также обновлять устаревшую информацию в будущем сделает платформу Watson поистине мощным инструментом для создания блокчейн-приложений.

Существует возможность интеграции IoT-платформы сервиса Watson с платформой Fabric консорциума Hyperledger. Такая интеграция позволит создавать смарт-контракты типа Chaincode с использованием в них оракулов с когнитивными вычислениями. IoT-платформа сервиса Watson включает встроенную функциональность, позволяющую добавлять выбранные IoT-данные в ваш закрытый блокчейн с целью построения оракулов. Такой подход позволяет защитить данные от просмотра неавторизованной третьей стороной.

После установки и развертывания рабочей среды Bluemix у вас появится возможность добавить в приложения нужные вам сервисы, включая IoT-платформу, в которую уже интегрировано несколько технологий. Технология Fabric является блокчейн-технологией, предоставляющей инфраструктуру закрытого блокчейна распределенным одноранговым узлам, которые копируют данные с устройств и проверяют транзакции через защищенные контракты.

На IoT-платформе Watson все данные, поступившие от одного или более типов устройств, преобразуются в формат, предусмотренный API соответствующих смарт-контрактов. Также на этой платформе все нерелевантные данные от устройств отфильтровываются и смарт-контрактам пересылается только требуемая им информация. На рис. 11.3 показано, как платформа IBM Watson

интегрируется с IoT-устройствами и API. В этом случае служба Watson действует как оракул в контрактах типа Chaincode, позволяя разработчику контролировать, какая именно информация будет предоставлена сторонам, участвующим в контракте. Эта функциональная возможность очень важна для соблюдения конфиденциальности.

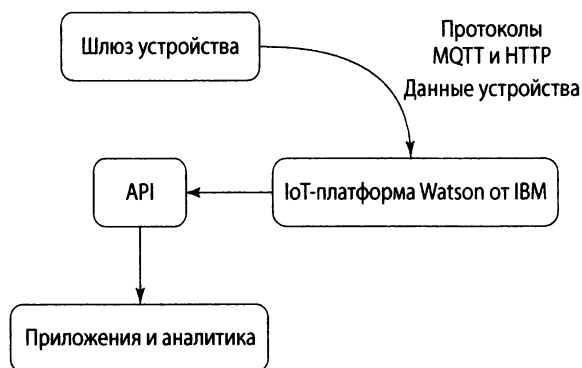


Рис. 11.3. Поток данных между средой Watson, API и устройствами

Построение собственной стартовой сети в Big Blue

Блокчейн-технология корпорации IBM и ее IoT-платформа предлагают новые перспективные инструменты, которые могут использоваться для решения важных проблем, встающих перед растущими и развивающимися компаниями.

- » **Защита.** Громадный объем данных, поступающих от миллионов устройств, резко усугубляет проблемы конфиденциальности информации. Кроме того, взломанные хакерами IoT-устройства уже использовались вредоносными организациями для нарушения работы веб-сайтов посредством организации распределенных DoS-атак (Denial of Service — отказ в обслуживании).
- » **Стоимость.** Большой объем сообщений, поступающих от устройств данных, и интенсивность процедур их анализа неуклонно возрастают с увеличением количества устройств, подключаемых к сети и использующих эти данные.
- » **Архитектура.** Централизованные облачные платформы становятся узким местом в любых сквозных IoT-решениях, а также неизбежно превращаются в главную цель для возможных атак.

Распределенные IoT-сети IBM, построенные на открытых стандартах, позволяют успешно решать многие проблемы, связанные с характерной для сегодняшних дней высокой централизацией IoT-решений, основанных на облачной технологии. Подключаемые устройства взаимодействуют непосредственно с распределенными реестрами, после чего поступившие от них данные могут использоваться третьей стороной для выполнения смарт-контрактов, что уменьшает необходимость прямого человеческого вмешательства.

IoT-платформа Watson от IBM, интегрированная с технологией Fabric, позволяет помещать поступающие данные непосредственно в закрытую блокчейн-сеть, что исключает необходимость централизованного сбора и хранения всех поступающих IoT-данных. Децентрализованная блокчейн-сеть также повышает защищенность IoT-устройств. Со временем для каждого из устройств будут созданы уникальные цифровые свидетельства идентичности. Такой новый подход к созданию и защите свидетельств идентичности чрезвычайно усложнит возможность их подделки.

Эти помещенные в блокчейн свидетельства идентичности позволяют IoT-устройствам подписывать транзакции, разрешая тем самым выполнение смарт-контрактов. Практическим применением данного подхода может быть страховой полис, который получает от IoT-автомобиля информацию о практике вождения различных лиц. Автомобиль сможет отправлять эти данные для публикации в блокчейн-среде технологии Fabric, а страховое свидетельство, оформленное в виде смарт-контракта типа Chaincode, сможет распознавать новые данные, пользуясь цифровым свидетельством идентичности автомобиля, и обновлять статистику полиса.

Новые возможности практически безграничны, и развитие Интернета вещей открывает широкие перспективы для бизнесменов и их клиентов или потребителей услуг в таких областях, как здравоохранение, организация складов, транспортировка грузов и логистика.

Существует три основных уровня облачных IoT-решений от IBM, которые отвечают нуждам различных задач IoT-бизнеса.

- » **Шлюзы устройств.** Шлюзы устройств используются в умных устройствах или сенсорах, собирающих определенные данные об окружающем физическом мире. Это могут быть датчики показателей погодных условий, контроллеры температуры в охлаждаемых контейнерах, измерители показателей жизнедеятельности пациентов. IoT-устройства этого типа отправляют собранные ими данные через Интернет для последующего анализа и обработки.
- » **IoT-платформа Watson от IBM.** На этом уровне корпорация IBM комбинирует с IoT-платформой свой суперкомпьютер, что позволяет

собирать данные от IoT-устройств, а затем анализировать их и принимать необходимые действия для решения возникших проблем. Сервис Watson предоставляет функции машинного обучения, машинных рассуждений, обработки естественного языка и анализа изображений, повышающие возможности обработки неструктурированных данных, поступивших от датчиков и сенсоров.

- » **Платформа IBM Bluemix.** Платформа Bluemix представляет собой облачную среду, базирующуюся на открытых стандартах и предназначенную для создания, выполнения и управления приложениями и сервисами. Она поддерживает IoT-приложения, упрощая включение в них аналитических и когнитивных возможностей.

Создать и настроить собственную структуру в блокчейн-среде IBM очень просто. Вам даже не придется обращаться за помощью к разработчикам! Как только настройка созданного вами блокчейна будет закончена, вы сможете интегрировать его с IoT-платформой Watson. Просто выполните следующие действия — и уже через несколько минут у вас будет готовое и функционирующее решение.

1. На аналитической панели своей учетной записи Bluemix щелкните на ссылке **Use Services or APIs (Использовать сервисы или API)**.
2. В каталоге сервисов, в разделе **Application Services (Сервисы приложений)**, щелкните на ссылке **Blockchain**.
3. Проверьте и уточните значения параметров создаваемого блокчейна.
 - **Выбранное пространство.** Если у вас вариантов больше, чем единственное пространство, выделяемое по умолчанию, убедитесь, что создаваемый сервис будет помещен именно в желаемое пространство.
 - **Параметры приложения.** Оставьте приложение неограниченным.
 - **Имя создаваемого сервиса.** Измените предложенное по умолчанию название на что-нибудь такое, что вам будет проще запомнить.
 - **Вариант плана.** Выберите бесплатный вариант плана.

4. Щелкните на кнопке **Create**.

Для вас будет создан блокчейн, размещенный на платформе Bluemix, и после его инициализации в ваше распоряжение будут переданы два равноправных узла.

Следует отметить, что у разработки экономичных IoT-приложений на основе блокчейна огромный потенциал. Распределенные реестры с внедренными в них смарт-контрактами могут обеспечить более высокий уровень защиты и доверительности, обеспечивая при этом возможность автоматизации процессов. Использование IoT-платформы Watson можно комбинировать с использованием

блокчейн-сервисов платформы Bluemix, получив в результате готовую к развертыванию платформу для IoT-приложений блокчейн-технологии, построенную на открытых стандартах.



СОВЕТ

Разработка и тестирование подобных приложений не составляет большой сложности, но, весьма вероятно, вам все же потребуется поддержка профессиональных разработчиков.

Для настройки своего первого проекта выполните следующее.

1. Настройте инфраструктуру своего закрытого блокчейна на платформе Bluemix.

Для настройки параметров интеграции своего закрытого блокчейна в блокчейн-сервисы платформы IBM вам потребуется помощь разработчика.

2. Создайте и разверните в блокчейне смарт-контракты, оперирующие данными от устройств.

Подходящим примером в этом случае может быть контракт, предусматривающий изменение стоимости доставки товаров, если она была выполнена с опозданием по отношению к установленному сроку.

3. Подключите свои устройства к IoT-платформе Watson корпорации IBM.

Лучше, если подключение шлюзов сенсоров к IoT-платформе Watson будет выполнено своими разработчиками. Когда эта работа будет выполнена, IoT-устройства начнут посылать данные, которые после получения должны быть отфильтрованы, обобщены и записаны в ваш блокчейн.

4. Интегрируйте данные своих IoT-устройств в распределенный реестр блокчейна.

Поручите разработчикам провести интеграцию устройств с IoT-платформой Watson таким образом, чтобы можно было отправлять данные в блокчейн-службы IBM, функционирующие на платформе Bluemix.

5. Установите пользовательский интерфейс для мониторинга.

- Активизируйте блокчейн на вкладке Settings (Настройки).
- Настройте соединение со службой Blockchain (Блокчейн).
- Щелкните на кнопке Add (добавить) и в открывшемся окне укажите сведения, необходимые службе Blockchain.
- Подтвердите все внесенные вами изменения.
- Откройте меню блокчейна, чтобы связать его со своими данными. Возможно, здесь вам потребуется помощь разработчика.
- Далее следуйте указаниям мастера настройки, последовательно вводя всю требуемую информацию, чтобы завершить связывание данных от устройств с контрактом в блокчейне.

6. Разблокируйте идентификатор в Chaincode.

Когда данные начнут поступать в реальном времени, смарт-контракты будут выполняться в соответствии с поступившими данными. Исходя из полученных результатов транзакция будет завершена и записана в цифровой реестр, а затем сведения о ней будут разосланы всем участвующим в контракте сторонам.

7. Создайте клиентское приложение для конечных пользователей.

В настоящее время еще предстоит преодолеть некоторые проблемы, существующие как в системе от IBM, так и в ранних блокчейн-разработках для Интернета вещей. Дело в том, что многие уже существующие IoT-устройства имеют ограниченную вычислительную мощность или с трудом поддаются модификации. Кроме того, процедуры шифрования и проверки данных требуют определенных затрат энергии, что может вызвать проблемы со сроком службы батарейки устройств.

Вот теперь вы можете создать собственный контракт класса Chaincode. Возможно, вам вновь потребуется помощь разработчика, поскольку эта процедура предполагает обращение к сайту GitHub и использование языка программирования Go. Вот краткий общий обзор всей процедуры, который поможет вам правильно оценить, что именно требуется для реализации проекта такого типа.

1. Создайте проект на сайте GitHub.

Именно здесь будут храниться созданные вами смарт-контракты.

2. Настройте локальную среду разработки и тестирования проекта Hyperledger.

Вам потребуется установить на свой компьютер несколько приложений, включая Docker, Pip, клиент Git, язык Go и Xcode (для пользователей Mac). Описание настройки приложения Docker вы найдете в главе 3.

3. Загрузите образец смарт-контракта от IBM.

Этот этап необязателен, но он позволяет сделать процедуру создания вашего первого контракта существенно проще.

4. Создайте тестовый смарт-контракт.

5. Создайте исполнительные файлы вашего контракта.

Ваш контракт должен быть помещен в исполняемый код. Образец контракта от IBM включает все элементы, необходимые для любого контракта.

6. Проверьте работу контракта в песочнице проекта Hyperledger.

7. Выложите контракт на сайт GitHub.



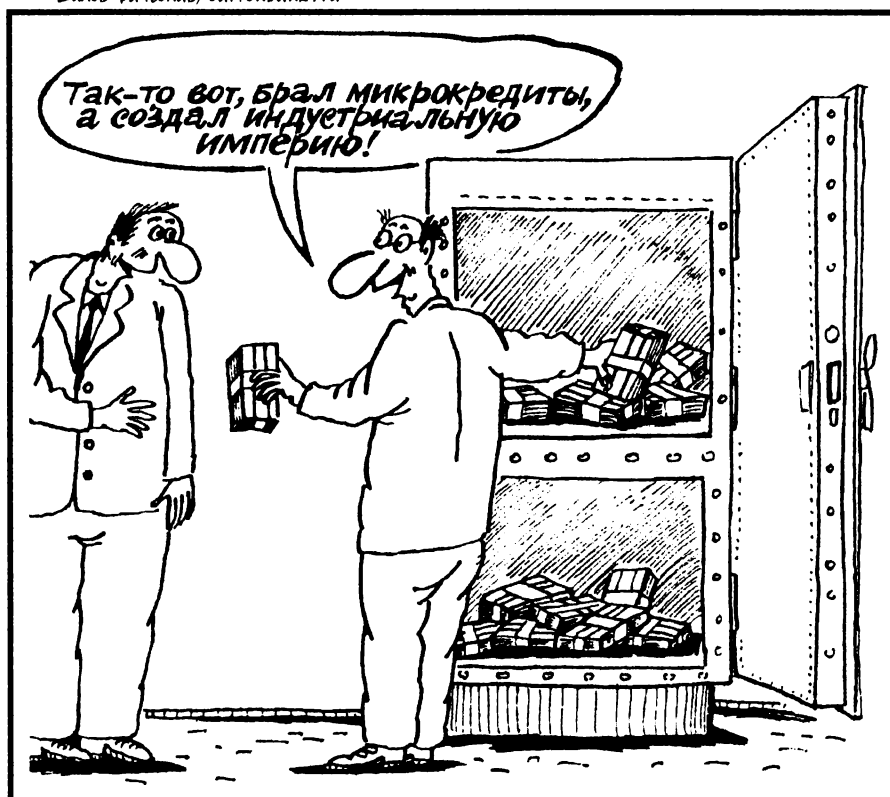
СОВЕТ

Поздравляю! Вы только что создали и настроили собственный контракт на платформе IBM. Позже вы сможете вернуться к нему, чтобы привязать его к IoT-устройству на аналитической панели службы Bluemix.

Часть IV

Блокчейн и экономика, право, государство

© Широв Вячеслав/cartoonbank.ru



В ЭТОЙ ЧАСТИ...

- » Будущее индустрии финансовых услуг при использовании блокчейн-технологии для перемещения денежных средств по всему миру быстро и недорого**
- » Недвижимость и блокчейн-технология**
- » Индустрия страхования: возможности сократить мошенничество и увеличить доходы за счет использования новых инструментов страхования**
- » Широкомасштабное внедрение постоянных систем в государственных службах и правовых учреждениях**
- » Прочие значительные глобальные тенденции в блокчейн-технологии и их влияние на нашу повседневную жизнь и мир, в котором мы живем**



Глава 12

Финансовые технологии

В ЭТОЙ ГЛАВЕ...

- » Рассматриваем вероятные тенденции в мировой банковской системе
- » Знакомимся с новыми инвестиционными инструментами
- » Выявляем возможные риски в банковских блокчейн-технологиях
- » Разрабатываем новые финансовые стратегии

Первыми, кто обратил внимание на блокчейн-технологии, были банки, правительственные структуры и некоторые финансовые учреждения, и в данный момент именно в этих сферах наблюдается самый быстрый рост числа пользователей блокчейнов. Мощные инструменты, созданные на базе новой технологии для управления финансами и перемещения денежных средств, неуклонно преобразуют наш мир новым и неожиданным образом, поэтому очень важно, чтобы эти финансовые структуры не оказались отставшими от жизни.

В этой главе вам предлагается краткий обзор того, что правительства разных стран предпринимают в данный момент по отношению к блокчейн-технологии и как это может отразиться на нас всех, ведь вопросы финансов и обращения

денежных средств являются частью нашей повседневной жизни, хотите вы этого или нет.

В этой главе вы познакомитесь с новыми тенденциями в банковской системе, с новыми нормативными актами, а также с новыми инструментами, которые предоставляют возможность выполнять перевод денежных средств быстрее и с меньшими затратами. Здесь также обсуждаются новые типы инвестиционных инструментов и другие инновации, появившиеся благодаря внедрению блокчейн-технологии. И наконец вы получите предупреждения о потенциальных рисках в отношении инвестиций, связанных с виртуальными валютами, а также в отношении некоторых финансовых продуктов, созданных на основе блокчейн-технологии.

Заглянем в хрустальный шар: новые тренды в банковском деле

Именно представители банковских структур первыми осознали опасность, которую представлял для них Биткойн, и оценили потенциал блокчейн-технологии в отношении возможной трансформации всей этой индустрии. Банковский сектор жестко регулируется правительственными структурами, и расходы на организацию банка и поддержку его функционирования могут оказаться очень велики. Этот жесткий контроль, с одной стороны, изолировал и защищал всю банковскую индустрию, а с другой стороны, был для нее тяжким бременем. Использование быстрой, эффективной цифровой валюты, которая не требовала издержек на манипулирование наличностью и позволяла отслеживать ее движение по всей финансовой системе, было одновременно и опьяняюще прекрасным, и угрожающим предложением. Сама идея, что ценность может существовать вне пределов контроля центральных властей, также вызвала интерес у финансовых учреждений и правительств, которые всегда стояли за спиной любой существующей валюты.

Сначала эти финансовые учреждения и правительства пытались теми или иными мерами подавить развитие блокчейн-технологии. А сегодня они используют эти же технологии для инвестиций за границу.

В 2013 и 2014 годах Комиссия по ценным бумагам и биржам США (U.S. Securities and Exchange Commission — SEC) выпустила предупреждение инвесторам о потенциальных рисках инвестирования с использованием виртуальных валют. Предупреждение заключалось в том, что инвесторы, привлеченные обещаниями высоких доходов, могут недостаточно скептически отнестись к этому новому инвестиционному пространству, столь нестандартному и передовому. В соответствии с тем документом SEC цифровая валюта являлась одной из

десяти главных угроз для инвестора. Сегодня SEC уже готова сотрудничать в этом вопросе с компаниями и инвесторами, поскольку криптовалюта приобретает все большую и большую поддержку во всех областях экономики и общественной жизни.

Еще два года назад многие страны по всему миру, включая Великобританию, Канаду, Австралию и Китай, начали проводить исследования, каким образом они могли бы создать собственные цифровые валюты, захватив всю созданную при этом криптовалюту в свое распоряжение и поместив эти деньги в блокчейн. Отправной точкой этих действий стал тот момент, когда выкристаллизовалось понимание, что возможные выгоды перевешивают риски. Биткойн продемонстрировал свою способность противостоять хакерам на протяжении нескольких лет, когда даже многие правительственные системы были скомпрометированы, что сделало его систему привлекательным вариантом для опробования. Инновации в блокчейн-технологии продемонстрировали свою способность обрабатывать миллиарды транзакций, необходимых для поддержки функционирования экономики, сделав криптовалюту достаточно надежной в необходимом масштабе.

Блокчейны представляют собой постоянные и неизменяемые записи каждой транзакции. Занесение денежной массы страны в блокчейн, контролируемый центральным банком, могло бы абсолютно изменить всю ситуацию по причине наличия постоянных сведений о каждой финансовой транзакции, в том или ином виде сохраненных в соответствующей записи блокчейна, даже если они не будут доступны для просмотра широкой публике. Блокчейн-технология и цифровая валюта позволяют сократить риск и затруднить мошенничество, обеспечив возможность абсолютного контроля в денежно-кредитной политике и налогообложении. Прежде всего, эта валюта не должна быть абсолютно анонимной, как биткойн. В действительности все должно быть как раз наоборот: она должна обеспечивать наличие полного и легко проверяемого следа каждой цифровой транзакции, проведенной отдельными лицами или организациями. Такой подход может даже позволить центральному банку играть в обороте денежных средств ту роль, которая сейчас принадлежит коммерческими банками.

Ответ на вопрос, каким будет будущее банковской системы, может одновременно пугать и восхищать. Потребители уже сейчас могут проводить платежи со своих телефонов почти мгновенно и практически в любом типе валюты или криптовалюты. Все больше и больше розничных магазинов начинают использовать криптовалюту как средство оплаты товаров и приема платежей от посетителей. В Кении сейчас пользоваться криптовалютой — более нормально, чем ею не пользоваться. Тем не менее это пока еще не основной вариант финансовых операций для большей части стран мира. Западные рынки все еще находятся на самой ранней стадии в принятии этой технологии.

Учитывая, что большинство людей хранят свои средства в казначейских билетах, выпущенных государством, или в ценных бумагах, также контролируемых правительственными службами, финансовые технологические инновации должны слиться с этими существующими системами, прежде чем можно будет увидеть и оценить главные преимущества блокчейн-технологии и цифровых валют. Если регулирующие органы найдут способы взимать налоги и регистрировать счета, массовое принятие клиентских кошельков с цифровыми токенами будет вопросом двух-трех лет.

Рынок “бизнес для бизнеса” начнет использовать блокчейн-технология гораздо раньше. Появления систем, ориентированных на производство, с соответствующими методиками и процедурами можно ожидать в течение ближайших двух лет. Среди прочих создатели систем Ripple и R3 приложили немалые усилия, чтобы сделать такую возможность реальной перспективой. Эти компании первыми сфокусировались на основных проблемах реализации цифрового представления депозитов. Это долговые расписки между внутренними подразделениями организации и между доверенными партнерами, такими как поставщики. Центральные банки, регулирующие и финансовые органы инвестируют значительные средства, чтобы сделать такой подход возможным. Быстрее всех в этом направлении продвигаются Канада и Сингапур.

Требования “Знай своего клиента” и положения по борьбе с отмыванием денег требуют от банков знать, с кем они ведут дела, и иметь гарантии, что это не участники схем по отмыванию незаконных средств и не террористы. Банки, выпускающие криптовалюты, по-прежнему должны будут строжайшим образом соблюдать эти требования. Но чтобы обеспечить их соблюдение, им потребуется точно идентифицировать каждое отдельное лицо, использующее их цифровую валюту. Во многих случаях индивидуальные банковские счета уже обрабатываются дебитовыми и кредитовыми службами транзакций, подобными распределенным реестрам в блокчейн-технологии, за исключением того, что они являются централизованными. Первыми кандидатами в этой области, вероятнее всего, будут регионы, в которых регулирующие органы, банки и центробанки работают совместно. Наилучшими кандидатами здесь являются Сингапур и Дубай, которые, кстати, уже проявили определенные инициативы в отношении блокчейн-технологии.

Быстрый перевод денег: без границ и прочих помех

Достичь реализации такого объема транзакций, который требуется для обеспечения успешной работы блокчейна, управляющего движением валюты в такой экономике, как в Великобритании или США, очень сложно. Только в США ежедневно осуществляются миллиарды транзакций на общую сумму более 17 000 миллиардов долларов в год. Чрезвычайно высокая ответственность для

новой технологии! Жизнь всей нации будет искалечена, если валютная система страны окажется скомпрометированной.

Руководители Международного валютного фонда, Всемирного банка, Банка международных расчетов и представители центральных банков со всего мира уже собирались для обсуждения перспектив использования блокчейн-технологии. Первым шагом на пути к более быстрым и более дешевым денежным переводам должно стать принятие блокчейна как протокола, упрощающего банковские переводы и межбанковские расчеты. Что же касается официальных цифровых валют, которыми обычные граждане смогут пользоваться в своей повседневной жизни, то они появятся гораздо позже.

Отдельные потребители напрямую не будут ощущать снижение затрат от использования блокчейн-технологии при проведении межбанковских расчетов. Экономия будет проявляться лишь во внутренней, скрытой от клиентов деятельности банка как снижение затрат на комиссионные, взимаемые посредниками.

В обозримом будущем потребители по-прежнему будут нуждаться в розничных точках торговли и коммерческих банках. Но с начала этого тысячелетия уже стали общепринятыми платежи через PayPal, Venmo, Cash и другие компьютерные системы. Новый способ оплаты посредством собственных телефонов также едва ли вызовет у них предубеждение.

Самой большой сложностью является тот факт, что, если все деньги станут цифровыми, компрометация системы станет всеобщей катастрофой с непредсказуемыми последствиями. Возможно, архитектура блокчейн-систем окажется достаточно прочной. Но проблема может состоять и в том, что программный код внутри системы может быть выполнен непредвиденным образом, как это произошло в случае децентрализованной автономной организации, DAO, которая в свое время подверглась успешной атаке в пределах системы Эфириум (см. главу 5). Если криптовалюта будет функционировать на основе традиционного открытого блокчейна, то необходимо получить согласие минимум 51% узлов сети, чтобы устранить возникшую проблему. Однако получение такого согласия может потребовать немало времени, что окажется практически неприемлемым для бизнесменов и людей, которые хотят стабильности и защищенности своих денежных накоплений на все времена.



ЗАПОМНИ

Многие блокчейны функционируют на демократической основе. Необходимо согласие большинства (более 51%) узлов, чтобы внести в них или в их работу любое изменение.

Создание перманентной истории

В будущем суверенитет данных и цифровая конфиденциальность приобретут очень большое значение. Предотвращать мошенничество станет проще,

поскольку, когда вся экономика перейдет на использование криптовалюты, во всех случаях в блокчейне будет оставаться контролируемый след, защищаемый от изменений всей системой. Этот факт весьма привлекателен для правоохранительных органов, но в то же время является настоящим кошмаром с точки зрения конфиденциальности потребителей.

С точки зрения потребителя, в этом случае навсегда остается контролируемый след любой операции, которая была выполнена с использованием кредитной или дебитной карты. С точки зрения учреждения наличие такого контролируемого следа является большим преимуществом, поскольку это повышает прозрачность документации и жизненных циклов движения данных активов между разными регионами. В конечном счете это повышает легитимность торговли активами и позволяет им поддерживать согласованность в своих ежедневных транзакциях.

Общепринятое в Европе “право быть забытым”, разрешающее гражданам не публиковать свои личные данные в Интернете, представляет собой очень сложную проблему для блокчейн-технологии, поскольку сама идеология блокчейна не позволяет ему что-либо забывать. Правительства и корпорации будут иметь постоянные исторические записи любой транзакции, что может быть разрушительным для национальной безопасности, если эта информация окажется открытой для широкой публики. А в случае компании это может позволить ее конкурентам получить важные сведения о том, сколько и во что она инвестирует.

Самой большой проблемой при использовании полностью открытых блокчейнов, подобных Эфириуму или Биткойну, является получение гарантий, что вы не отправляете деньги на поддержку терроризма в страну, занесенную в список Отдела по контролю за иностранными активами (OFAC) США. Суть в том, что решения этой проблемы не существует, поскольку в системе все анонимно и любой может открыть кошелек, указанный в качестве адреса получателя средств. Можно, конечно, создать алгоритм отслеживания перемещения транзакций (правительство США пользуется подобными средствами уже многие годы), тем не менее в мире полностью открытых блокчейнов активы может перемещать любой.



ТЕХНИЧЕСКИЕ
ПОДРОБНОСТИ

Отдел по контролю за иностранными активами (OFAC) США обеспечивает проведение акций в отношении конкретных организаций или отдельных личностей в тех странах, которые считаются потенциально опасными. Однако правительству не удастся проследить историю транзакций, если для их проведения используются полностью анонимные платформы.

Необходимость соблюдения правила “Знай своего клиента” и требований по защите от отмыwania денег требует использования в среде распределенного реестра авторизуемого блокчейна. Стартап R3, компания по созданию ПО,

разработала систему Corda, закрытую авторизуемую платформу, подобную блокчейну, которая прямо обеспечивает решение многих из упомянутых выше проблем. В частности, эта система не распространяет в глобальном масштабе данные своих участников. Это делает данные в блокчейне системы Corda закрытыми, что было основным нефункциональным требованием со стороны более 75 банков, работавших вместе с R3, для принятия ими блокчейн-технологии. Им требовалось сохранить конфиденциальность и при этом обеспечить строгие требования регулирующих органов.

Выход на международную сцену: глобальные финансовые продукты

В будущем блокчейн-технология позволит ввести в оборот много новых типов ценных бумаг и инвестиционных продуктов. Откроются новые рынки, позволяющие более эффективно просчитать риски, поскольку обеспечение кредита будет гораздо более прозрачным и взаимозаменяемым по всем учреждениям, когда они будут отчитываться по нему в поддерживающей блокчейн-системе.



СОВЕТ

Знаменитый экономист из Перу, Эрнандо де Сото, оценил, что если предоставить беднякам всего мира права на их земли, дома и незарегистрированный бизнес, то это выведет из тени ценности на сумму 9,3 триллиона долларов. Это то, что понимается под словом *мертвый капитал*.

Вполне можно представить, что страны, которые смогут освободить свой мертвый капитал, т.е. незаконенную недвижимость, которой обладают ее жители, получают возможность пакетировать ее и продавать соответствующие проценты по этим активам на мировом рынке. Это будет подобно прозрачным ценным бумагам на строительство новой недвижимости в Колумбии или Перу.

В будущем с помощью блокчейн-технологии многие страны смогут освободить свой мертвый капитал, и владельцы недвижимости, невозделываемой земли и не подлежащей кредитованию собственности получают возможность продавать проценты на эти активы на глобальном рынке.

Эти активы будут весьма притягательны, поскольку управляющие ими лица смогут активно выявлять неэффективные активы, пользуясь прозрачностью блокчейн-технологии и предоставляемой ею возможностью поместить один на место другого. Использование блокчейнов для управления этими активами предоставит их распорядителям возможность всегда владеть только высокоэффективными ценными бумагами, удаляя сомнительные варианты, реклассифицируя их и продавая как новые ценные бумаги.

Для индивидуальных клиентов микроинвестиции станут весьма привлекательным вариантом, доступным в глобальном и локальном масштабах через торговые платформы на основе блокчейн-технологии. Блокчейн-технология также предоставит им средства для инвестирования в компании и их конкретную деятельность без необходимости предоставления установленного минимума или обращения к посредникам, которые будут брать проценты с инвестиций.

Децентрализованные автономные организации (DAO) уже существуют, и создание их инвестиционных пулов имело место благодаря нескольким готовым к риску и более технически подкованным инвесторам. Возможно, должно пройти некоторое время, прежде чем рядовой инвестор воспользуется одной или целой подборкой рекомендаций со стороны своего управляющего вложить деньги в проект подобной децентрализованной организации.

Децентрализованная организация избавляет от большого объема неизбежной бумажной работы и различных бюрократических манипуляций, связанных с инвестированием, посредством создания системы голосования, построенной на базе блокчейн-технологии, и предоставления акций тем, кто вложил в нее свои средства. В любом блокчейне концепция “программный код — это закон” делает его неумолимым и не прощающим ошибок. Риски достаточно велики, особенно в том случае, если плохо написанный программный код используется непредвиденным способом. Последствия подобных атак на систему могут быть весьма серьезными. Прозрачная природа исходной системы при плохом программном коде предоставляет хакерам широкое поле для поиска уязвимостей, позволяя им атаковать систему многократно, каждый раз получая о ней все больше и больше информации.

В следующем разделе речь пойдет о возможных результатах и преимуществах, которые будут получены от использования блокчейн-технологии в мировой экономике.

Начисление зарплаты без границ

Глобализация уже объединила весь мир и современные компании не признают границ. Мгновенное и почти бесплатное перечисление зарплаты весьма заманчиво и позволяет организациям избавиться от ненужной головной боли. Однако здесь есть и определенные недостатки.

Самым большим риском является потеря фондов из-за действий хакеров. Если вам платят в криптовалюте и вы подверглись хакерской атаке, вернуть украденные у вас средства будет невозможно. Здесь не существует центров разрешения споров и не существует служб поддержки клиентов, куда можно было бы пожаловаться по поводу потери своих средств. Похитители цифровой валюты имеют глобальный доступ к вашим сбережениям, оставаясь при этом практически анонимными. Хакеры могут находиться где угодно.

При существующей структуре блокчейна каждый пользователь сам отвечает за свою безопасность. В настоящее время рядовые пользователи обычно не несут основного бремени по защите и страхованию себя от потерь. Крупные компании и правительства предлагают им защиту и страхование, и так было всегда, сколько мы себя помним. Рядовые граждане освободились от бремени защиты своих сбережений с тех пор, как еще в средние века перестали держать при себе все свое золото (в большей или меньшей степени).

Однако подобные проблемы едва ли удержат компании от начисления заработной платы с использованием криптовалюты. Стартап Bitwage и компания BitPay конкурируют на рынке начисления зарплаты через систему Биткойн. При этом в Bitwage сотрудникам фирм и независимым работникам по контракту позволяет получать часть начисленных им сумм в криптовалюте, даже если их работодатели исходно не предлагали им такой возможности. С другой стороны, в платежной системе BitPay имеются провайдеры службы начисления зарплаты Zuman и Incoin, интегрированные в ее платежные и зарплатные API. И вновь раньше всех эти новшества были приняты в тех регионах, где прежде полностью отсутствовали или имелись лишь неадекватные решения.

Торговля быстрее и лучше

Технология блокчейна будет способствовать более быстрой и, возможно, более открытой торговле. В последние годы финансирование глобальной торговли было ограничено. Некоторые банки, такие как Barclays, даже вовсе ушли с растущих африканских рынков, оставив за собой вакуум в области финансирования торговли. А ведь компании по-прежнему нуждаются в капитале для перевозки своих товаров.

Децентрализованные автономные организации и микроинвестирование смогут удовлетворить эту потребность и обеспечить инвесторам большую доходность, чем та, которая сейчас существует на этом рынке. Прозрачность данных обо всех проданных товарах, защита идентичности и бесшовное глобальное отслеживание, обеспечиваемые блокчейн-технологией, открывают новые широкие возможности для малых инвесторов.

Совместимость между различными валютами, которую обеспечивают такие компании, как Ripple, также способствует расширению торговли, поскольку они предлагают более гибкие инструменты вычисления обменных курсов иностранных валют, чем при использовании прежних механизмов передачи. Выведение наиболее популярных цифровых валют на валютные биржи повысит уровень адаптируемости и интеграции для недостаточно обслуживаемых рынков.

Компания BitPesa конвертирует минуты телефонных разговоров в сети M-pesa в Кении в биткойны. Используя эту технологию, она предлагает бизнесу быстрый и недорогой способ отправки и получения платежей между Африкой

и Китаем. Торговля между африканскими странами и Китаем представляет собой рынок с оборотом в 170 миллиардов долларов. Для проведения платежей за границу сейчас требуется несколько дней, и за это взимается немалая плата. Если же использовать цифровую платформу компании BitPesa, платежи осуществляются мгновенно и совсем недорого.

Гарантированные платежи

Гарантированные платежи, которые разрешены через транзакции, размещенные в блокчейне, расширят торговлю в тех местах, где уровень доверия не высок. В системах такого типа более бедные страны смогут принимать участие в конкуренции на тех же самых игровых полях, что и более богатые. Если это произойдет в ближайшие десять лет, глобальная экономика претерпит существенные изменения, а стоимость товаров и труда может возрасти.

Международные компании платят своим сотрудникам, исходя из конкурентного ценообразования, а также с учетом их предыдущих зарплат. Хотя блокчейн-технология будет способствовать достижению одного уровня для всех отраслей экономики, это не произойдет в одночасье. Разработчики и другие эрудированные работники могут стать исключением из общего правила, поскольку им будет проще обеспечить себя анонимной работой.

Финансовое вовлечение и равная глобальная торговля — очень важные темы для правительств. Принятие цифровых валют в национальных масштабах с большей вероятностью произойдет в небольших и развивающихся странах. В большинстве крупных стран имеются мощные децентрализованные структуры, которые будут препятствовать быстрому изменению таких жизненно важных систем, как деньги.

И наоборот, мощные централизованные структуры малых стран позволят им решительно перешагнуть через устаревшую инфраструктуру и бюрократию. Например, большинство стран Африки и Южной Америки не имеют стационарных телефонов или адресов, но во всех этих странах есть смартфоны, а значит, и возможность создавать криптовалютные кошельки. Недостающей частью является лишь общая торговая ликвидность и способность оплачивать базовые потребности, такие как коммунальные услуги, аренда и питание с использованием криптовалюты.

Микроплатежи: новая природа транзакций

Микроплатежи — это новая форма транзакций. Компании — эмитенты кредитных карт могут использовать блокчейн-технологии для размещения записей о транзакциях, предотвращения мошенничества и снижения собственных издержек.

Организации глобального масштаба, такие как Visa и MasterCard, предоставляющие пользователям преимущества в виде отложенных платежей, всегда будут нужны потребителям в капиталистических обществах. Даже если конечная стадия процесса изменится, у вас по-прежнему будут те же самые точки доступа в качестве клиентов. Однако физические платежные карты со временем исчезнут. В действительности этот процесс происходит уже сейчас, даже без участия блокчейн-технологии. Однако при использовании блокчейн-технологии идентификация клиента, выполняющего платеж, будет более жесткой в отношении возможного воровства.

Людам по-прежнему будут необходимы кредиты для ведения бизнеса и на личные нужды. Компании — эмитенты кредитных карт будут по-прежнему получать свои прибыли за счет взимания платы за транзакции. Кредиты позволяют миру двигаться вперед и рынки капитала всегда будут существовать, пока будет существовать сложившаяся социальная структура общества. Стоимость пересылки денег между группами людей будет снижаться, но это только на руку финансовым организациям. Они всегда стремились сфокусировать свои усилия прежде всего на предоставлении своим клиентам наилучшего выбора на их рынках инвестиционных или банковских услуг.

Вытеснение мошенничества

Система Биткойна была создана в ответ на разразившийся финансовый кризис, когда мошенничество и прочие неэтичные действия различных лиц послужили причиной коллапса мировой экономики. Она являет собой переход от взгляда на мир под лозунгом “доверять или не доверять” к системе, не требующей доверия. Это тонкое различие остается незамеченным для большинства. *Система без доверия* — это тот случай, когда вы с одинаковой степенью доверяете и не доверяете любому субъекту в сети. И что еще более важно, блокчейн-технология обеспечивает среду, в которой разрешено совершать транзакции без какого-либо доверия.

Тот же самый тип среды может использоваться не только лишь для обеспечения обмена ценностью в компьютерной сети. Позвольте привести пример, который поможет мне проиллюстрировать все потенциальные возможности этой технологии.

Я направляюсь в бар и охранник у входа останавливает меня и просит предъявить мое удостоверение личности. Я открываю бумажник и протягиваю ему мои водительские права. Эти права содержат гораздо больше информации обо мне, чем требуется охраннику в данном случае, и которую я не считаю нужным ему предоставлять (например, мой адрес). Все, что ему нужно

выяснить из моего документа, — это лишь то, что мне больше 21 года. Ему даже необязательно знать мой точный возраст — достаточно лишь убедиться, что он соответствует установленным ограничениям.

В будущем система идентификации личности на основе блокчейн-технологии позволит вам выбрать, какую именно информацию о себе вы хотите предоставить тому или иному лицу и на каком уровне. Чем более анонимными будут хранимые в этой системе данные, тем безопаснее они будут. Блокчейн-система поможет предотвратить похищение подтверждений идентичности и личных данных за счет того, что не будет предоставлять информацию тем, кто в ней не нуждается или не имеет разрешения ее видеть.

Другой важный аспект блокчейн-технологии заключается в том, что она смещает обнаружение мошенничества лишь после того, как оно уже произошло (в прошлом) в настоящее время, в тот момент, когда оно происходит в действительности. В существующих на настоящий момент схемах аудит является всего лишь частичным выявлением того, что уже произошло и что отменить уже нельзя. Группа аудиторов со стороны приходит в офис, случайным образом выбирает несколько файлов и анализирует, все ли в них на месте и проведено корректно. Сделать что-либо еще, помимо этой схемы, оказывается слишком дорого и требует очень много времени.

В системах хранения информации, построенных с использованием блокчейн-технологии, появляется возможность провести аудит файла непосредственно при его создании, обнаружив и пометив неполные или некорректные файлы непосредственно в тот момент, когда они создаются. В результате руководитель получает инструмент, позволяющий ему выявить и откорректировать файлы еще до того, как это станет проблемой.

Еще одним интересным свойством блокчейн-систем является возможность прозрачно делиться данными с третьей стороной. В будущем предоставить доступ к данным будет не сложнее, чем отправить электронное письмо с вложенным файлом, за исключением того, что получатель получит доступ к *оригинальным* данным, а не к их копии, как это происходит при отправке файлов по электронной почте. Когда вы отправляете файл, на вашем компьютере остается ваша версия, а получатель будет иметь собственную его версию. При использовании блокчейн-технологии у всех заинтересованных сторон будет доступ к одной и той же версии документа.

Блокчейн выступает как третья сторона, свидетельствующая о моменте времени и факте создания файла. Он может хранить подробную информацию о каждом субъекте, который получал доступ к документу через систему, как изнутри, так и снаружи. Он может показать, что было удалено из файла, а не только предоставить вам данные, которые имеются в нем в текущий момент.

Файлы в блокчейне также могут разделяться сторонами в режиме редактирования таким образом, чтобы не ставить под угрозу законность документов.

Это означает, что вы сможете увидеть возраст файла, полную его историю и как он выглядел по мере своего развития. Еще более интересно то, что вы также сможете увидеть, не исчезло ли что-нибудь из файла. Эта концепция называется *доказательство несовершенства*. В большинстве файловых систем в такой ситуации вам могут предоставить только то, что имеется в файле на данный момент, тогда как блокчейн-технология позволяет узнать и то, что в файле *отсутствует*, чего он сейчас не имеет.

В результате аудит становится более полным и обходится дешевле. Обновление правил проведения аудита может быть сделано более централизованно. Когда регулирующие узлы в сети блокчейна имеют совместный и прозрачный взгляд на транзакции актива, отчет по этим транзакциям может быть предоставлен непосредственно по месту нахождения регулирующего узла, без предоставления полномочий целой сотне или более других учреждений придерживаться одного и того же набора правил.

Системы, построенные на основе блокчейн-технологии и полностью интегрированные в работу организации, позволят точно знать, где и когда была потрачена каждая копейка. Конечную, сводную информацию о том, как были потрачены деньги, собрать сложнее всего для любых организаций и правительств. И именно потому, что так сложно все учесть, те, кто хочет совершить хищение, находят необходимые им лазейки.

Полная и точная сводная информация может стать для компании прекрасной возможностью сохранить растрачиваемые впустую ресурсы и выявить тех, кто приложил к этому руку. Неприбыльные организации, которые должны жестко придерживаться установленных для них норм и правил по учету того, как они расходуют свои средства, могут получить от подобных систем наибольший выигрыш. Они могли бы полностью удовлетворить свои потребности в аудите и подотчетности спонсорам, не препятствуя им в достижении тех благих целей, которые они перед собой поставили.

Одна система, которую подвергли тщательному исследованию, будет непосредственно интегрирована в рабочий процесс сотрудников по оказанию медицинской помощи. Изначально эта система проектировалась для отслеживания медицинских записей, но она сможет отслеживать в хронологическом порядке и все оборудование, медикаменты и расходные материалы, которые были использованы для каждого пациента. Преимущество этой системы — в ее монументальном постоянстве и неизменяемости, особенно если принять во внимание, как много мошенничества и воровства имеет место в мире неправительственных организаций.



Глава 13

Управление недвижимостью

В ЭТОЙ ГЛАВЕ...

- » Оценка глобальных тенденций в управлении недвижимостью
- » Мертвый капитал и методы исправления ситуации
- » Как Фанни Мей намеревается существовать в мире блокчейна
- » Планы Китая в отношении развития блокчейн-технологии

Управление недвижимостью можно считать одной из тех сторон жизни общества, которые в наибольшей степени подверглись влиянию инноваций, открытых миру блокчейн-технологией. Однако это влияние в каждой стране мира ощущается по-своему. В западном мире можно наблюдать появление таких вещей, как прозрачные ипотечные ценные бумаги, торгуемые на биржах, функционирующих на основе блокчейн-технологии. В Китае интеграция блокчейна уже имеет место в такой области, как нотариальное заверение — важнейший элемент любой операции с недвижимостью. В развивающемся мире на блокчейн-технологии возлагают самые большие надежды, поскольку ее внедрение позволит освободить мертвый капитал и повысить объемы торговли.

В этой главе обсуждаются инновации, которые уже воплощены в сфере недвижимости в различных странах мира. Также мы рассмотрим возможные грядущие изменения в этой сфере и то значительное влияние, которое может оказать на нее блокчейн-технология.

Недвижимость представляет собой существенную часть мирового богатства и играет важную роль в обеспечении стабильности экономики. Однако в предстоящие несколько лет в этой сфере ожидаются быстрые и весьма значительные изменения, так что понимание того, где эти изменения произойдут и как ими можно будет воспользоваться, несомненно, будут очень полезны.

Исключение титульного страхования

Титульное страхование (или страхование правового титула) представляет собой страхование риска финансовых потерь, которые вы можете понести в результате обнаружения дефекта в титуле собственности (документе, подтверждающем право собственности на недвижимость). Оно необходимо, если вы хотите взять ипотечный кредит под свой дом или дополнительно его финансировать. Титульное страхование защищает инвестиции банка в отношении проблем с вашими правами на эту недвижимость, которые могут быть следствием отсутствия необходимого их подтверждения в официальных записях либо незаконности предыдущих сделок, либо возникнуть в результате мошенничества или подлога.

Страхование титула необходимо, когда для управления титульной системой используется общее законодательство. В этом случае *покупатель* отвечает за получение гарантий, что права продающего на собственность имеют силу. В таких системах необходимо провести поиск свидетельств о корректности прав продавца на собственность и приобрести соответствующую страховку. В тех регионах, где используется титульная система Торренса, покупатель может полностью доверять информации в государственном земельном регистре и не проводить поиск данных где-либо, помимо записей в этом регистре.

Блокчейн-технология была предложена как дополнение, предназначенное для оказания помощи покупателям в титульных системах общего права. Идея проста: блокчейн по самой своей сути является максимально открытой и одновременно надежной системой хранения записей; в нем нельзя осуществить какие-либо изменения или внести исправления в хранимые данные без жесткой фиксации любых выполненных действий. Теоретически блокчейн-технология способна преобразовать титульную систему общего права в распределенную титульную систему Торренса.

Однако прежде потребуется преодолеть много различных проблем. В каждом округе с титульной системой общего права имеется собственная структура регистрации прав на земельную собственность, в которой все документы или записи о передаче прав собственности на любой участок земли или любой доход с любого участка земли в этом округе регистрируется и помечается. Только в США есть сотни таких округов. Тысячи подобных отдельных структур создают неимоверное количество записей данных. Блокчейн-структура сама по себе не может изменить законы и принципы, по которым эти записи создаются и упорядочиваются.

Необходимо создать новые законы, согласно которым любая информация об имущественном праве или передаче земель, чтобы ее можно было считать действительной, обязательно должна быть записана в единой системе. Тогда это будет просто титульная система Торренса, которая, в принципе, может сделать блокчейн-технологии избыточной. Исключениями могут стать лишь те регионы, в земельных регистрах которых присутствует множество мошеннических записей.

Далее в этом разделе мы подробнее поговорим о сфере управления недвижимостью и о том, где применение блокчейн-технологии могло бы оказаться полезным.

Защищенные отрасли

В каждой отрасли существуют системы самозащиты, направленные на предотвращение проникновения в них новых конкурентов. Это может быть строгий административный надзор, гарантированные правительством монопольные права или же сверхвысокие затраты на первоначальных этапах. Индустрия, выстроенная вокруг операций покупки и продажи недвижимости, не претерпевала каких-либо значительных изменений за последние 40 лет и вполне созрела для окончательного развала. Множество различных участников внесли свой вклад в этот процесс разрушения.

Вот несколько типов бизнеса, которые выросли вокруг процедуры покупки и продажи дома.

- » **Агенты по недвижимости.** Агенты по недвижимости помогают потенциальным покупателям сравнить возможные варианты и подобрать подходящее жилье. Они также помогают вести переговоры о цене и связываются с продавцом от имени покупателя. Эти услуги достаточны ценны и их нежелательно заменять чем-либо при внедрении блокчейн-технологии. Конечно, вы можете купить дом и без участия агента по недвижимости; тем не менее многие предпочитают работать с ними, поскольку это улучшает и ускоряет всю процедуру.

- » **Жилищные инспекторы.** Назначение жилищного инспектора — обнаружить возможные дефекты дома до того, как вы его купите (здесь речь идет о тех дефектах, устранение которых может стоить вам немалых денег). Обнаруженные жилищным инспектором дефекты можно использовать при ведении с продавцом переговоров о более выгодной цене. В будущем дома все так же будут подвергаться износу — этот процесс отменить невозможно. Однако блокчейн можно использовать для записи сведений о проведении ремонта имущества и о дефектах, которые были обнаружены жилищным инспектором.
- » **Закрывающие представители.** При закрытии сделки финальным этапом является проведение расчета. Закрывающие представители координируют оформление документов о закрытии, подписывают их и передают деньги соответствующим сторонам. Блокчейн-технология позволяет отказаться от закрывающих представителей, потому что выполняемые ими функции могут быть встроены в смарт-контракт или чейнкод.
- » **Ипотечные кредиторы и обслуживающие лица.** Ипотечные кредиторы и связанные с ними службы предоставляют финансы для ипотечных займов и собирают текущие платежи по ним. Их невозможно заменить программными средствами блокчейн-технологии, но они сами могут использовать эту технологию для сокращения собственных издержек на поддержку документооборота и проведение аудита.
- » **Оценщики недвижимости.** Задача оценщика недвижимости состоит в осмотре собственности и определении, сколько она может стоить. Процедура оценки выполняется каждый раз, когда собственность покупается или рефинансируется. Компании, подобные Zillow, в свое время приложили немало усилий для сбора данных о рыночной стоимости, но все же каждый дом уникален и нуждается в периодической переоценке. Даже в процессе ипотечного кредитования может потребоваться несколько раз вызывать оценщиков, чтобы удовлетворить потребности всех сторон. Может оказаться полезным записывать подобные данные в блокчейн — в качестве открытого свидетельства.
- » **Кредитные эксперты.** Кредитные эксперты собирают о вас кредитную и финансовую информацию, а также данные о вашей трудовой деятельности и послужном списке, чтобы оценить, можете ли вы претендовать на кредит. Затем они принимают решение, отвечаете ли вы требованиям, необходимым для получения продукта, который они предлагают. Как и агенты по недвижимости, кредитные эксперты помогают выбрать наилучший вариант из числа доступных.

Программное обеспечение блокчейн-технологии может быть использовано для того, чтобы помочь кредитным экспертам отслеживать документы, которые они вам предоставили, и следить за процессом с целью обеспечения справедливого кредитования.

- » **Оформители займов.** Оформитель займа помогает кредитным экспертам в подготовке информации об ипотечном кредите и заявке на его предоставление для ипотечного андеррайтера. Сейчас для этой цели используется специальное программное обеспечение, которое извлекает информацию об источниках доходов анализируемого получателя займа. Это ПО не использует блокчейн-технологию, но обращение к ней может сделать наличие таких работников излишним.
- » **Ипотечный андеррайтер.** Ипотечный андеррайтер определяет, можете ли вы претендовать на ипотечный заем. Он одобряет или отклоняет вашу заявку на его предоставление, исходя из вашей кредитной истории, сведений о трудоустройстве, вашем имуществе и долгах. В некоторых организациях проводятся исследования по автоматизации данного процесса с использованием искусственного интеллекта. Однако это программное обеспечение не относится к блокчейн-технологии.

Действия каждого из этих участников процесса направлены на достижение главной цели — защитить от потерь покупателя, продавца и ипотечного кредитора. В большинстве сфер деятельности стоимость ведения бизнеса со временем понижается — повышение эффективности диктуется конкуренцией и осуществляется за счет инноваций, обеспечивающих снижение издержек. Ипотечная индустрия весьма привлекательна в качестве кандидата на внедрение инноваций на основе блокчейн-технологии, прежде всего потому, что в ней имеют место противоположные процессы: стоимость ведения бизнеса постоянно возрастает. В США типичный договор по ипотечному займу имеет более 500 страниц и требует не менее 7500 долларов для оформления. А это в три раза больше, чем требовалось 10 лет назад. Блокчейн-технология способна удовлетворить все требования по защите покупателя, продавца и ипотечного кредитора, одновременно обеспечив снижение уровня необходимых расходов.

Клиенты ипотеки и “Фанни Мей”

Федеральная национальная ипотечная ассоциация (Federal National Mortgage Association, в народе называемая “Fannie Mae”) является одновременно и финансируемым правительством предприятием, и публичной акционерной компанией. В настоящее время она является основным источником финансирования для ипотечных кредиторов и доминирует на пост-рецессионном рынке, с которого ушли частные финансы.

С момента рецессии 95% всех займов на приобретение дома, совершенных в США, прошли через Фанни Мей. А это около 5 триллионов долларов в ипотечных активах. За несколькими исключениями займы, которые не прошли через Фанни Мей или ее близкого кузена Фредди Мака (Freddie Mac), являются огромными (обычно более 417 тысяч долларов каждый). Такие займы по-прежнему финансируются через частный капитал.

В системе Фанни Мей для оценки потенциальных заемщиков кредиторы используют специальное программное обеспечение. Оно помогает им ориентироваться при предоставлении обычных займов. Кредиторы отправляют поступающие заявки на кредиты в компьютерную систему Фанни Мей, и она “выплывает” им ответ, принять или отклонить ту или иную заявку. Существуют интерактивные инструменты, использующие это новейшее программное обеспечение, которые доступны непосредственно клиентам, нуждающимся в кредитах, что позволяет им обойти традиционные методы получения ипотечных кредитов. В Фанни Мей и Фредди Мак также проводятся исследования в отношении использования блокчейн-технологии для дальнейшего расширения этого процесса и непосредственного выхода на потенциального клиента.

Ипотека в мире блокчейна

Ипотека в мире блокчейна не так уж сильно отличается от ипотеки в обычном мире. Единственное, что следует отметить особо, — ипотека в блокчейне будет менее дорогой при заключении сделки.

Учитывая, что большинство людей за время своей жизни только в редких случаях покупает несколько домов, это различие может показаться не столь уж важным. Но деньги способны накапливаться. Сейчас блокчейн-технология позволяет снизить стоимость получения ипотечного кредита до уровня 2007 года.

Сокращение стоимости получения кредита

Стоимость оформления ипотечного кредита постоянно растет, и причина здесь проста: банки пытаются оградить себя от штрафов, взимаемых с них в том случае, если они оформили что-то не так на любом этапе ипотечного процесса. Иначе говоря, банки поставили перед собой цель получить гарантии в отношении полного соответствия документации всем имеющимся требованиям как на момент ее создания, так и спустя годы, если она будет подвергнута аудиту. Большие банки вынуждены платить миллиарды в качестве штрафов за несоблюдение правил ведения документооборота. Сейчас они требуют предоставления не только всех необходимых документов, но и доказательств, что они следовали правильной процедуре и отправили вам все необходимые документы.

Программное обеспечение, созданное на основе блокчейн-технологии, позволяет сократить избыточность, которую банки стали вводить в свои рабочие процессы после рецессии. Издержки на оформление, хранение и аудит документации выросли до небес с момента вступления в силу Закона о реформировании Уолл-стрит и защите потребителей Додда–Франка, но блокчейн-технология позволяет сократить эти издержки.

Компаниям, которые хотели бы удовлетворить требования банков в отношении блокчейн-решений, следовало бы предоставить банкам доказательства, что они придерживались рекомендаций, введенных в акте Додда–Франка. Также было бы полезно помочь банкам документировать, почему были приняты определенные решения по займам, и помочь им указывать местонахождение документов, которые они использовали в процессе оформления займа, даже если банк не владеет этими документами.

Блокчейн-приложения могут обеспечить сокращение стоимости оформления среднего ипотечного займа на сумму до 4 тысяч долларов. Ипотечная индустрия во многом схожа с индустрией кредитования покупки автомобилей и индустрией выдачи кредитных карт. Аналогичные приложения способны сократить административные издержки в этих областях, вызванные введением закона о защите потребителей, в то же время позволяя инвестирующим компаниям удовлетворять его требования.

Знай свой последний известный документ

Один из крупнейших источников затрат в процессе ипотечного кредитования часто выявляется лишь через годы после того, как заем был предоставлен. Иногда желающие помочь ходу процесса предоставления займа добавляют в файл клиента ненужные документы или старые файлы, которые не использовались при предоставлении займа, но остались в папке клиента. Также вполне возможно элементарное дублирование записей. Когда наступает момент проведения аудита такого файла, в нем обнаруживается слишком много информации для просеивания. Банки платят деньги независимым фирмам, осуществляющим проверку их записей, и потому пытаются определить, какие именно документы были использованы в процессе принятия окончательного решения о предоставлении кредита.

Программное обеспечение на базе блокчейна позволяет решить эту проблему очень элегантным методом. Блокчейн-реестры представляют собой распределенную систему хранения записей, которая позволяет многим сторонам совместно работать с данными во времени, не теряя при этом информации о том, как эти данные выглядели в любой момент их совместной обработки. А это означает, что полдюжины независимых организаций, которые совместными усилиями помогают вам приобрести себе дом, смогут теперь

взаимодействовать в одном и том же документальном пространстве, в едином блокчейн-реестре, где будет храниться цепочка ваших документов.

В данном случае создателем такой цепочки будете вы сами. А затем к этой цепи будут добавляться подцепочки, такие, например, как заказ на строительство дома. Впоследствии вы сможете предоставить доступ к этой цепочке другим сторонам, например банкам, наемным работникам, кредитным агентствам, оценочным компаниям и так далее, позволив им вносить свои записи в вашу цепь. Каждая из этих сторон получит возможность добавить в вашу цепочку свои данные, а все остальные авторизированные вами стороны смогут их прочесть и пополнить своими собственными.

Блокчейн-технология может повлиять на потребность содержать централизованные хранилища файлов. Она позволяет автоматизировать некоторые процедуры работы с бумагами и гарантирует получение четких исторических сведений по вашему займу в любой момент времени, сокращая потребность в проведении аудита и соответствующей подготовки документов к проверке.

Это отличная идея, но она не требует тесного сотрудничества всей отрасли. Каждое ее звено, в котором будут предприняты соответствующие шаги, будет работать на усиление всей системы и добавлять ей ценности, подобно тому, как каждый дополнительный владелец факс-машины автоматически повышал эффективность всей системы факсимильной связи, что делало обладание такой машиной более полезным для всех.

Прогнозирование региональных тенденций

Блокчейн-технология ведет непростую битву за то, чтобы стать основным программным решением. Часто первая встреча с ней вызывает у людей чувство страха, поскольку многие не понимают, как она работает или каковы будут фактические последствия от ее широкомасштабного внедрения. Также многие из ее первых сторонников, подобно первым сторонникам любых новых технологий, воспринимаются как люди слегка “не от мира сего”. Помимо прочего, блокчейн-технология унаследовала лихую славу Биткойна, вызванную запрещенными и незаконными действиями, совершенными с использованием этой системы.

Тем не менее 2016 год был поворотной точкой в этой индустрии. К этому времени стало понятно, что блокчейн-технологию можно использовать не только в разрушительных целях, и те, кто хотят остаться на стороне закона, просто должны разработать соответствующую стратегию ее использования.

Практически в каждом крупном банке уже запущены программы исследования и экспериментирования с блокчейн-технологией, либо он уже присоединился к консорциуму. Многие банки начинают переход на новую технологию с межбанковских расчетов и переводов за границу, поскольку эти задачи относительно просто решаются в блокчейн-приложениях. Следующей и более преобразующей ступенью эволюции станут системы и данные, защита которых обеспечивается за счет децентрализации.

Далее в этом разделе речь пойдет о существующих в блокчейн-технологии тенденциях, характерных для США, Европы, Китая и Африки.

Соединенные Штаты Америки и Европа: перегруженность инфраструктуры

Соединенным Штатам и европейским странам может потребоваться больше времени для перехода на блокчейн-технологию, чем другим странам. Несмотря на то, что компании в этих странах тратят миллиарды долларов на поддержание инфраструктуры, все дело состоит именно в этом: поддержка и *сохранение* уже существующего. Здесь уже имеются решения для тех проблем, которые предполагается решить с помощью блокчейн-технологии. И в этом случае вам не удастся просто сказать, что блокчейн-технология позволит получить лучшее решение, — это решение должно быть в *десять* раз лучше существующих систем либо допускать реализацию через интеграцию.

Одна из основных проблем, с которыми столкнулись Соединенные Штаты, состоит в том, что в них имеет место децентрализация власти и принятия решений. По этой причине следует ожидать, что каждое графство и каждый штат выработает собственные правила внедрения или использования блокчейн-технологии. И этот процесс уже начался.

Переход к блокчейн-технологии может инициировать принятие законов и требований в отношении денежных переводов. В США на федеральном уровне ясно определено, какие типы организаций могут иметь право осуществлять перевод денежных средств. Учитывая, что все основные открытые блокчейн-системы сейчас используют криптовалютные токены для обеспечения своей защиты, их будущее с точки зрения закона пока остается весьма туманным, что стало мощным стимулом для разработки частных закрытых и эксклюзивных блокчейнов, функционирующих без токенов.

Требования к государственным лицензиям в отношении компаний, использующих блокчейн-технологии в приложениях, не связанных с платежами, являются неоднозначными. Можно ожидать, что в этой области будут приняты некоторые акты и законы относительно защиты потребителей. Например, в Европе уже существует закон о праве “быть забытым”. Соблюдение этих правил

может оказаться непростым делом, поскольку введенные в блокчейн данные сохраняются в нем практически навсегда и не могут быть удалены кем бы то ни было, даже если все этого хотят.

В США участие в незаконной передаче денежных средств во многих штатах рассматривается как тяжкое преступление. Тяжелые последствия от фактов несоблюдения требований закона через инновации вынуждают блокчейн-компании тратить очень много денег и времени на их улаживание — в среднем от 2 до 5 миллионов долларов в год на компанию. Юридические сборы являются тяжким бременем для этих технологических стартапов.

Законодательство каждого штата по отношению к блокчейн-индустрии до сих пор не вполне ясно. Штаты Нью-Йорк и Вермонт уже начали интеграцию этой технологии в рамки закона. В Нью-Йорке повысили соответствующие сборы, что вынудило инновационные компании переместиться на более дружественные территории. С другой стороны, в штате Вермонт приняли закон, согласно которому записи в блокчейне могут быть представлены для рассмотрения в суде.

В Люксембурге правовая основа для электронных платежных учреждений была создана еще в 2011 году, что явилось первым шагом на пути к реализации идеи “электронных денег”. Люксембург и Великобритания стали родным домом для множества блокчейн-компаний, так как правовая среда этих стран позволяет им легче ориентироваться и находить требуемые возможности. Так, за менее чем 1 миллион долларов их владельцы могли получить лицензию платежного оператора от Европейского Союза. Такая лицензия предоставляла компании доступ к 28 странам ЕС. Подобный подход позволил странам ЕС достичь превосходства над США в финансово-технических инновациях.

Китай: первый, кто вышел за ворота

В Китае поняли, что граждане страны использовали блокчейн-системы для скрытого перемещения ценности за ее пределы и генерирования нового богатства в менее контролируемой системе. По этой причине законоположения по криптовалютам пересматривались в Китае несколько раз, что оказывало сильное влияние на рыночный курс биткойна.

В Китае в различных отраслях сейчас ищут в блокчейн-технологии возможности решения многих проблем, сходных с теми, которые существуют и в других частях света. Здесь быстро перешли к использованию блокчейнов как дополнений к тому, что уже делалось, добавив тем самым уровни определенности в таких областях, как Интернет вещей (IoT) и нотариальное засвидетельствование. В целом для западных стран свойственны распределенные и децентрализованные силовые структуры, тогда как в Китае они централизованы в значительно большей степени. Именно это обеспечило Китаю быстрое

продвижение как в отношении законодательных актов, так и в отношении принятия инноваций.

Альянс China Ledger, блокчейн-коалиция, получившая поддержку от Всеки-тайского собрания народных представителей, высшего органа государственной власти Китая, является хорошим примером быстрых действий со стороны как государства, так и экономики. Этот альянс привлек к сотрудничеству Антонио Ди Йорио и Виталика Бутерина, основателей Эфириума, а также получил поддержку разработчика ядра Биткойна Джефа Гарцика и менеджера компании UBS Innovation Алекса Балтина.

Развивающийся мир: блокпосты на пути к блокчейну

Будущее уже здесь — оно просто еще не проявило себя. Это утверждение особенно справедливо в развивающихся странах, которые часто очень нуждаются в новой технологии, но не имеют необходимых ресурсов и такой политической обстановки, которые позволили бы этой инновации укорениться на их почве. Некоторые небольшие страны прибегают к протекционистским мерам с целью блокировать импорт тех товаров, которые могут быть произведены в пределах их границ, тогда как в других странах просто не доверяют качеству и добрым намерениям тех товаров и услуг, которые приходят из внешних источников. Еще хуже тот факт, что некоторые политические системы много выигрывают от неэффективности и двусмысленности, от которых их юридические системы должны были бы давно избавиться.

Эрнандо де Сото Полар — экономист из Перу и автор, много писавший о неформальной экономике и важности прав на собственность и бизнес. Одной из важнейших проблем, мешающих истинному развитию многих развивающихся стран, является *мертвый капитал*. Это собственность, которая не имеет документального оформления и не признается законом, либо текущие системы на местах, которым нельзя доверять. Владельцам таких земель очень трудно или просто невозможно найти финансирование или продать их. Неопределенность также значительно снижает стоимость таких активов. В западном мире вы можете взять деньги в долг под заставу активов или относительно свободно продать их. Именно это привело в конечном счете к различным инновациям и экономическому процветанию.

Технология, которая оказывается возможной благодаря блокчейну, может очень быстро изменить эту печальную реальность в развивающихся странах. Прозрачные записи о правах владения на землю будут означать, что можно будет эти земли продавать либо получать под них кредиты. А это может сделать недвижимость на побережье Колумбии просто неотразимой. Необратимые платежи и доподлинно известная идентичность способны открыть новые пути для кредитования и коммерции.

Многие стартапы и хакеры неоднократно собирались, чтобы попытаться привести это видение будущего в реальность. Даже крупнейшие мировые игроки, такие как Всемирный банк, регулярно проводят обсуждения возможностей блокчейна и его влияние на развивающийся мир. Биткойн и блокчейн-технология активно приходят в страны Африки, где местные валюты и инфраструктура вызывают глубокое недоверие. Компания BitPesa, платежная и торговая платформа, обслуживающая многие африканские страны, сейчас расширяет область своей деятельности на Великобританию и Европу. Она также расширила спектр своих предоставляемых сервисов вплоть до таких услуг, как выплата заработной платы.

Помимо множества препятствий, с которыми развивающиеся страны сталкиваются на пути к своему развитию и инновациям, у них есть и определенные преимущества, которых у западных стран никогда не будет. Отсутствие у развивающихся стран уже существующей инфраструктуры позволяет им сделать решительный скачок к уровню западных стран. Об этом свидетельствует безудержное распространение сотовой телефонной связи среди населения развивающихся стран. В этих странах также отсутствуют регулирующие органы и законы о защите потребителей. И эта особенность особенно притягательна для блокчейн-стартапов, которые согласно законодательству западных стран неизбежно попадают в серую зону. Также в развивающихся странах часто имеется всего несколько человек, принимающих решения на государственном уровне, что в определенной степени упрощает возможность встречи с такими людьми, имеющими достаточно власти для проведения изменений.



Глава 14

Страхование

В ЭТОЙ ГЛАВЕ...

- » Построение нового страхового бизнеса
- » Индивидуальный пошив личной страховки
- » Создание новых рынков страхования
- » Снижение издержек неожиданным образом

В страховании блокчейн-технология в наибольшей степени может повлиять на то, как частные лица и компании будут покупать и получать страховое покрытие, и это произойдет раньше, чем вы можете подумать! Полезно будет познакомиться с возможными последствиями внедрения этих новых технологий, которые уже просматриваются на горизонте.

В этой главе мы поговорим о том, как эти новые технологии работают и в чем их основные ограничения. Вы узнаете, как устройства из Интернета вещей (IoT) смогут сотрудничать со страховыми компаниями и как самоисполняемые блокчейн-контракты будут определять политику и структуру компаний.

Эта глава подготовит вас к фундаментальным изменениям в технологии, способным снять бремя доказательства. Прочитав ее, вы сможете принимать более грамотные решения в отношении страхового покрытия и платежей, построенных на базе блокчейн-технологии. Вы поймете, как стоимость покрытия может повлиять на ваш выбор, и познакомитесь с различными типами покрытия, которые станут доступными в недалеком будущем.

Точный раскрой страхового покрытия

Устройства Интернета вещей (IoT devices), неизменяемость данных, децентрализованные автономные организации (DAO) и смарт-контракты — все это способствует совершенствованию страхования для потребителей. Сведение всех этих технологий воедино стало возможным лишь благодаря развитию блокчейн-технологии.

Некоторые вещи блокчейн-технология позволяет делать действительно хорошо, и это ведет к двум главным изменениям в том, как страховки будут продаваться и покупаться в будущем. Во-первых, индивидуальные пользователи смогут получать больше пользовательского покрытия, а во-вторых, откроются новые рынки, которые прежде были просто невозможны по причине чрезмерных расходов.

Индивидуальное страхование

Перестройка страхования к ориентации на индивидуального пользователя приведет к существенному смещению приоритетов. Управление активами станет менее критическим, и страховые компании получат возможность сфокусироваться на вычислении рисков и сопоставлении спроса и предложения.

Предположим, у вас есть возможность создать рыночную платформу для страхования клиентов. Существует много различных способов организации этого нового бизнеса. Один из них — рынок по требованию, куда пользователи будут направлять свои заявки, оформленные либо как обычные смарт-контракты, либо как Chaincode-контракты. Если вы еще недостаточно знакомы с этими новыми типами самоисполняющихся цифровых контрактов, обратитесь за разъяснениями к главе 5, посвященной системе Эфириум, или к главе 9, в которой обсуждаются разработки концерна Hyperledger.

В модели этого типа вы как страхующее лицо можете рассчитать страховую премию для конкретного страхового случая, основываясь на исторических данных и прочих факторах вычисления рисков, используемых в той модели расчета риска, которую выберете. Если клиент заинтересуется вашим предложением, он сможет повысить цену или подписаться, в зависимости от используемой модели спроса.

Этот новый тип страхования может быть принят для пирингового или краудфандингового варианта страхования либо в обычной страховой компании, которая воспользуется новой технологией. В любом случае страховка будет создана в децентрализованном реестре криптовалюты в формате смарт- или Chaincode-контракта, гарантирующего осуществление выплат клиента инвестору и наоборот при возникновении страхового случая. Ключевым элементом

здесь является блокчейн-технология, поскольку только она обеспечивает необходимую функциональность, которая еще несколько лет назад была либо невыполнима, либо запрещена.

Блокчейн-технология позволяет организовать почти бесшовную передачу ценности, допускающую даже микроплатежи, поскольку операционные издержки здесь очень невелики. В результате появляется возможность выйти на новые рынки, на которых нет действующей монетарной системы либо правовой системы или соответствующих инстанций и стоимость проведения транзакций и оспаривания перевешивают выгоду от предоставления страхового покрытия.

Работая со смарт-контрактами, можно использовать распределенные автономные организации (DAO) для управления большими группами участников при небольших издержках и затратах времени. Эту модель можно использовать для оформления новой компании и ее администрирования, а также, возможно, для организации краудфандинговой страховой платформы.

Самоисполняемая природа смарт-контрактов может также высветить многое в издержках от корректировки требований и действий третьих лиц, что поможет в обработке и сборе фондов.

Следует отметить, что законность всех этих действий по-прежнему остается под вопросом. Определение проблем с нарушением конфиденциальности и прав потребителей здесь затруднено. Также каждая страна имеет собственные законодательные нормы и требования по предоставлению информации. Однако, если эти нормы и требования удовлетворяются, сама страховая индустрия и практика страхования у клиентов могут существенно измениться.

Новый мир микрострахования

Микрострахование — это страхование для защиты людей с небольшими доходами от различного рода рисков, таких как несчастный случай, болезнь или стихийное бедствие. Благодаря блокчейн-технологии этот вид страхования становится более приемлемым.

Обдумывая возможности микрострахования, обратите внимание на существование двух категорий объектов страхования (которые могут иметь место и одновременно).

- » Страхование малодоходных хозяйств, ферм и других объектов, страховка которых должна учитывать специфические нужды, — как правило, это страхование с низкой премией и с индексацией.
- » Страхование малоценных товаров, изделий или услуг.

Самая большая проблема, связанная с контрактами такого типа в обычной модели страхования, состоит в том, что издержки на их оформление и реализацию непропорционально высоки в сравнении с возможной выгодой, что делает эти рынки малопривлекательными для обслуживания.

Почти полная прозрачность границ для транзакций в блокчейн-системах, позволяющая перемещать ценность за очень невысокую плату и практически беспрепятственно между любыми уголками мира без возможности вернуть отправленное обратно, открывает широчайшие перспективы по обслуживанию большего количества людей и с меньшими издержками.

Ключевое преимущество блокчейна состоит в том, что создание смарт-контракта обеспечивает выполнение защищенных транзакций без необходимости участия третьих лиц, а это означает, что издержки при страховании существенно снизятся.

Принципы микрострахования на основе блокчейн-технологии очень просты и включают всего четыре этапа.

1. Предложение заключить соглашение по кредитованию/страхованию.

Владельцу делается предложение о предоставлении ссуды под его имущество через его страхового агента при условии, что эта собственность зарегистрирована в цифровом реестре. Предложение может быть направлено потенциальному клиенту как через каналы страховой компании, так и через открытые платформы, например Facebook.

2. Соглашение анализируется.

Далее заемщик может обдумать поступившее предложение и принять его либо отклонить. Предложение хранится в виде открытой записи, и если заемщик принимает его, он может заказать соответствующую страховку через стандартные каналы проведения оплат, после чего процедура переходит к третьему этапу.

3. Соглашение подписывается и нотаризируется.

Если обе стороны пришли к соглашению, страховка выплачена и заемщик получил соответствующее имущество, соглашение подписывается цифровым способом и нотаризируется в реестре блокчейна, что делает его практически полностью защищенным от несанкционированного доступа. Вся информация о последующих транзакциях безопасно сохраняется в четкой контролируемой последовательности, что гарантирует возможность проведения аудита, если он когда-либо потребуется.

4. Подтверждающие токены.

Обе стороны получают специальные цифровые токены, которые служат доказательством идентичности каждой из сторон в отношении заключенного ими соглашения. Эти токены будут использоваться для криптографического подтверждения того, что обе стороны подписали данное соглашение.

Помимо этих простых способов использования, смарт-контракты позволяют осуществлять индексируемое страхование, которое будет очень полезно для страхования в сельском хозяйстве и других областях, где ценность в значительной степени зависит от динамических факторов, которые могут быть точно задокументированы доверенной третьей стороной. Например, в подобном случае застрахованный фермер может получить автоматически начисляемые выплаты при наступлении определенных условий, таких как засуха, если информация об этом поступит из доверенной метеорологической базы данных. В результате его неизбежные потери будут автоматически компенсированы согласно договору о страховке.

Свидетельство для вас: Интернет вещей

Блокчейн-технология позволяет создавать новый тип свидетельств идентичности как для людей, так и для вещей. В традиционной модели они создаются, когда уполномоченные представители выдают сертификат. Для людей этот сертификат должен быть документом, таким как свидетельство о рождении или водительские права. Однако “вещи” тоже могут иметь подобные сертификаты, назначение которых — помочь потребителям оценить их качество и аутентичность.

С годами такие типы сертификатов постепенно теряли свое значение. При их создании использовались все более и более сложные способы защиты, но это лишь повышало их стоимость. Блокчейн-технология позволяет записывать подобные сертификаты в неизменяемый хронологический реестр, в котором любой сможет их найти и проверить. Дополнительной функцией в этом случае является возможность обновлять эти записи при возникновении новых событий того или иного рода.

Устройства Интернета вещей сейчас могут автономно публиковать любые типы данных в своих записях и обновлять сведения о текущем состоянии, в котором они находятся. Сейчас, когда эти устройства могут говорить сами за себя и имеют собственные истории и идентификационные записи, открыто опубликованные и доступные третьим лицам, страхование — это только одна из многих отраслей, в которых они могут найти свое применение.

Проекты Интернета вещей в области страхования

Весьма вероятно, что в будущем Интернет вещей окажет существенное влияние на три аспекта нашей жизни, обеспечив 1) соединение с автомобилем, 2) соединение с домом и 3) соединение с самим собой.

По своей сути Интернет вещей является подрывной технологией, и как таковой он радикально изменит широкий диапазон различных сфер нашей жизни,

таких как сведения об оригинальных производителях оборудования (ОЕМ) в автомобилестроении, защита жилища, провайдеры кабельных и сотовых сетей. Во всей этой мешанине найдется место и страховым компаниям, в частности тем, которые страхуют собственность и занимаются страхованием от несчастного случая.

Данные, собранные сенсорами в новых приборах и устройствах, вместе с информацией об установках автоматики и дополнительными параметрами управления, открывают новые возможности, когда речь идет о новых компаниях, появившихся в страховой отрасли. В комбинации с децентрализацией, свойственной блокчейн-реестрам, и смарт-контрактами весь процесс может быть автоматизирован до такого уровня, который был просто невозможен ранее.



ВНИМАНИЕ!

Новый стиль жизни, быть всегда в сети, пришедший со столь радикальными изменениями в технологиях, устраняет некоторые из существующих рисков, но при этом открывает дорогу новым, самым важным из которых является информационная защита. А это означает, что факторы риска должны быть просчитаны заново. Например, самоуправляемый автомобиль уменьшит для вас риск попасть в аварию, просто благодаря отсутствию человеческого фактора в его управлении, однако надежность этой технологии будет оставаться под вопросом, пока не будет собрано достаточно данных о его поведении непосредственно из реального мира.

Последствия появления действительно больших данных

Большие (по объему) данные стали важной проблемой начиная с 2000 года, а в наши дни эта проблема породила целую индустрию, оцениваемую в 200 миллиардов долларов, и имеет особенно большое значение для финансового сектора. Однако управление большими данными связано с несколькими трудностями, которые все больше проявляются даже в нашей повседневной жизни.

- » **Управление.** Если у вас есть большая многонациональная организация или консорциум, проблема совместного доступа к данным становится исключительно важной. Механизмы контроля версий все еще несовершенны и иногда сложно определить, какая копия является последней и наиболее актуальной среди прочих.
- » **Достоверность данных.** Как доказать, что именно вы, а не кто-либо иной, являетесь создателем данных, о которых идет речь?
- » **Монетизация и передача данных.** Как можно передать, купить или продать права на любые данные и при этом иметь гарантии, что существовать будет только одна их копия?

- » **Изменение данных.** Как можно убедиться, что данные не подвергались изменениям, если внесение в них каких-либо изменений не предполагалось?

Все эти проблемы вполне разрешимы при использовании криптовалюты и блокчейн-реестра. Самой большой трудностью, над которой сегодня работают в этой индустрии, является масштабирование блокчейн-технологии до размеров, которые будут соответствовать требованиям современных организаций в отношении объема и затрат на хранение их данных.

Устраняем третью сторону из страхования

Одним из величайших преимуществ, которое блокчейн-технология принесла в современный мир финансов, являются смарт-контракты, позволяющие совершать финансовые транзакции без привлечения третьей стороны, такой как банки или посредники.

Говоря простым языком, *смарт-контракт* представляет собой протокол, разрешающий двум сторонам записывать их транзакции в реестр блокчейна. Эти контракты могут использоваться практически для чего угодно, от обмена товарами (которые в этом случае должны иметь цифровые сигнатуры) до обмена информацией или деньгами.

В данном случае ключевым фактором безопасности, в отличие от обычных финансовых баз данных, является тот факт, что информация распространяется для проверки и сохранения между всеми компьютерами в сети, что делает ее хранение децентрализованным. Данные являются уникальными и их невозможно скопировать или изменить, что обеспечивает превосходные возможности для аудита.

Децентрализованная безопасность

В основе нынешней бизнес-модели лежит то, что можно назвать *парадигмой централизованного доверия*, согласно которой некий промежуточный участник, такой как банкиры, брокеры или юристы, координирует и обеспечивает достоверность финансовых транзакций и процедур обмена товарами.

Централизации свойственны некоторые неизбежные риски, такие как разрушение данных или их похищение. Блокчейн-технология борется с этими рисками посредством создания децентрализованной системы, работа которой построена на полном взаимном недоверии всех ее участников, которые по этой причине держат друг друга под постоянным контролем.

Чтобы построить такую систему, необходимо создать распределенный реестр, в котором будет использоваться криптовалюта (подобная биткойну, эфиру или фактому), и в которой каждый участвующий в работе системы является одновременно и ее пользователем, и лицом, отвечающим за ее техническую поддержку и сохранение.

Краудфандинговое страховое покрытие

Как и в случае обычных краудфандинговых инициатив, основная идея заключается в объединении в общий пул ресурсов, поступающих от многочисленных организаций или частных лиц, с целью покрытия непредвиденных недостатков в плане страхования. Например, план пенсионного страхования активизируется только при достижении возраста 65 лет, но человек может быть вынужден уйти на пенсию раньше из-за непредвиденных обстоятельств, и этому несчастному, весьма вероятно, потребуются дополнительные фонды.

Экономическое неравенство возрастает из года в год, и множество недостаточно застрахованных или вообще не застрахованных людей могли бы получить пользу от такой системы. Механизм краудфандинга в потенциале может принести пользу всем трем сторонам в рассматриваемой ситуации.

- » **Страховщики** выигрывают за счет увеличения дохода, поскольку больше людей будет заинтересовано в их страховых планах. Иначе говоря, они получают доступ к большей доле незастрахованного населения. Кроме того, страховые компании смогут улучшить узнаваемость их бренда — их можно будет позиционировать как компании, проявляющие заботу о людях.
- » **Жертвователи** получают выигрыш от возможного освобождения от налогов, если структура компании это допускает. Для них также возможно получение и других преимуществ, таких как скидки или бесплатное обслуживание.
- » **Соискатели** (те, кто нуждается в страховке), безусловно, окажутся в наибольшем выигрыше, так как смогут получить наилучшую страховую защиту и более доступное для них покрытие.

Компания Cognizant предлагает интересный собственный взгляд на краудфандинговое страхование, который они изложили в основополагающем документе (whitepaper) своей компании. Ознакомиться с ним можно на веб-странице <https://goo.gl/u3Kd3U>.

Использование DAO как системы страхования

Децентрализованные автономные организации (DAO) — это корпоративные организации, которые не имеют постоянных наемных работников, но способны выполнять все функции, свойственные обычным корпорациям. Возможность создавать такие организации напрямую связана с улучшениями в блокчейн-алгоритмах, которые имели место за последние несколько лет и привели к созданию того, что сейчас называется “блокчейн 2.0”.

В сущности, децентрализованная автономная организация представляет собой некоторую форму “продвинутого” смарт-контракта. Эта организация способна вести себя как корпорация, в которой все акционеры принимают непосредственное участие в определении политики ее поведения, но при этом сама корпорация не находится под прямым контролем какой-либо определенной группы или отдельного лица.

По этой же причине любая децентрализованная автономная организация никогда не контролируется ее разработчиками и они не имеют возможности вводить или отклонять правила ее поведения. В результате мы получаем строгую пиринговую, децентрализованную модель страхования. Хотя уязвимости в отношении проверки подлинности здесь все еще существуют, эта система непременно будет улучшаться, а в реальности такие же проблемы существуют даже в современных централизованных системах страхования.



Глава 15

Блокчейн и государство

В ЭТОЙ ГЛАВЕ...

- » Чтение блокчейн-документов
- » Построение смарт-городов
- » Создание идентичности, защищенной от взлома

В этой главе речь пойдет о захватывающих нововведениях, которые сейчас имеют место в правительственных кругах разных стран и поддерживающих их компаниях и происходят благодаря инновационным проектам, базирующимся на блокчейн-технологии.

Повседневный бизнес, к сожалению, подвержен аферам и жульничеству, и в этой главе будет рассказано, как правительства в разных странах ведут борьбу с киберпреступностью и хищениями свидетельств подлинности. Также вы узнаете об инициативе создания смарт-городов, что может стать решающим фактором экономического роста и устойчивого развития — и во многих случаях именно блокчейн-технология здесь используется для наведения мостов через провалы в технологии.

Смарт-города в Азии

Смарт-города используют преимущества современной технологии для расширения функциональных возможностей своей инфраструктуры, обеспечения безопасности и проведения улучшений в таких проблемных областях, как городской трафик и качество воздуха. Превращение городов в смарт-города как бизнес активно расширяется, и муниципалитет почти каждого более-менее крупного города уже принял концепцию смарт-городов.

Блокчейн-технология особенно полезна в вопросах интеграции с Интернетом вещей (IoT), активно проводимой в смарт-городах. Несколько интересных проектов уже запущены в пилотном режиме с целью коммерческого развертывания. Министерство внутренней безопасности США исследует защищенность IoT-устройств, используемых Службой таможенного и пограничного контроля (Customs and Border Protection — CBP). Компании, такие как Slock.it, предоставляют подключенным устройствам возможность использовать блокчейн для входа в смарт-контракты. Их первым продуктом был смарт-замок, имеющий доступ к блокчейну, который мог бы использоваться клиентами компании Airbnb, предоставляющей через Интернет услуги кратковременной аренды жилья по всему миру. Интеграция этих технологий позволяет данным устройствам использовать их сенсоры для настройки смарт-контрактов. Аналогичная технология может использоваться и для городских парковочных счетчиков.

На рис. 15.1 представлена домашняя страница Сингапурского проекта Smart Nation. Сингапур собрал стартапы со всего мира с целью разработки приложений этой новой технологии в пределах его “регулируемой песочницы”. Это поистине радужное приглашение для компаний, занимающихся блокчейн-технологией, которые до этого времени вынуждены были работать в *серой зоне* (полулегальная среда, в которой еще нет четкого правового оформления и регулирования). Хотя следует сказать, что многие страны, как и Сингапур, уже предпринимают конкретные усилия для определения правового пространства и четкого указания таким компаниям, что им разрешено, а что — нет.

Блокчейн-технология также может использоваться в смарт-городе для безопасного распространения информации между сетями. Сейчас многие города исследуют методы использования блокчейн-технологии для смягчения ситуации с транспортными пробками. Сингапурский проект Smart Nation предполагает использование мобильных телефонов своих горожан для анализа условий автобусных поездок, которые они совершают. Собранные данные затем предполагается анализировать с целью выяснения, когда существующую дорожную сеть необходимо будет модернизировать. Сингапур является лидером в разработке концепции смарт-города и уже начал оказывать услуги по разработке смарт-городов в других странах.



Рис. 15.1. Сингапурский проект Smart Nation

Далее в этом разделе мы обсудим некоторые из многих попыток реального применения блокчейн-технологии, предпринимаемых в настоящее время в Азии.

Города-спутники в Индии

В 2015 году правительство Индии запустило проект Smart Cities Mission, согласно которому в этой стране предстоит построить 100 новых смарт-городов. Многие из этих новостроек будут расположены в так называемом “промышленном коридоре” между городами Дели и Мумбаи, общей протяженностью 1000 км. Инфраструктура общей стоимостью 11 млрд. долларов уже распланирована между 33 городами, и большая часть этих разработок будет финансироваться по модели государственно-частного партнерства. Ожидается, что проект привлечет до 90 млрд. долларов иностранных инвестиций, которые будут использованы для создания бизнес-парков, производственных зон и смарт-городов, расположенных вдоль выделенного железнодорожного грузового коридора.

Эти смарт-города разрабатываются в целях индустриализации индийской экономики и повышения уровня урбанизации населения страны. Государственное вмешательство в форме централизованного планирования городов необходимо в целях предотвращения чрезмерного перенаселения уже существующих

городов. Индия особенно уязвима к изменению климата из-за ее огромного и в своей массе очень обедневшего населения. По этой причине очень важно, чтобы новые города были жизнеспособными и продуманными. Они нуждаются в низкоэнергетических строительных материалах, интеллектуальных сетях, эффективной транспортной системе, интегрированных ИТ-системах, электронном управлении и инновационном водоснабжении.

Сингапур является первым примером разумно спланированного города. Несмотря на высокую плотность населения, он обладает превосходной инфраструктурой и обеспечивает высокое качество жизни. Многие из частных организаций Сингапура обладают знаниями и ресурсами, которые просто необходимы для разработки индийских смарт-городов. В сотрудничестве с индийским правительством частный сектор способен предоставить капитал, практический опыт и технологии, которые требуются для реализации столь обширных планов.

Власти индийского штата Андхра-Прадеш и Денежно-кредитное управление Сингапура объявили об инновационном партнерстве в области финансовых технологий, где главное внимание уделяется блокчейн-технологии и цифровым платежам. Целью Сингапура является разработка интерактивной рыночной площадки для инновационных финансовых решений в Индии.

Руководство Сингапура проявило интерес к партнерству с Индией в разработке смарт-города, а также новой столицы штата Андхра-Прадеш, расположенного на юго-востоке страны. Были организованы комитеты для анализа потенциала сотрудничества с Индией в отношении ее плана построения 100 новых городов, а также в отношении дальнейшей разработки инфраструктуры 500 уже имеющихся городов и мегаполисов.

Министр городского развития Индии вел переговоры и с нынешним, и с предыдущим премьер-министрами Сингапура. Он интересовался опытом Сингапура в создании смарт-городов, уделяя особое внимание интеллектуальным транспортным системам, улучшенному управлению водными ресурсами и электронному управлению. Министр городского развития также изучал схемы создания государственного жилья Сингапура и действующие здесь правила жилищного строительства. Был проявлен интерес и к схемам финансирования транспортной инфраструктуры.

Индийские власти также привлекли группу сингапурских экспертов для участия в разработке города-спутника в штате Химачал-Прадеш. Этот проект, общей площадью 20 га, предназначен для разгрузки перенаселенного города Шимла, в котором за последние десятилетия отмечался чрезмерно быстрый рост населения. Цель сингапурской команды — оказать индийским разработчикам помощь в проработке образовательных, жилищных и коммерческих аспектов проектируемого нового города.

Как Сингапур, так и Малайзия проявили интерес к инвестированию в другой город-спутник рядом с храмом Джатия Деви, недалеко от города Шимла, столицы штата Химачал-Прадеш. Правительство Сингапура проводит исследование с целью оценки различных вариантов. Правительство штата Химчал-Прадеш рассматривает проект создания пяти городов-спутников вблизи уже существующих городов с использованием частногосударственной модели финансирования.

Сингапурская корпорация Ascendas-Singbridge запустила проект создания в Индии своего восьмого научно-технологического парка. Как ожидается, первое здание Международного технологического парка Гургаон (International Tech Park Gurgaon), расположившегося на территории 24 га, будет завершено к середине 2017 года. Этот проект, общей стоимостью 400 млн. долларов, предусматривает создание 720 тыс. м² бизнес-площади, на которой будут размещаться компании бурно растущего IT-сектора индийской экономики.

Китай и проблема больших данных

Блокчейн-технология широко обсуждалась в Китае как возможное средство повышения надежности больших данных. Она рассматривалась, прежде всего, как способ решения проблемы доверия, связанной с совместным использованием данных двумя и более сторонами, не имеющими общих побудительных мотивов. Блокчейн-технология предлагает много новых решений для отслеживания свидетельств собственности, происхождения или идентичности.

Компания Peernova — это многообещающий стартап из США, направляющий основные усилия на решение проблем больших данных. Изначально он фокусировался на майнинге в системе Биткойна, но затем переориентировался на общее применение блокчейн-технологии и привлек инвестиции на сумму 4 млн. долларов от холдинга Чжэцзян Чжуннань, строительной компании из Китая. В своих разработках Компания Peernova планирует использовать блокчейн-технологию опрашивания традиционных баз данных и отслеживания изменений.

Возможные варианты использования включают проверку любых изменений в подмножествах больших хранилищ данных и использование более эффективного и полного криптографического аудита вместо традиционного аудита с целью предоставления ориентира для компании. Также предполагается оказать помощь хедж-фондам в вычислении налоговой ответственности по их инвестициям с использованием блокчейна для отслеживания многолетней истории инвестирования денежных средств.

Корпорация Dalian Wanda, крупнейший разработчик по недвижимости в Китае, тоже проявила определенный интерес к блокчейн-технологии. Она объединилась с компанией Cloudera, занимающейся разработкой ПО больших

данных, с целью запуска блокчейн-проекта, получившего название “Hercules”. Как предполагается, блокчейн-технология обладает большим потенциалом в отношении ее использования для получения прогнозов на основании больших данных, имеющих важное значение для менеджеров, по мере их поступления. Это позволит менеджерам вместо реагирования на уже возникшие события предпринимать необходимые превентивные действия в таких ситуациях, как модификация их протоколов, а также проводить мониторинг поведения пользователей в их системах.

Корпорация Dalian Wanda и компания Cloudera намерены продолжать развитие проекта Hercules и интегрировать свои новые технологии в различные отрасли, полагающиеся на информационные технологии и большие объемы данных. Проект Hercules будет реализован как пакет с открытым кодом, предназначенный для поддержки нужд бизнеса. Его назначение — упростить для организаций развертывание блокчейн-приложений на больших кластерах данных.

Вам может показаться довольно необычным партнерство компании, начинавшей с майнинга цифровой валюты, с обычной строительной компанией, образованное с целью решения задач аудита хедж-фондов или же решения проблем системных администраторов в компаниях по недвижимости, работающих с большими данными. Тем не менее это так — это мир блокчейн-технологии и это действительно Дикий Запад. В мире блокчейна недостаток талантов и высокий спрос на проекты и инвестиции — вот что подпитывает эту среду.

Битва за статус финансовой столицы мира

Блокчейн-технология вступила в свои права с момента ее проникновения в общественное сознание благодаря бурному потоку новостей, имевшему место в 2015 году. С тех пор множество стартапов начали работать над бета-версиями и предварительными сборками своих проектов — почти 2000 новых блокчейн-стартапов были сформированы только в преддверии 2016 года. Многие из них в конечном счете появятся на рынке в 2017 и 2018 годах в Сингапуре, эмирате Дубай и Лондоне, где контролирующие органы приветствуют инновации и где идет ожесточенная конкурентная борьба за право стать финансовой Меккой для всего мира. Для этих лидеров речь здесь идет не только о новых финансовых технологиях и смарт-городах. Это, прежде всего, погоня за релевантностью по отношению к миру, смещающемуся к не знающим границ и глобально финансово подвижным гражданам.

Первые блокчейн-инициативы Лондона

В 2016 году правительство Великобритании опубликовало отчет под названием “Технология распределенного реестра: помимо блокчейна” (<https://goo.gl/asIz6L>), в котором утверждалось, что технология распределенного реестра (блокчейна) может быть использована для снижения уровня коррупции, ошибок и мошенничества, что позволит сделать многие процессы значительно более эффективными. Здесь также утверждалось, что блокчейн-технология способна изменить отношения между гражданами и правительством за счет обеспечения большей прозрачности и надежности. Однако в действительности власти в Лондоне были очень дружелюбно настроены к этой технологии по крайней мере еще с 2014 года. Многие ранние блокчейн-стартапы были зарегистрированы или работали в Лондоне, поскольку неофициально это было самое безопасное место для ведения такого бизнеса. В те времена это было очень важно, поскольку многие предприниматели мира криптовалют были арестованы в 2014 и 2015 годах.

С момента опубликования этого отчета блокчейн-технология была одобрена для использования в приложениях, создаваемых для центрального правительства Великобритании, включая департаменты Белого дома (не министерские департаменты, такие как Земельный регистр, Комиссия по лесному хозяйству и Агентство по пищевым стандартам), для местных властей и для делегированных правительств Шотландии, Уэльса и т.д.

Вот несколько интересных проектов и экспериментов, которые имели место в Великобритании.

- » **Распределение социальной помощи на основе блокчейна.** Министерство труда и пенсий в партнерстве с банком Barclays, компанией RWE и стартапом GovCoin из университетского колледжа Лондона начали эксперимент, в котором блокчейн-технология будет использоваться для распределения социальной помощи с использованием приложения для смартфонов. В пробной версии предполагается проанализировать возможности проведения платежей и их отслеживания с использованием блокчейн-технологии.
- » **Правительственный распределенный регистр.** Компания Credits, провайдер блокчейн-платформы, и правительство Великобритании сотрудничают в вопросе создания рабочей среды, которая позволит агентствам правительства Великобритании проводить эксперименты по использованию блокчейн-технологии.
- » **Международные платежи на основе блокчейн-технологии.** Банк Santander запустил пробную версию блокчейн-системы международных платежей. Пилотная программа для персонала включает

приложение, которое подключается к платформе Apple Pay. Пользователи могут использовать сенсорный интерфейс для проведения платежей в пределах от 10 до 10 000 фунтов.

- » **Использование блокчейн-технологии для торговли золотом.** Королевский монетный двор объединился с компанией CME Group, оператором рынка, с целью использования блокчейн-технологии для создания рыночной платформы торговли золотом в надежде сделать Лондон более привлекательным городом для торговых операций с золотом.

Все приведенные выше примеры имеют целью доказать, что блокчейн-технология действительно является надежной новой платформой для обмена ценностью. Успех или провал этих начинаний определит будущий курс Великобритании и всего остального мира в отношении этой инновации.

Регулируемая песочница Сингапура

Сингапур, как и Великобритания, избрал собственный вариант сделать работу в нем в области блокчейн-технологии настолько простой, дружелюбной и финансово привлекательной, насколько это возможно. В 2015 году представители правительства Сингапура отправились в Сан-Франциско, чтобы сделать официальное заявление и привлечь предпринимателей к работе в том окружении, которое они называли “регулируемой песочницей”, обыграв в этом названии программистский термин *песочница разработчика*, которым называют безопасную среду, в которой разработчики могут создавать и тестировать свое программное обеспечение. Власти Сингапура имели в виду ту же самую идею — безопасную среду для создания компаний по разработке ПО.

На тот момент компании, занимавшиеся блокчейн-технологией, как в США, так и во многих других странах все еще находились в серой зоне с точки зрения закона. Идея безопасного места, где можно будет работать и инвестировать в эти разработки средства, оказалась чрезвычайно привлекательной для многих предпринимателей, включая и меня (автора этих строк). Если вы еще не были в Сингапуре, вам следует обязательно его посетить! Это красивый, чистый и безопасный город.

Сингапур предпринял необходимые шаги в исследовании новой технологии — и это принесло плоды. Сингапурский банк, OCBC, использовал блокчейн-технологии для перемещения средств за границу. Он отправлял средства своим дочерним компаниям, OCBC Malaysia и Bank of Singapore.

Компания R3 также проявляла активную деятельность в Сингапуре. Она совместно с Денежно-кредитным управлением Сингапура открыла лабораторию для проведения исследований и разработок в области технологии цифровых

регистров. Компания R3 работает на бирже для поддержки межбанковских платежей, где банки получили возможность вносить наличные деньги и получать цифровую валюту.

Центральный банк Сингапура также запустил свой пилотный проект совместно с восемью иностранными и местными банками и с валютной биржей. Этот проект подтверждения концепции имеет целью использование блокчейн-технологии для проведения межбанковских платежей в пределах этой банковской группы. В пилотном проекте также преследуется цель проанализировать возможность проведения внешних транзакций в иностранной валюте.

Следует отметить, что не только блокчейн-компании проводят свои эксперименты в Сингапуре. В эти игры вовлечены и более крупные игроки — банки Bank of America, Merrill Lynch, Bank of Tokyo-Mitsubishi UFJ Ltd, DBS Bank Ltd, Hong Kong and Shanghai Banking Corp Ltd, OCBC Bank, United Overseas Bank, финансовые конгломераты Credit Suisse и JP Morgan, корпорация IBM и Сингапурская биржа.



СОВЕТ

Каждый банк во всем мире должен знать, кем является тот, с кем он ведет дела. Эта концепция носит общее название “Знай своего клиента” (Know Your Customer — KYC) и имеет целью препятствовать отмыванию денег и финансированию терроризма.

Следующим этапом будет определение транзакций в иностранной валюте на основе решений Сингапура в отношении поддержки требований KYC. Это может привести страну к необходимости впервые в мире проложить путь к реализации обеспечения идентичности личности на основе блокчейн-технологии. Кстати, в Сингапуре уже сейчас имеется надежная и современная цифровая система обеспечения идентичности, которую будет относительно несложно подключить к блокчейну.

Инициатива “Дубай-2020”

Правительство эмирата Дубай приняло амбициозный план: к 2020 году перенести все правительственные документы и системы в блокчейн. В соответствии с этой инициативой предусмотрен полный отказ от бумажных документов, что делает эту страну мировым лидером в использовании блокчейн-технологии и резком повышении эффективности во всех сферах жизни общества.

Министр по делам Кабинета министров и будущему детализировал, как новая схема позволит пользователям обновлять и проверять свои полномочия через блокчейн. Им потребуется лишь один раз войти в систему со своими учетными данными, чтобы получить доступ как к государственным, так и к частным объектам, таким как страховые компании и банки. В эмирате Дубай

также допускают возможность разделить их технологию с другими странами, что позволит упростить пересечение границ. Вместо паспортов путешественники смогут использовать предварительно аутентифицированные цифровые кошельки либо предварительно утвержденные свидетельства идентификации.

Правительство эмирата Дубай предварительно оценило, что их блокчейн-инициатива в потенциале позволяет сохранить 25,1 млн. часов продуктивной деятельности. Этот резкий скачок в эффективности также будет способствовать сокращению выбросов в атмосферу углекислого газа.

Глобальный совет по блокчейну эмирата Дубай объявил о создании семи новых государственно-частных совместных проектов, в которых объединяются усилия и ресурсы стартапов, местного бизнеса и правительственных подразделений. В этих проектах блокчейн-технология будет применена в следующих областях.

- » **Здравоохранение.** Эстонская компания Guardtime, занимающаяся разработкой ПО, будет сотрудничать с компанией Du, крупнейшим оператором телекоммуникаций в эмирате Дубай, с целью проведения технологической экспертизы по оцифровке записей системы здравоохранения и их перенесения в блокчейн.
- » **Торговля алмазами.** В соответствующем пилотном проекте блокчейн-технология будет использоваться для аутентификации и отслеживания перемещения алмазов. В Дубайском мультитоварном центре будет проведена оцифровка *сертификатов Кимберли* (документов, созданных ООН для ограничения торговли спорными алмазами).
- » **Передача титулов собственности.** Титульные документы на право собственности будут оцифрованы и записаны в блокчейн. Сингапурский блокчейн-стартап, известный как Dxmarkets, уже разработал соответствующий проект подтверждения концепции.
- » **Регистрация бизнеса.** Глобальный блокчейн-совет (GBC) исследует возможности использования блокчейн-технологии для регистрации бизнеса. В данном случае речь идет не о децентрализованных автономных организациях (DAO) проекта Эфириум, а о возможности упрощения проверки подлинности с помощью программы Flexi Desk. В настоящее время этот проект находится на стадии демо и включает несколько объектов, используемых для подтверждения концепции.
- » **Туризм.** Пилотная программа Dubai Points, запущенная в сотрудничестве со стартапом Louyal, предусматривает использование блокчейн-технологии в помощь туристической индустрии. Ее целью является повышение заинтересованности в туристических поездках

посредством предоставления путевок путешественникам, которые посетили определенные места. Для упрощения процедуры предоставления наград предполагается использование смарт-контрактов. Эти путевки во многом будут похожи на криптовалюты, поскольку ими можно будет торговать или вести обмен.

- » **Морские перевозки.** Корпорация IBM в сотрудничестве с Глобальным блокчейн-советом (GBC) работает над использованием блокчейн-технологии для улучшения морских перевозок товаров и для логистики. Целью программы является оказание помощи местным компаниям в сотрудничестве по вопросам обмена товарами. Как решение в вопросах соблюдения договорных условий и урегулирования разногласий предполагается использование смарт-контрактов.

Эмират Дубай, как и Сингапур, вложил свои деньги и таланты в обеспечение того, чтобы в скором времени он смог доминировать в блокчейн-пространстве. Это одно из неоспоримых преимуществ маленького правительства и централизованной власти.

Регулирование посредством битлицензий: город Нью-Йорк

Если вы намереваетесь запустить блокчейн-стартап в городе Нью-Йорке, будьте готовы к дополнительным расходам. В июне 2015 года Нью-Йоркский департамент финансовых услуг (New York State Department of Financial Services — NYDFS) принял окончательную версию *битлицензии*, нормативно-правовой базы для цифровых валют, предназначенной для предоставления этой отрасли большей ясности в правовом отношении. В действительности это решение просто вытолкнуло многие блокчейн-стартапы за пределы Нью-Йорка. Эта лицензия сама по себе стоит 5 тыс. долларов, а размер ее может достигать 500 страниц. Она предусматривает получение отпечатков пальцев всех лидеров компании и, что еще хуже, обширные проверки всевозможных данных в применении к вашему бизнесу. Неизбежные расходы, связанные с подачей заявки, можно оценить примерно в 100 тыс. долларов. Эта сумма включает затраты времени, юридические и дополнительные сборы. В результате битлицензия находится в полном противоречии с теми мерами по развитию блокчейн-технологии, которые принимаются в других финансовых центрах мира, таких как Лондон, Сингапур или Дубай.

Окончательная версия битлицензии является результатом почти двух лет исследований и дебатов по поводу того, как данная технология должна регулироваться. Все это началось после того, как было решено, что существующие правила не подходят для компаний, занимающихся цифровыми валютами.

Есть и хорошая новость: Нью-Йоркский блокчейн-бизнес больше не нуждается в одобрении со стороны NYDFS для очередных обновлений программного обеспечения или проведения дальнейших раундов финансирования венчурного капитала. Согласно документам нормативно-правовой базы только компании, занимающиеся цифровыми валютами, должны получить одобрение для изменений, которые “предлагаются к существующему продукту, услуге или деятельности, которые могут привести к тому, что такой продукт, услуга или деятельность будет существенно отличаться от того, что ранее было указано в заявке на лицензирование суперинтендантом”.

Первой компанией, получившей битлицензию, была Circle, компания — провайдер биткойн-кошельков. Эта лицензия позволяла им работать в Нью-Йорке в пределах установленной нормативно-правовой базы. Компания Circle — одна из очень немногих компаний, которые имеют право легально заниматься своей деятельностью. Большинство блокчейн-стартапов сейчас просто отказываются работать в Нью-Йорке, поскольку финансовые издержки и объем необходимых усилий превышают любой возможный выигрыш. Только очень хорошо финансируемые стартапы могут позволить себе приложить требуемые для получения усилия.

А вот компанию Ripple вынудили получить даже вторую лицензию. Эта итерация процесса ее лицензирования должна была обеспечить ей право хранить и продавать цифровую валюту XRP, которая является тем цифровым токеном, на котором строится функционирование ее блокчейна Ripple Consensus Ledger (RCL). Наличие этой второй лицензии позволило компании Ripple на законном основании вести дела с теми бизнес-клиентами, которые хотели бы использовать ее технологии для международного перемещения фондов.

В прочих регионах США также были приняты аналогичные законопроекты по регулированию цифровых валют с требованием лицензирования. В штате Калифорния подобные требования должен был ввести законопроект AB 1326, однако он не был принят после того, как Фонд электронных рубежей (Electronic Frontier Foundation — EFF) выступил против него. Фонд EFF — это некоммерческая правозащитная организация, базирующаяся в Сан-Франциско, поставившая своей целью защиту прав потребителей и создателей новых технологий.

Блокчейн на защите границ всего мира

Правительства многих стран исследовали блокчейн-технологии как инструмент обеспечения защиты их границ. В Великобритании была поставлена амбициозная цель добиться гарантий, что прибывающим в ее аэропорты пассажирам

больше не придется испытывать каких-либо задержек на пути к выходу. Это заявление резко контрастирует с длинными очередями к пропускным контрольным пунктам, которые сейчас можно обнаружить практически в любом аэропорту мира. Основная сложность, которую Великобритания должна преодолеть в этом вопросе, состоит в умении *опознавать пассажира*, т.е. способности абсолютно точно узнавать любое представленное пассажиром свидетельство его идентичности, даже если он прибыл из другой страны. Оpozнание пассажиров является важной проблемой для всех стран, ведущих борьбу с терроризмом.

США рассекретили свою технологию опознания пассажиров в Системе оценки глобальных путешествий (Global Travel Assessment System — GTAS). Более подробные сведения о ней можно найти на сайте GitHub (<http://www.github.com/US-CBP/GTAS>).

Компьютеры, камеры и сенсоры, используемые для внешнего сканирования и аутентификации пассажиров, должны быть достаточно надежными и хорошо защищенными, чтобы гарантировать национальную безопасность. Блокчейн-технология, обладающая качеством гарантированной неизменяемости данных, является весьма многообещающей технологией для использования в подобных случаях. Этот подход сейчас тщательно тестируется.

Другое интересное применение, которое может быть реализовано с использованием блокчейн-технологии, — это создание биографической идентичности, т.е. свидетельства идентичности, которое строится с течением времени. С биографическим свидетельством идентичности могут быть связаны любые данные, а конфиденциальность и удобочитаемость связанных данных может контролироваться теми, кто их публикует. С течением времени такое свидетельство пополняется дополнительными атрибутами. Атрибуты могут быть чем угодно, начиная с характеристик личных коммуникационных устройств и заканчивая сведениями о том, что документы были проверены при пересечении границы. Все эти атрибуты помещаются в личную цепочку свидетельства идентичности органами сертификации или теми, кто был уполномочен на это органами сертификации.

Министерство внутренней безопасности и идентичность вещей

Министерство внутренней безопасности США совместно с Научно-техническим управлением проводят исследование защищенности устройств Интернета вещей (IoT) в отношении границ Соединенных Штатов. Работа ведется с участием корпорации Factom со штаб-квартирой в городе Остин, штат Техас. Эта корпорация представляет собой блокчейн-стартап, работающий в области улучшения защиты цифровых свидетельств идентичности для IoT-устройств.

В корпорации Factom разработали учетные записи, в которых фиксируются ID-устройства, сведения об изготовителе, перечень доступных обновлений, известные проблемы с защитой и сведения о доверенных контактах вместе с отметками времени для повышения защищенности. Целью является ограничение потенциальных возможностей повреждения прежних записей для устройства, что усложняет хакерам задачу их спуфинга (подмены).

Паспорта будущего

Компания ShoCard (<http://www.shocard.com>) занимается разработкой приложений, работающих с использованием блокчейна, созданного компанией Blockscyrpher. Были созданы прототипы, позволяющие создать собственное свидетельство идентичности личности в защищенной среде блокчейна. Доступ к созданному программой от ShoCard идентификатору будет предоставляться приложением на смартфоне и может применяться для защищенного использования всевозможных видов учетных данных.

Новый тип документов

Возможно, вы слышали о компании Smartrac, однако куда более вероятно, что вы уже не раз держали в руках какие-то элементы ее технологии. Компания Smartrac — это ведущий производитель радиочастотных идентификаторов (RFID) и других идентификационных чипов, которые помещаются внутрь таких вещей, как паспорта или ID-карточки.

Одной из самых больших проблем, с которыми страны сталкиваются при борьбе с хищениями свидетельств подтверждения личности, является аутентификация базовых документов, на основании которых было выдано свидетельство идентичности. Это такие вещи, как карточки социальной защиты, свидетельства о рождении, различные дипломы и прочие документы, которые в наше время можно быстро и недорого состряпать.

Компания Smartrac билась над решением этой проблемы много лет, используя все более и более сложные технологические решения. Ее последней разработкой является технология dLoc, предусматривающая использование клейких стикеров и специального программного обеспечения аутентификации, что обеспечивает возможность сверить документ с соответствующей записью в блокчейне.

Данные документа связываются с уникальным идентификатором, размещенным на коммуникаторе ближней идентификации и наклеенным на документ, посредством создания 32-битового хеша, который может быть распознан только выпустившим его агентством при указании закрытого ключа. Значение хеша помещается в облачное хранилище и записывается в открытый блокчейн,

после чего документ со стикером dLoc может быть проверен уполномоченным лицом с помощью настольного ридера или смартфона, оборудованного NFC-ридером.

Все это позволяет реализовать две замечательные возможности, которые прежде были просто неосуществимы для бумажных документов.

- » Сохранение неизменяемой истории документа, свидетельствующей о его истинных возрасте и владельце.
- » Возможность для сертифицирующих органов криптографически подписывать свидетельства аутентичности документа. В результате, если базовый бумажный документ будет похищен (или скопирован) до наклейки на него стикера dLoc, на нем не будет адекватной подписи, а если он исчезнет уже после его регистрации, у владельца останется возможность отметить этот документ как украденный.



Глава 16

Прочие применения блокчейна

В ЭТОЙ ГЛАВЕ...

- » Познакомьтесь с инициативами правительств, избравших собственную линию поведения.
- » Узнайте об улучшениях в уровнях инфраструктуры Интернета для вашего бизнеса и дома
- » Создайте собственное свидетельство вашей личности в блокчейне
- » Монетизируйте свою информацию с помощью смарт-контрактов

В этой книге мы уже обсудили наиболее заметные блокчейн-проекты и их воздействие на соответствующие области общественной жизни, однако сейчас блокчейн-технология так или иначе уже коснулась практически всех ее аспектов.

В этой главе речь пойдет о нескольких иных интересных и необычных применениях блокчейн-технологии, о таких, о которых вы даже не подозревали. Некоторые из наиболее удивительных трансформаций произойдут в правительственных системах, выразятся в появлении новых уровней доверия для Интернета и возникновении новых направлений предпринимательской деятельности, ставших возможными благодаря блокчейн-технологии. Здесь вы

также узнаете о наиболее впечатляющих изменениях, которые происходят уже сейчас, и о том, как эти изменения повлияют на вашу жизнь, на ту сферу общественной деятельности, в которой вы работаете, и на правительственные ведомства и учреждения, которые обеспечивают вашу защиту.

Правительства, отклонившиеся от общепринятых (пока) норм

Некоторые небольшие страны пришли к заключению, что для того чтобы успешно конкурировать в глобальной экономике, необходимо предложить больше и сделать это таким образом, чтобы не обременять своих граждан. Для того чтобы конкурировать на международном рынке, они должны отказаться от многих традиционных понятий относительно “предоставления гражданства”. В мире, который постепенно переходит от жестких непроницаемых границ к границам более проницаемым и условным, когда люди получают возможность выбирать, где им жить и какую страну называть своим домом, эти маленькие страны преуспевают.

Гражданство становится товаром, продуктом потребления, который можно заказать и приобрести, при этом каждая нация предоставляет своим гражданам разные преимущества. Страны постепенно отходят от модели пассивного гражданства, когда вы просто рождаетесь гражданином своей страны, к такой модели, где вы можете выбрать гражданство, исходя из тех преимуществ, которые предлагает та или иная страна.

Исходя из этой новой модели, гражданство больше не привязано жестко к физическому местонахождению. Правительство может существовать и без границ или некоторого физического местоположения. В прежних моделях гражданство всегда определялось конкретным физическим местоположением, которое могло быть захвачено, в результате чего прежнее гражданство аннулировалось другой нацией или внутренними силами, например как следствие революции.

Блокчейн-технология и другие инновации высшего класса активно воспринимаются в таких регионах, — во-первых, потому что они делают их существование возможным, а во-вторых, потому что они помогают снизить нагрузку на правительство, позволяя создать более эффективные системы, доступ к которым граждане могут при необходимости получить в любом уголке мира, даже если физически территория страны была захвачена.

Такие страны, как Сингапур, Эстония и Китай, можно считать признанными лидерами в подобном типе инициатив. Реализации концепций смарт-нации в

Сингапуре и электронного резидентства в Эстонии представляют собой уникальные системы, которые направлены на сокращение бумажной работы и затрат времени граждан, а также на повышение эффективности разделяемых ресурсов. А усилия Китая по сокращению мошенничества существенно изменили динамику развития блокчейн-пространства.

Сингапурский проект смарт-нации

Проект смарт-нации (Smart Nation) Сингапура — это попытка в национальных масштабах улучшить в будущем жизнь всех граждан этой страны и тех, кто в ней проживает временно. Люди, бизнес-структуры и правительство работают сообща. Проект охватывает самые разные аспекты общественной жизни — от использования цифровых свидетельств идентичности до обширной сети сенсоров в Интернете вещей, позволяющих оптимизировать работу государственных служб.

В Сингапуре убеждены, что люди, наделенные новейшими технологиями, смогут вести более осмысленную и наполненную жизнь. Здесь новые технологии, сети и большие данные в полной мере используются для ведения полномасштабного и активного поиска новых идей и методов через “регулируемые песочницы”, активную вербовку и стимуляцию инновации от стартапов.

Красочный рисунок с кратким описанием передового Сингапурского проекта можно найти на веб-странице <https://goo.gl/EGmF4X>.

Сингапур имеет возможность быстро протестировать и развернуть новую технологию, поскольку в его правительстве имеется только один уровень. Это позволяет эффективно координировать политические усилия и действия государственных структур. Проект смарт-нации — это превосходный пример популярной доктрины о том, что новая технология всегда одерживает верх над политикой.

Эстонская инициатива электронного резидентства

Эстония — это маленькая страна, входящая в состав Европейского Союза и насчитывающая всего 1,3 млн. жителей. У нее очень мало ресурсов для удовлетворения нужд своих граждан, но благодаря технологиям она оказалась способной превзойти возможности многих более крупных наций. В Эстонии развернута система цифровых ID-карточек, предназначенных для использования в интерактивных службах, и она стала первой страной, предложившей всему миру концепцию *электронного резидентства* (*e-Residency*), т.е. цифрового свидетельства личности, доступного любому человеку во всем мире, заинтересованному в ведении бизнеса интерактивно.

Получение электронного резидентства в Эстонии отнимет у вас всего несколько минут, а стоимость проведения фоновой проверки ваших данных обойдется вам чуть меньше 100 долларов. Получение карточки электронного резидентства не делает вас гражданином Эстонии, но предоставит вам много иных преимуществ.



СОВЕТ

Вы тоже можете получить электронное резидентство в Эстонии. Для этого просто зайдите на сайт <https://apply.gov.ee>.

После выхода из состава Советского Союза Эстония сделала очень большие инвестиции в новые технологии. Она полностью отказалась от концепции традиционного управления и обратилась к тому, что здесь называют *принципом одного окна* (т.е. одна точка доступа). Этот принцип предусматривает для граждан страны возможность доступа ко всем налоговым и таможенным службам с помощью одного защищенного логина из любого места в мире, где есть Интернет. Эта система обеспечивает возможность выполнения простых и понятных безбумажных транзакций, при этом практически все, за исключением женитьбы и приобретения недвижимости, может быть выполнено полностью в интерактивном режиме. Граждане Эстонии могут провести любой банковский перевод или уплатить налог за считанные минуты.

Жители Эстонии ожидают от своего правительства дальнейших упрощений и расширения использования новейших ИТ-решений. За период с 2009 по 2016 год активная разработка и внедрение электронных служб позволили сократить количество посещений бюро налоговой и таможенной служб Эстонии более чем на 60%, что обеспечило существенное снижение их общих издержек.

В 2015 году Эстония улучшила свою налоговую декларацию о доходах и социальном обеспечении, что позволило ей собрать на 125 млн. евро больше налога на добавленную стоимость (НДС), чем в предыдущем году, и все это благодаря разработке и интенсивному использованию электронных служб. В частности, эстонское правительство добавило в декларацию налоговый калькулятор, который извлекал данные граждан страны из объединенной банковской системы. Это решение также упростило отправку счетов в систему.

В настоящее время эстонцы обратились и к блокчейн-технологии. Следующей большой разработкой будет создание облачной структуры, связанной с блокчейн-реестром. Эстония привлекла компании Ericsson, Arcera и Guardtime к совместной разработке и управлению гибридной облачной платформой, которая призвана обеспечить масштабируемость, устойчивость и защищенность данных по налоговой отчетности и онлайн-консультациям по вопросам здравоохранения.

Компания Nasdaq также занимается разработкой блокчейн-сервисов в Эстонии. Она создает рыночную площадку для частных компаний, которая обеспечит отслеживание движения акций, которые эти компании выпускают, и позволит им немедленно проводить транзакции. Она фокусируется на совершенствовании процесса голосования по доверенности для предприятий. Это будет способ зарегистрировать свой бизнес.

Проект компании Bitnation, осуществляемый в сотрудничестве с Эстонией, предполагает предоставление нотариальных услуг тем, кто получил в Эстонии статус электронного резидента. Этот сервис позволит электронным резидентам, независимо от того, где они живут или ведут свой бизнес, нотариально засвидетельствовать свои браки, свидетельства о рождении или бизнес-контракты, помещаемые в блокчейн-реестр. Нотариально заверенные в блокчейне документы пока не являются юридически обязательными в эстонской юрисдикции или в какой-либо иной стране или штате, но обеспечивают гражданам возможность доказать возраст этих документов.

Повышение качества нотариальных услуг в Китае

В Китае отношение к криптовалюте в разные времена было различным — от любви до ненависти. С одной стороны, граждане Китая часто предпринимали попытки использовать токены как средство отмывания денег и их вывода из страны либо как инструмент сокрытия доходов от налогообложения. Это вынуждало китайское правительство все более и более ужесточать правовые нормы в отношении использования криптовалют. Тем не менее, когда движущая сила криптовалют, блокчейн-технология, доказала свою полезность и помимо обеспечения перемещения ценности, отношение к ней в Китае заметно изменилось.

Интересным примером раннего ее использования была компания Ancun Zhengxin Co., пионер в переходе к электронным сервисам нотариализации данных в Китае через партнерство более чем со 100 традиционными нотариальными конторами в 28 провинциях страны. Она также предлагает электронные хранилища данных и блокчейн-решения по нотариализации через традиционные конторы.

Компания Ancun поместила тысячи записей в общедоступный для поиска блокчейн-реестр, разрешающий пользователям повторно обращаться к ним с целью проверки подлинности и возраста нотариально заверенных документов.



СОВЕТ

Многие стартапы работают над сходными концепциями и в Соединенных Штатах. Примером может быть компания Tierion (<http://www.tierion.com>), позволяющая хешировать данные и снабжать их отметкой времени, после чего ваша информация привязывается к блокчейну Биткойна.

Доверительный уровень для Интернета

За последние 30 лет в Интернете были созданы новые уровни — один уровень поверх другого, — каждый из которых позволял сделать работу в Интернете проще и безопаснее. Блокчейн-технология является очередным новым уровнем Интернета. Лучше всего представлять его себе как уровень доверия. Для широкой публики он, скорее всего, останется практически неосознанным и просто сделает интерактивные взаимодействия более приятными. Реализация блокчейн-технологии со временем позволит устранить раздражающие проблемы, которые часто возникают при работе в Сети и вызываются отсутствием достаточных способов убедиться в том, что полученной информации можно доверять.

Есть две ключевые области, в которых уже начаты работы, о которых вы можете не знать, но которые вам, безусловно, понравятся: электронная почта практически без спама и новый тип идентификации личности в интерактивном режиме.

Электронная почта без спама

Вы, наверное, ненавидите спам так же, как и я, но здесь имеет место и большая проблема, чем слишком много ненужных писем. Нынешние системы электронной почты больше не являются защищенными. В конце 2016 года сайт Yahoo! подвергся одной из крупнейших в мире хакерских атак. Был скомпрометирован один миллиард аккаунтов пользователей, а их личные данные выставлены напоказ.

Необходимость надежной защиты электронной почты вынуждает обратиться к блокчейн-технологии, поскольку почтовая служба находится почти на грани разрушения. И один из ведущих участников борьбы за интерактивную безопасность принял этот вызов. Компания McAfee, пионер в создании антивирусного ПО, разработала новую платформу для электронной почты, построенную на основе блокчейн-технологии.

Пакет John McAfee SwiftMail (<http://www.johnmcafeeswiftmail.com>) представляет собой почтовую систему, построенную на основе блокчейн-технологии. Внешне она мало чем отличается от почтовых систем, которыми вы пользовались прежде. Она очень проста в навигации, а некоторые разработчики уже создали мобильные и веб-приложения, чтобы сделать ее использование еще более удобным.

Блокчейн-реестр SwiftMail позволяет получить подтверждение, что ваша почта является подлинной и что отправленные вами электронные письма были

получены заинтересованными сторонами, что устраняет необходимость доверять ваши данные третьей стороне, например Yahoo!. Также в этой системе при отправке электронной почты взимается небольшая плата, что в значительной степени позволяет избавиться от спамеров.

В SwiftMail приняты строгие меры по защите личных данных, тогда как многие провайдеры почтового сервиса уже потеряли интерес к этой проблеме. Джон Мак-Афи говорит: “Если проблема защиты личных данных вас больше не интересует, почему бы вам не дать свой бумажник первому встречному, после чего позволить ему просмотреть его содержимое и записать все, что он найдет внутри? Нет? Тогда почему же мы верим, что если мы не будем делать что-то плохое, то нас не должно заботить, есть ли у кого-то наша информация?”

Система SwiftMail использует адрес кошелька, подобный адресам биткойн-кошельков, который хранится в приложении на вашем компьютере. Это 32 случайных символа без каких-либо метаданных, которые можно было бы использовать для взлома, а пользователь может быстро создать новый кошелек точно так, как в системе Биткойна. Почтовые отправления сами по себе представляют строку из 256 бит, причем полное шифрование делает перехваченные данные совершенно бесполезными для похитителей.



ЗАПОМНИ!

В настоящее время ПО SwiftMail можно загрузить только для платформ Android, Linux и Windows. Для устройств от Apple пока не существует соответствующей версии этого программного обеспечения. Учтите это, чтобы не загрузить на свои устройства не ту версию ПО.

В прочих проектах в этой области, включая проект “21” (<http://www.21.co>), сейчас работают над тем, чтобы присоединить к системе электронной почты выходной буфер на основе блокчейн-технологии. Уже созданы варианты почтового ПО, в которых за отправку вам почтового сообщения от адресата, который находится вне вашей сети, с него взимается определенная плата. А вам при этом предоставляется выбор — оставить эти деньги себе или пожертвовать их на благотворительность.

Владение собственным свидетельством идентичности

Одним из фундаментальных положений, о которых любят вести разговоры энтузиасты блокчейн-технологии, является личная ответственность за владение данными, которые вы создали и которые идентифицируют вас уникальным образом. Это положение может показаться несколько прямолинейным, но большинство людей не владеют или не контролируют те данные, которые представляют их личность.

В большинстве случаев контроль осуществляется централизованными базами данных, которые являются уязвимыми для хакерских атак. Эти базы данных

содержат некую информацию о вас, и органы сертификации подтверждают, что эта информация является правильной и не подвергалась изменениям. В информационную эру ваши данные являются свидетельством, подтверждающим вашу личность. Чем в большей степени эти данные будут распространены, тем выше вероятность того, что они попадут в руки тех, кто захочет ими воспользоваться для собственных злонамеренных целей.

Свидетельства личной идентичности, построенные на основе блокчейн-технологии, передают контроль над этими данными в руки тех людей или организаций, которых эти данные представляют. Централизованные базы данных и органы сертификации вовсе необязательно окажутся не у дел. Данным по-прежнему потребуется защищенное место хранения и по-прежнему будет смысл в существовании третьей стороны, подтверждающей аутентичность документов.

Основное значение изменения порядка ответственности относительно свидетельств личной идентичности состоит в том, что в результате становится сложнее похитить, использовать для шантажа или манипулировать теми документами, которые были положены в основу идентификации вашей личности. При необходимости любая информация будет представлена заинтересованным лицам, но без предоставления доступа к прочим конфиденциальным данным.

Источники информации и блокчейн-технология

Блокчейн-технология не отменяет проблему относительно того, что информация должна откуда-то поступать. Также очень важно, чтобы на эту информацию можно было положиться. Это тот самый человеческий фактор, который пока не удастся исключить из уравнения, даже когда вы ходите действовать по контракту, сохраненному в блокчейн-системе.

В блокчейн-системе не существует центральной власти для поддержания честности или принуждения к ней. Предсказать честное поведение авторов информации в будущем невозможно. Отсюда следует логическое заключение: каждая транзакция должна стоить меньше, чем восстановление репутации. Репутация доверенных авторов строится со временем, и чем дольше действия автора остаются честными и корректными, тем более ценной становится его репутация. Эта концепция сходна с ценностью имени бренда.

Из этого раздела вы также узнаете, как художники и другие творческие личности могут использовать блокчейн-технологию с целью монетизации своих работ.

Доверенное авторство

Смарт-контракты и встроенные в цепочки программы обеспечили новую возможность для знающих лиц и корпораций — монетизировать свою информацию. Этим элементам блокчейн-систем необходимы доверенные источники информации, на основании которой будут выполняться определенные действия. Такими доверенными источниками могут быть рейтинговые агентства, метеорологические центры и вообще почти что угодно.

Можно также включить в блокчейн-инфраструктуру устройства Интернета вещей (IoT) и заставить их выдавать собственные мнения и свидетельства в блокчейн-сеть. Им тоже потребуется заработать с течением времени необходимое доверие, но в любой момент они все же могут быть испорчены. Прежняя честность не предотвращает будущей нечестности или повреждения источника информации.

Не все смарт-контракты и встроенные в цепочки программы являются самодостаточными или работают от непогрешимых источников. Более практичным и приемлемым для использования в бизнесе вариантом будет требование, чтобы вся информация поступала из источников за пределами известной Вселенной любой заданной блокчейн-сети. Несколько стартапов бьются над этой проблемой, рассматривая ее с разных сторон.

В корпорации Factom был создан Acolyte — сервис, обеспечивающий пользователям возможность строить во времени репутацию той информации, которую они предоставляют в сеть. Создатели смарт-контрактов могут подписываться и вознаграждать используемые ими источники информации (оракулы). Кроме того, они могут присваивать им рейтинг в отношении того, насколько им можно доверять.

В стартапе Augur был выбран совершенно иной подход: они являются пионерами в использовании идеи рынка предсказаний. В Augur была разработана одноименная платформа, которая вознаграждает пользователей за правильное предсказание будущих событий реального мира, таких как результаты выборов или приобретение контрольного пакета акций корпорации. Ставки производятся посредством торговли виртуальными акциями в отношении результата предстоящих событий. Пользователи делают деньги, покупая акции правильного результата. Стоимость акций колеблется в зависимости от того, как сообщество воспринимает вероятность того, что событие действительно произойдет. В сущности, платформа Augur похожа на обычный сайт ставок. Любой может сделать предсказание. Кто угодно может создать рынок предсказаний для любого выбранного им события. А это позволяет, например, вам как владельцу бизнеса провести опрос о том, что именно, по мнению людей, наиболее вероятно для вашего бизнеса в будущем. Этот опрос может также вскрывать внутреннюю информацию, которую автор хотел бы иметь возможность превратить в капитал.

Права на интеллектуальную собственность

Одной из наиболее пострадавших отраслей, которые борются с правами на интеллектуальную собственность, является музыкальная индустрия. На артистов сверху оказывают экономическое давление множество посредников, которые зависят от их творческой работы. Начинающие и малоизвестные артисты не могут сделать музыку основным источником своих доходов, поскольку им достается лишь небольшая доля общего дохода. Только мегазвезды могут сделать это и только благодаря огромному количеству поклонников.

Интернет значительно расширил для артистов всех уровней возможность делиться своими творениями. В то же время он даже усложнил для рядовых исполнителей возможность достичь материального благополучия с помощью того, что им нравится делать. В музыкальной индустрии пищевая цепь достаточно длинна, и каждый посредник забирает себе некоторый кусок пирога и увеличивает время, необходимое для того, чтобы вознаграждение, наконец, дошло до артиста. Часто артист вынужден ждать до 18 месяцев и более, чтобы получить полагающиеся ему деньги, причем ему достается лишь 0,000035 доллара за выпущенный экземпляр его произведения. Описанная выше ситуация — наилучший сценарий при текущем состоянии рынка, и при этом никто как будто бы открыто не обманывает артиста.

Блокчейн-технология была предложена как возможное средство облегчения колоссального финансового бремени, которое несут на себе творческие личности. Например, можно использовать криптовалюту для сокращения стоимости транзакций, связанных с кредитными карточками и мошенничеством. Это решение также позволит открыть новые рынки в развивающихся странах, население которых не имеет нормального доступа к кредитным карточкам.

Однако еще более интересной, но менее очевидной, является возможность миграции всей экосистемы музыкальной индустрии в блокчейн-систему, которая будет использовать смарт-контракты или и встроенные в цепочки программы для проведения немедленной оплаты за каждое использование произведения. Такой подход также может сделать очевидным право собственности на лицензии и упростить для клиентов лицензирование музыкального произведения для коммерческого использования.

По этой проблеме уже запущено несколько проектов, имеющих целью содействие созданию здоровой, устойчивой и бесконфликтной экосистемы в мире музыки, — такой, которая не заменит существующий рынок, но будет способна предоставить артистам возможность получать немного больше от их тяжелой работы.

Проект UjoMusic, который сейчас находится в стадии бета-тестирования, — это платформа, предоставляющая пользователям возможность напрямую

продавать и лицензировать свои музыкальные произведения. В ней используются сеть Эфириума, смарт-контракты для выполнения операций и эфир (криптовалюта системы Эфириум) как средство платежа. Вы можете загрузить всю песню либо только вокальную или инструментальную ее линию для коммерческого или некоммерческого использования. Оплата исполнителю осуществляется немедленно и проводится в эфирах.

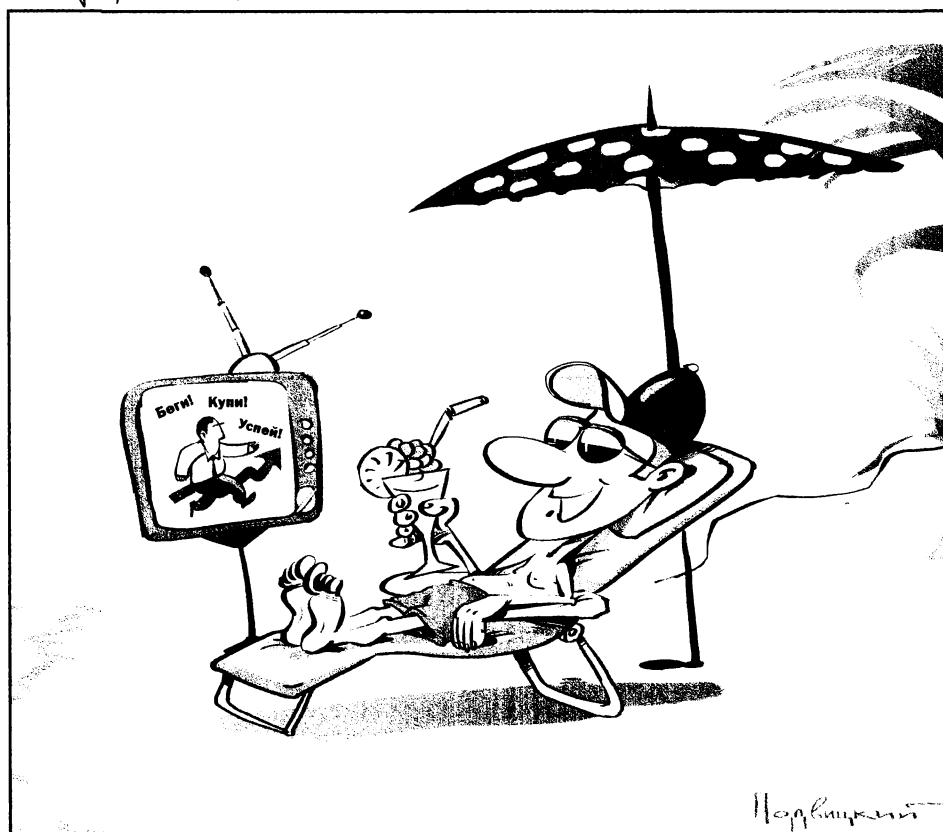
Компания Peertracks — это еще один блокчейн-стартап, который работает над изменением музыкальной индустрии. Здесь создан музыкальный потоковый веб-сайт, позволяющий его посетителям загружать произведения и знакомиться с новыми исполнителями. Осуществляется это с помощью одноранговой сети под названием “MUSE” и создания токенов для каждого отдельного артиста. Эти токены функционируют подобно другим криптовалютам и их ценность меняется в зависимости от популярности артиста.

Блокчейн-технология вовсе не устраняет необходимость музыкальных записей и их дистрибьюторов. Однако им придется действовать быстро, если они не хотят, чтобы их место заняли новые компании, успешно приспособившиеся к новой, более эффективной модели рынка, подобно тому как Netflix в свое время вытеснил Blockbuster.

Часть V

Великолепные десятки

© Подвицкий Виталий/cartonbank.ru



ДЕЛАЙ, КАК МЫ! ДЕЛАЙ, ЛУЧШЕ НАС!

В ЭТОЙ ЧАСТИ...

- » Познакомьтесь с десятью бесплатными блокчейн-ресурсами, которые помогут вам не отставать от бурно развивающейся технологии блокчейна и связанной с ней индустрии
- » Усвойте десять правил, которые никогда не следует нарушать, работая с криптовалютой или с приложениями из мира блокчейна
- » Узнайте больше о десяти ведущих блокчейн-проектах и организациях, которые сейчас определяют будущее этой индустрии



Глава 17

Десять бесплатных блокчейн-ресурсов

В ЭТОЙ ГЛАВЕ...

- » Познакомьтесь с бесплатными образовательными ресурсами по блокчейн-технологии
- » Включитесь в жизнь блокчейн-сообщества
- » Будьте в курсе последних новостей из мира блокчейна
- » Углубите свои знания с помощью прочих блокчейн-ресурсов

Из этой главы вы узнаете об интересных бесплатных ресурсах, имеющих в экосистеме блокчейн-технологии, которые помогут вам всегда быть в курсе последних событий и даже непосредственно принимать участие в жизни блокчейн-сообщества. Здесь вы узнаете, где можно найти бесплатные инструменты для создания *оракулов* (источников данных, на основании которых строится работа смарт-контрактов), видеоролики, которые помогут вам расширить свои знания, а также сведения о компаниях и организациях, которые формируют будущее блокчейн-индустрии.

Университет корпорации Factom

Корпорация Factom представляет собой блокчейн-компанию, которая развернула и обслуживает сеть Factom, проект с открытым кодом. Ее назначение — создание пользовательских блокчейн-приложений для больших корпораций и правительственных структур. В ней также был создан блокчейн-реестр, используемый в качестве сервисного продукта для ипотечной индустрии США.

Университет Factom (<http://www.factom.com/university>), созданный в корпорации, представляет собой постоянно растущую базу знаний, назначение которой — обучение всех желающих основам блокчейн-технологии, а также предоставление необходимой информации о платформе Factom и ее API. База данных включает видеоматериалы и учебные курсы, которые помогут всем желающим пройти путь от новичка до эксперта. Университет Factom планирует запустить сертификационную программу, поэтому заходите на этот сайт почаще!

Сайт Ethereum 101

Эфириум (Ethereum) — это краудфандинговый проект с открытым кодом, в рамках которого был построен блокчейн-реестр Эфириум. Это один из наиболее важных проектов в данной области, поскольку в нем впервые был реализован язык программирования, встроенный непосредственно в блокчейн. Благодаря этому встроенному языку программирования сеть Эфириума обеспечивает пользователям возможность создавать смарт-контракты и децентрализованные автономные организации (DAO) и развертывать децентрализованные приложения.

Сайт Ethereum 101 (<http://www.ethereum101.org>) представляет собой веб-сайт, созданный членами сообщества Эфириума. Это курируемое хранилище высококачественного обучающего контента по блокчейн-технологии и сети Эфириум. Общее управление этим сайтом возложено на Энтони Д'Онофрио, директора сообщества Эфириума.

Разработки в сети Ripple

Компания Ripple предоставляет решения по организации финансовых расчетных отношений в глобальном масштабе. Ее распределенная расчетная сеть создана на основе технологии с открытым кодом, использовать которую может любой желающий. Компания Ripple предупреждает, что возможности ее блокчейна могут использоваться только лицензированными финансовыми организациями.

В компании Ripple была разработана мощная база знаний по ее платформе (<http://www.ripple.com/build>). Материалы этой базы данных предназначены преимущественно для разработчиков. Компания Ripple также предлагает некоторые ресурсы для финансовых регулирующих органов. С этими материалами стоит ознакомиться, даже если вы не являетесь сотрудником этих органов, поскольку они дают углубленное представление о юридической неустойчивости и неопределенности, которые проявились с появлением блокчейн-технологии.

Программируемые деньги на основе Ripple

Стивен Зейлер, являющийся сотрудником компании Ripple, подготовил и разместил в YouTube серию роликов о том, как можно создать программируемые деньги в сети Ripple, используя язык JavaScript. Эта серия роликов предназначена преимущественно для JavaScript-программистов. На момент написания этих строк уже выпущено десять видеороликов, которые проведут вас по всем этапам разработки. Вы можете ознакомиться с этой серией роликов YouTube, перейдя по адресу <https://goo.gl/g8vFPL>.

Информация о проекте DigiByte

Проект DigiByte представляет собой децентрализованную платежную сеть, создание которой было вдохновлено появлением системы Биткойна. Она позволяет переводить денежные средства через Интернет и предлагает более быстрое выполнение транзакций при меньшей комиссии, чем в сети Биткойна. Эта сеть также открыта для тех, кто хочет майнить ее собственные токены.

Основатель системы DigiByte, Джаред Тейт, разместил в YouTube серию видеороликов, получившую название “DigiKnow”. Ее назначение — рассказать вам практически обо всем, что необходимо знать, чтобы успешно пользоваться системой DigiByte. Здесь я представляю ссылку на первый видеоролик серии, в котором излагаются основные принципы блокчейн-технологии и рассказывается, как работает сеть DigiByte и как в ней создается новая ценность: <https://youtu.be/scr6BzFddso>.

Университет блокчейн-технологии

Университет блокчейн-технологии — это образовательный веб-сайт, на котором размещены обучающие материалы по экосистеме блокчейна для разработчиков, менеджеров и предпринимателей. Здесь предлагаются открытые и закрытые программы обучения, дискуссионные материалы по хакерству и деморолики различных событий. Обучающие программы на этом сайте ориентированы на развитие общей направленности на поиск решения и практическое обучение на личном опыте. Физически университет блокчейн-технологии находится в городе Маунтайн-Вью, штат Калифорния, а его сайт доступен по адресу <http://blockchainu.co>.

Основы системы Биткойн

Сайт Bitcoin Core (<https://bitcoin.org>) первоначально был создан Сатоши Накомото специально для размещения на нем основополагающего документа (whitepaper) по Биткойн-протоколу. Теперь этот сайт используется для размещения обучающих материалов по ядру и протоколу системы Биткойн, а также различных версий оригинального программного обеспечения системы Биткойна, предназначенных для загрузки пользователями.

Основное назначение сайта — обеспечение децентрализованности системы Биткойна и ее доступности для среднестатистического пользователя.



ЗАПОМНИ

Этот проект поддерживается сообществом Биткойна и не все размещенные на нем материалы контролируются основной командой разработчиков системы. Не забывайте об этом, знакомясь с материалами этого сайта.

Блокчейн-альянс

Блокчейн-альянс был основан Блокчейн-палатой цифровой коммерции (Blockchain Chamber of Digital Commerce) и новостной организацией Coincenter. Это государственно-частное объединение, построенное на сотрудничестве блокчейн-сообщества, правоохранительных и регулирующих органов. Их общая цель — сделать экосистему блокчейна более защищенной и способствовать дальнейшим разработкам по развитию этой технологии. Осуществляется это посредством борьбы с криминальной активностью в экосистеме блокчейна за счет предоставления образовательной и технической помощи, а также

периодического проведения информационных сессий по системе Биткойна, прочим цифровым валютам и другим решениям, использующим блокчейн-технологию.

Узнать больше о мероприятиях этой организации или присоединиться к ней вы сможете, зайдя на сайт <http://www.blockchainalliance.org>.

Блог Multichain

Компания Multichain оказывает помощь организациям в быстрой разработке приложений на основе блокчейн-технологии. Она предлагает платформу, которая может пустить в обращение миллионы активов в пределах закрытого блокчейна, предоставив вам возможность отслеживать и контролировать активность в своей сети, пользуясь инструментами этой компании. Эта компания считается не только успешной в создании набора инструментов и платформы, но и признанным лидером в экосистеме блокчейна.

Вот самые лучшие, на мой взгляд, посты, которые можно найти в их блоге, доступном по адресу <http://www.multichain.com/blog>.

- » Четыре реальных случая использования блокчейн-технологии (<http://www.multichain.com/blog/2016/05/four-genuine-blockchain-use-cases/>)
- » Остерегайтесь невозможного смарт-контракта (<http://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/>)
- » Фиаско концепций смарт-контрактов и DAO (<http://www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/>)
- » Представление о блокчейнах с нулевым знанием (<http://www.multichain.com/blog/2016/11/understanding-zero-knowledge-blockchains/>)

Платформа HiveMind

Пол Шторц — основатель площадки Truthcoin, пиринговой системы оракулов и площадки предсказаний для системы Биткойна. Он создал боковую блокчейн-цепь в системе Биткойна с алгоритмом консенсуса типа “proof-of-work”, в которой сохраняются данные о состоянии рынков прогнозирования. Благодаря этому Биткойн получил возможность поддерживать финансовые

деривативы и смарт-контракты через платформу HiveMind, разработанную в соответствии с основополагающим документом проекта Truthcoin. Чтобы узнать больше, обратитесь к ресурсам и обучающим материалам на сайте <http://bitcoinhivemind.com>.



Глава 18

Десять правил, которые никогда не следует нарушать в мире блокчейна

В ЭТОЙ ГЛАВЕ...

- » Узнайте больше о своей правовой уязвимости
- » Получите представление о технических недостатках блокчейн-систем
- » Выявите в своей системе точки, наиболее уязвимые для внешних атак
- » Разработайте наилучшие рекомендации по безопасности своей системы

В этой главе разговор пойдет о том, что обязательно следует принимать во внимание, пользуясь приложениями на основе блокчейн-технологии и работая с криптовалютами, которые обеспечивают их функционирование.



ЗАПОМНИ!

Обязательно проконсультируйтесь со своими сертифицированными бухгалтером и адвокатом, прежде чем принимать финансовые решения. Технология блокчейн является достаточно новой, и правила, которыми она регулируется, разработаны еще не полностью.

Не используйте криптовалюты или блокчейн-приложения, чтобы обойти требования закона

Легальность и правовое зонирование криптовалют все еще не являются устоявшимися и подвержены колебаниям во многих уголках мира. Я вовсе не шутила, когда советовала вам обсуждать свои действия с вашими бухгалтером и адвокатом. Это позволит вам с пользой потратить свои деньги и избежать возможных неприятностей.

Вот несколько простых вопросов, которые мне задают очень часто.

- » **Могу ли я использовать криптовалюту как средство сокрытия денег?** Эта идея очень опасна. **Запомните:** в блокчейн-реестре записи обо всех транзакциях хранятся вечно, поэтому, даже если вы полагаете, что найдете какой-то хитрый способ спрятать от всех несколько токенов, у тех, кто следит за проявлениями плохого поведения, будет достаточно времени, чтобы их найти.
- » **Могу я использовать блокчейны как средство скрытно вывести деньги из своей страны?** Во многих странах существуют ограничения на суммы, которые ее граждане могут вывезти из страны. Вам не стоит этого делать по той же самой причине, которую я указала выше: в блокчейн-реестре записи обо всех транзакциях хранятся вечно.
- » **Могу я использовать криптовалюту для приобретения запрещенных товаров?** Ответ, как вы, наверное, уже догадались, — нет! В блокчейн-реестре свидетельства о ваших незаконных действиях останутся *навсегда!*



ЗАПОМНИ!

Не делайте с помощью криптовалют или блокчейн-приложений ничего такого, что было бы незаконно делать с обычными деньгами.

Делайте свои контракты настолько простыми, насколько это возможно

Децентрализованные автономные организации (DAO), смарт-контракты и чейн-коды — все это весьма популярно на текущий момент. Обещание сокращения административных и юридических расходов является очень заманчивым аргументом для многих корпораций. Однако важной характеристикой этой технологии, упускаемой иногда из виду, является то, что это всего лишь программный код. А это означает, что здесь нет человека, который будет интерпретировать те правила, которые вы взвалили на всех с требованием следовать им. Программный код становится законом, но этот закон охватывает лишь то, что явно включено в контракт, сохраненный в блокчейне. Иногда тот “жир”, который был удален, может оказаться очень важным.

Никто не будет интерпретировать смысл программного кода. А это означает, что, если этот программный код будет выполнен так, как вы не ожидали или не предполагали, некому будет позаботиться о соблюдении той цели, ради которой создавался контракт. И поскольку программный код здесь — это закон, с этой точки зрения ничего противозаконного в данном случае не произошло и вообще произойти не может. Вот почему вам всегда следует делать свои контракты простыми и модульными, чтобы можно было четко контролировать и точно предсказывать любые возможные результаты его выполнения. Также хорошей идеей будет тщательное тестирование работы контракта, лучше с привлечением сторонних разработчиков, которых следует дополнительно протестировать для поиска любых способов его взлома.

Достигаемость блокчейн-реестра, в котором вы создаете свой проект, также имеет значение. Можете представлять его себе как некую юрисдикцию. Убедитесь, что смарт-контракт сможет выполняться на основании поступающих внешних данных, но при этом он не должен запрашивать суммы со счетов, к которым у них нет доступа. Это означает, что все активы должны быть некоторым образом задержаны на некоторое время, что может усложнить движение потоков наличности.

Еще один важный вопрос, который стоит тщательно обдумать, — это выбор источника информации, который ваш контракт будет использовать в процессе выполнения. Если это данные о погоде, необходимые для выполнения страхового контракта, то подумайте, можете ли вы доверять этому источнику и положиться на него? Возможна ли манипуляция исходными данными, необходимыми для вашего контракта? Следует все хорошо продумать, прежде чем приступить к реализации оракула для контракта.

Публикуйте данные с осторожностью

Основным свойством любого блокчейн-реестра является тот факт, что если данные были в него помещены, то извлечь их из него будет чрезвычайно сложно. А это означает, что все записанное в него будет доступно там очень долгое время. Если вы опубликуете здесь зашифрованную конфиденциальную информацию, можете не сомневаться в том, что рано или поздно она вполне сможет оказаться расшифрованной, и все, что вы опубликовали, окажется доступным для прочтения кому угодно.



СОВЕТ

Подумайте о следующем, прежде чем публиковать информацию в блокчейн-реестре.

- » Насколько для меня важно, чтобы эта информация в какой-то момент не оказалась расшифрованной?
- » Могу ли я поделиться этой информацией со всей Вселенной, с каждым, кто захочет с ней ознакомиться?
- » Является ли эта информация опасной для третьей стороны или является ли она тем, за публикацию чего меня могут привлечь к ответственности?

В криптографии ведутся исследования по разработке методов шифрования с квантовыми доказательствами, но поскольку квантовые вычисления, как и квантовое шифрование, все еще находятся на фазе тестирования, очень сложно сказать, на что будут способны технологии, скажем, через 20 лет.

Сохраняйте, делайте резервные копии и тщательно оберегайте свои закрытые ключи



ЗАПОМНИ

Блокчейн — это структура, которая ничего не прощает. Ее совершенно не волнует тот факт, что вы забыли свой закрытый ключ или пароль. Множество криптоглупцов осталось ни с чем и утопило в великом блокчейн-океане свои бесчисленные токены — сокровище, которое никто никогда не найдет.

Закрытые ключи, которые контролируют доступ к вашей криптовалюте, часто “живут” в ваших крипто-кошельках, поэтому очень важно тщательно их защищать и охранять. Будьте очень аккуратны в обращении с интерактивными

сервисами, которые хранят ваши деньги для вас. Многие криптовалютные биржи и сайты интерактивных кошельков неоднократно подвергались ограблениям.



СОВЕТ

Храните на сайтах любых интерактивных служб или на доступных из Интернета устройствах лишь небольшое количество своих токенов, предназначенных лишь для повседневного использования. Относитесь к своему криптовалютному кошельку, как к обычному кошельку для наличных денег. Не храните в нем слишком много денег, поскольку в любой момент его можно потерять. Многие сотни известных вредоносных приложений ищут возможности заполучить ваши закрытые ключи и украсть ваши токены.

Держите большую часть своей криптовалюты в *холодных хранилищах*, т.е. в таких хранилищах, которые полностью отключены от Интернета. Это может быть бумажный кошелек либо компьютер, который не подключен к Сети, либо специальное устройство (так называемый *аппаратный кошелек*), специально разработанное для безопасного хранения криптовалюты, которое подключается к Интернету только для проведения необходимых транзакций, а затем вновь отключается от него.

Если вы предпочтете хранить токены в бумажных кошельках, обязательно заламинируйте их и сделайте копии. Также не забывайте, что принтеры часто имеют доступ к Интернету и поступающие на них данные могут быть получены третьими лицами. Настоящие параноики пользуются только такими принтерами, которые не имеют доступа к Сети. Храните копии своих бумажных кошельков в различных местах, таких как банковская ячейка или безопасное место у вас дома.



ЗАПОМНИ

Делайте резервные копии своих цифровых кошельков и храните их в безопасных местах. Эти копии пригодятся вам, если откажет компьютер или вы по ошибке удалите нужный файл. Резервная копия позволит восстановить кошелек и в том случае, если ваше мобильное устройство было повреждено или украдено. Кроме того, не забудьте зашифровать свой кошелек. Шифрование кошелька позволит установить пароль, который потребуется ввести, прежде чем можно будет получить доступ к вашим токенам.



ВНИМАНИЕ!

Шифрование — полезное средство для защиты от воров, но оно не способно защитить от программ, перехватывающих те данные, которые вводятся с клавиатуры. Всегда используйте надежный пароль, который должен включать буквы, цифры, знаки пунктуации и иметь длину не менее 16 символов. Наиболее надежные пароли генерируются

особыми программами, разработанными специально для этой цели. Однако надежные пароли труднее запомнить. Подумайте о том, чтобы записать их на бумаге, а затем заламинировать ее, как в случае закрытых ключей. Учтите, что при работе с криптовалютами возможности восстановления забытых паролей весьма ограничены, а значит, забыть свой пароль означает просто навсегда утратить свои токены.

ИНСТРУМЕНТ БЕЗОПАСНОГО ХРАНЕНИЯ ТОКЕНОВ

Для защиты своих биткойнов можете воспользоваться кошельком BitGo. Хотя это интерактивная служба электронных кошельков, для перемещения токенов на сайте BitGo от вас потребуют указать как онлайн-, так и оффлайн-подписи. Благодаря такому подходу этот инструмент более защищен, чем стандартные интерактивные кошельки.

Кошелек на сайте BitGo имеет три ключа. Один хранится непосредственно на этом сайте, второй хранится у вас, а сохранение третьего осуществляется от вашего имени третьей стороной — службой восстановления ключей. При проведении любой транзакции необходимы две подписи, которые обычно предоставляются системой BitGo и вами. Если же вы потеряли один из своих ключей, то в этом случае вам на помощь придет служба восстановления ключей. Однако кошелек на сайте BitGo не является бесплатным — за каждую транзакцию здесь берут небольшую плату.

Подробнее о кошельках BitGo можно узнать по адресу <https://www.bitgo.com/wallet>.

Трижды проверяйте все адреса, прежде чем отправлять на них валюту

Криптовалюта привлекает пристальное внимание немалого числа негодяев, поэтому будьте осторожны, отправляя свои деньги кому-либо. Как только деньги покинут ваш кошелек, они уйдут навсегда, и не существует никаких способов их возврата. Здесь нет никаких возвратных платежей, и у вас не будет возможности обратиться в службу поддержки клиентов. Как только транзакция будет проведена, деньги уйдут навсегда.

Трижды проверяйте набранный вами адрес кошелька получателя, прежде чем подтвердить операцию отправки. Вы должны полностью удостовериться, что отправляете свои деньги на правильный адрес.

Пользуйтесь биржами с осторожностью

Криптовалютные биржи являются главными объектами, на которые хакеры направляют свои усилия с целью кражи токенов. Они выглядят, как горшки с золотом, которые так и просятся, чтобы их утащили, и более 150 из них уже подверглись успешным атакам.

Не забывайте об этом, пользуясь услугами бирж, и всегда следуйте наилучшим рекомендациям в отношении того, как следует безопасно хранить свои токены, которые были даны в этой книге. Проведите небольшое исследование в отношении той биржи, услугами которой вы пользуетесь, просто чтобы убедиться, что на ней приняты все необходимые меры по обеспечению безопасности.

И наконец, пользуйтесь биржами исключительно для того, чтобы вводить и выводить средства. Не используйте их как место *хранения* своих токенов. Гораздо надежнее хранить крупные суммы криптовалют в холодных хранилищах или в ламинированных бумажных кошельках с несколькими копиями.

Относитесь к сетям Wi-Fi с осторожностью

Если роутер вашей сети Wi-Fi будет настроен неправильно, вполне возможно, что кто-то получит полный журнал всей вашей сетевой активности. Если вы работаете в открытой сети Wi-Fi, вполне обоснованно будет предположить, что ее владелец сможет получить информацию о вашей активности.



ВНИМАНИЕ!

Используйте только те сети Wi-Fi, которым вы доверяете, и убедитесь, что вы изменили исходный пароль вашего собственного роутера на что-то, что в качестве пароля будет обеспечивать более надежную защиту. В большинстве случаев исходный пароль Wi-Fi роутеров устанавливается на предприятии их производителя и имеет стандартное значение, например “admin”, а значит, эта защита легко может быть преодолена третьей стороной.

Тщательно выбирайте блокчейн-разработчиков

Блокчейн-технология является достаточно новой, и следовательно, не так много людей имеют значительный опыт работы в ней, когда дело доходит до создания блокчейн-приложений.

Если вы задумываетесь над тем, чтобы нанять разработчика, который поможет вам в создании собственного блокчейн-проекта, прежде всего, проверьте сведения о возможных претендентах на сайте GitHub, уточните, какой конкретно работой они занимались, и лишь затем принимайте решение. Этот человек не обязательно должен иметь опыт работы именно в области блокчейн-технологии, но если он его не имеет, это должен быть достаточно опытный разработчик приложений, пусть и вне мира блокчейна.

Имеется не так много внешних ресурсов, на которых разработчик мог бы найти необходимую помощь, оказавшись в тупике. Неопытные разработчики могут потратить гораздо больше времени на преодоление возникших затруднений, а значит, время создания вашего приложения может существенно увеличиться.

Не дайте обвести себя вокруг пальца

Вся блокчейн-индустрия не имеет такого уровня защиты и безопасности, каким обладают банки и другие финансовые институты, и также здесь нет законов, направленных на вашу защиту и защиту вашего финансового благополучия. Здесь нет положений о защите клиента и нет Федеральной корпорации по страхованию вкладов, финансируемой правительством. Если вас ограбили или надули, у вас нет возможности обратиться к кому-либо за помощью.

Кроме того, вокруг этой индустрии в последние годы было слишком много рекламной шумихи без достаточного освещения ее реальной ценности. В 2016 году на свет явилось более тысячи новых блокчейн-компаний, все еще требующих необходимой экспертизы. Если вы подыскиваете подходящий проект, находящийся в стадии разработки, и пытаетесь решить, стоит ли он ваших инвестиций, в любом случае хорошей идеей будет не пожалеть времени и обязательно убедиться, что это вообще имеет смысл. Дайте себе ответы на следующие вопросы.

- » Будет ли в этом проекте генерироваться реальная ценность?
- » Будет ли ценность создаваться способом, который принесет вам пользу?
- » Существуют ли другие, более проверенные, технологии, которые можно было бы использовать для достижения тех же результатов и с той же самой эффективностью или даже с лучшей?

Блокчейн-технология, безусловно, является мощной и многообещающей, но при всех ее достоинствах подходить к ней следует с должным вниманием и осторожностью.

Не занимайтесь торговлей токенами, если вы не вполне понимаете, как это делается

Курсы криптовалют очень изменчивы и способны колебаться в значительной степени в любой момент времени и без всякой видимой причины. Многие криптовалюты имеют очень небольшую глубину, и их продажа в больших количествах может привести к краху их рыночной стоимости. Кроме того, работа с открытыми блокчейнами означает, что вам, вероятно, понадобится владеть некоторой суммой соответствующей криптовалюты, чтобы просто иметь возможность их использовать.

Не бросайтесь с головой в торговлю токенами, пока не пройдет достаточно времени, чтобы вы смогли хорошо понять поведение этого рынка. Если вы все-таки решитесь на торговлю криптовалютами, не забывайте сообщать о предпринятых вами действиях своему бухгалтеру. Ему может потребоваться сообщать о ваших выигрышах или потерях при определении размеров налога на прибыль.



Глава 19

Десять самых интересных блокчейн-проектов

В ЭТОЙ ГЛАВЕ...

- » Знакомимся с новыми блокчейн-инициативами
- » Обсуждаем реализованные блокчейн-проекты глобального масштаба

Новые блокчейн-стартапы возникают каждый день. Предприниматели уже увидели возможности извлечь выгоду из мощных блокчейн-инструментов, обещающих быстрее пересылать деньги, обеспечивать защиту компьютерных систем и создавать цифровые свидетельства идентичности.

В этой главе речь пойдет о некоторых самых интересных блокчейн-проектах и компаниях. Прочитав эту главу, вы получите представление о том, какие удивительные вещи могут происходить в области создания программного обеспечения на блокчейн-платформе. У вас даже могут появиться некоторые идеи о том, чем вы сами сможете заняться!

Консорциум R3

Многие банки инвестировали определенные средства в создание прототипов блокчейн-приложений: одни — для проверки возможности удовлетворения требований положения “Знай своего клиента”, направленного на предотвращение возможности отмывания денег, другие — для снижения стоимости пересылки денег за границу. Им пришлось преодолеть несколько серьезных проблем, связанных с защитой личной информации и отношением закона к криптовалютам как к вещи полулегальной, попадающей в “серую зону”.

Проект R3 (<http://www.r3cev.com>) представляет собой инновационную компанию, которая создала консорциум более чем с 75 ведущими финансовыми институтами всего мира с целью интеграции и получения преимуществ от использования новой блокчейн-технологии. Целью проекта R3 является улучшение процедуры обмена валюты через границы, снижение расходов на аудит и повышение скорости межбанковских переводов средств и оплат.

Три “столпа” проекта R3 можно сформулировать следующим образом.

- » **Блокчейн-система для финансового мира.** Компания R3 разработала технологию базового уровня, предназначенную для поддержки нужд глобальных финансовых институтов.
- » **Исследования и разработка.** Компания R3 создала двухсторонний исследовательский центр, предназначенный для выработки и тестирования индустриальных стандартов для блокчейн-технологии в коммерческой сфере.
- » **Создание программных продуктов.** Компания R3 в тесном сотрудничестве с различными организациями работает над созданием программных продуктов, предназначенных для решения проблем по всей цепи создания стоимости.

Компания R3 разработала блокчейн-платформу для финансовых учреждений, которая получила название “Corda”. Платформа Corda представляет собой распределенный реестр, предназначенный для управления и синхронизации выполнения финансовых соглашений между регулируемыми финансовыми учреждениями. В отличие от большинства прочих блокчейн-реестров, рассылающих свои транзакции по всей сети, в Corda транзакции могут выполняться параллельно, на различных узлах и без соблюдения требования, чтобы каждый узел сети знал о транзакциях, осуществляемых на других узлах. История сети строится на основе требования “need-to-know”, т.е. “необходимо знать”.

Основные функциональные особенности платформы Corda включают следующее.

- » **Контролируемый доступ.** Только стороны, имеющие на это право, могут видеть те или иные данные.
- » **Отсутствие центрального контроллера.**
- » **Регулирующие и контролирующие/наблюдающие узлы.**
- » **Подтверждение сделки сторонами вместо широкого пула несвязанных подтверждающих узлов.**
- » **Поддержка большого разнообразия механизмов консенсуса.**
- » **Отсутствие собственной криптовалюты.**

Платформа T ZERO: расширение фондового рынка

Проект T ZERO представляет собой платформу, на которой блокчейн-технология интегрируется с уже существующими рыночными процедурами с целью сокращения времени проведения платежей и их стоимости, а также повышения их прозрачности, эффективности и документированности. Платформа T ZERO позволяет достичь этого благодаря ее модульной структуре и широкой адаптируемости.

Компания T ZERO является дочерним предприятием компании Overstock.com и фокусируется на разработке и коммерциализации финансовых технологий, построенных на базе криптографически защищенных децентрализованных реестров. С момента своего создания в октябре 2014 года компания T ZERO (<http://www.t0.com>) уже создала получившие признание работающие коммерческие блокчейн-продукты.

В партнерстве с корпорацией Keystone Capital, независимой брокерско-дилерской организацией, находящейся в Калифорнии, был проведен первый публичный выпуск блокчейн-акций. Эти компании совместно предоставляют брокерские услуги тем клиентам, которые торгуют блокчейн-акциями.

Патрик Бирн, основатель и исполнительный директор компании Overstock, возглавил эту инициативу. Непрозрачные бизнес-практики Уолл-стрита открыли для себя рыночные возможности этой прозрачной и заслуживающей доверия торговой платформы, на которой клиенты знают, что они покупают и по какой цене. Комиссия по ценным бумагам и биржам США объявила компанию S-3, родительскую для компании Overstock.com, заслуживающей доверия, что и позволило последней выпустить в оборот свои блокчейн-акции. По вопросу тестирования этой платформы было заключено соглашение о сотрудничестве с Коммерческим банком Китая, крупнейшим в мире банком.

Бирн достиг этого благодаря Medici, мажоритарной дочерней компании Overstock.com по финансовым технологиям. Компания Medici фокусируется на применении блокчейн-технологии к решению важнейших проблем финансовых транзакций. Ее первой инициативой было решение сделать прозрачными расчеты по ценным бумагам.

Распределенные системы компании Blockstream

Компания Blockstream (<http://www.blockstream.com>) имеет превосходную репутацию в отношении поддержки блокчейн-технологии, и ее основное направление — создание распределенных систем. Компания Blockstream предлагает специализированное оборудование и программные решения для организаций, использующих сети, работающие на базе блокчейн-технологии.

Основной программной платформой компании является Blockstream Elements, сегмент проекта с открытым кодом. Для блокчейн-разработчиков она предлагает несколько ресурсов и высокопроизводительный протокол.

В компании Blockstream главным полем для инноваций являются боковые цепочки (sidechain), которые позволяют масштабировать эффективность использования уже существующих блокчейнов, расширить их функциональные возможности и уровень приватности посредством добавления таких функций, как смарт-контракты и конфиденциальные транзакции. Боковые цепочки позволяют не принимать во внимание нехватку ликвидности, которая так характерна для многих криптовалют. Кроме того, боковые цепочки позволяют организовать передачу цифровых активов между различными блокчейн-реестрами.

Боковые цепочки делают возможным для практических торгующих компаний совместное использование блокчейн-реестра, не беспокоясь о цене транзакции или низкой скорости работы сети. Инфраструктура распределенного управления активами может также использовать сеть системы Биткойна, разрешая отдельным лицам и организациям выпускать разные классы активов.

Компания Blockstream также работает над созданием сети Lightning Network, представляющей собой такую надстройку, которая позволит системе Биткойна поддерживать микроплатежи без замедления работы всей его сети. Сеть Lightning Network будет поддерживать большой объем мелких платежей с использованием пропорциональных сборов за проведение транзакции и работать при этом очень быстро. Сейчас работа ведется в основном в направлениях развертывания прототипов сети Bitcoin Lightning, создания процедуры консенсуса и обеспечения совместимости.

Блокчейн проекта OpenBazaar

Проект OpenBazaar (<http://www.openbazaar.org>) представляет собой проект с открытым кодом, в пределах которого создается децентрализованная сеть, предназначенная для ведения пиринговой цифровой коммерции. Вместо традиционной модели, в которой покупатели и продавцы взаимодействуют друг с другом через централизованные сервисы, такие как Amazon или eBay, платформа OpenBazaar соединяет их напрямую. В этом проекте для снятия комиссионных сборов и реализации ограничений будет использоваться криптовалюта системы Биткойна.

Чтобы работать на платформе, вам необходимо загрузить и установить на своем компьютере программу OpenBazaar. Она обеспечит вам соединение с другими людьми, желающими купить или продать товары или услуги. Это пиринговая сеть, которая не контролируется никакой компанией или организацией. После загрузки и установки приложения вам останется лишь позиционировать себя как покупателя или продавца, что не составит большой сложности. Когда будете готовы приобрести что-нибудь, просто проведите соответствующий поиск и посмотрите, что вам предложат. В некотором роде это очень похоже на анархистскую версию сайта eBay.

Проект OpenBazaar в определенной степени напоминает печально известный сайт Silk Road, но не является его подобием. В отличие от Silk Road, его пользователи не являются анонимными. Их легко можно отыскать по их IP-адресам, что делает эту платформу мало привлекательной для криминальных элементов. Вы можете извлечь информацию о местонахождении продавца из API проекта OpenBazaar и отобразить расположение всех участников в сети. Существует несколько способов скрыть свое местоположение, и изучаются возможности более конфиденциального обмена сообщениями, но на текущий момент в сети практически нет незаконной торговли.

Проект OpenBazaar сейчас работает над повышением своей привлекательности для большинства коммерческих организаций и независимых розничных торговцев. Тот, кто хочет сэкономить деньги, умеет обращаться с биткойнами и знает, как в этой системе следует проводить транзакции, может получить значительное конкурентное преимущество перед своими конкурентами.

Ищем себе кодировщика: компания Code Valley

Компания Code Valley (<http://www.codevalley.com>) взяла традиционную модель разработки программного кода и перевернула ее с ног на голову. Сама себя она позиционирует под лозунгом “Мировой компилятор”. Компания Code Valley предоставляет своих разработчиков для создания программного обеспечения в сотрудничестве с другими разработчиками посредством использования механизма, который в Code Valley называют “агенты”.

Каждый “агент” в этой системе возвращает фрагмент кода для проекта заказчика. В компании Code Valley также работают над открытием торговой площадки для предпринимателей.

Обратившись в компанию Code Valley, клиент получает доступ к глобальной сети разработчиков, которые хотят и могут создать для него программное обеспечение. Компания Code Valley работает подобно интерактивному веб-сайту программистов-фрилансеров, например Upwork. В этой системе разработчики стремятся получить от клиентов предложения по созданию программного обеспечения. Клиенты же, со своей стороны, должны тщательно отбирать среди них тех, кто действительно сможет эффективно работать над их проектами.

Работа компании Code Valley также немного напоминает поведение объекта доступа к данным (Data Access Object — DAO) — в том, что когда создается новый проект, он запускает процесс образования скрытого, похожего на пчелиный улей компилятора программ. Приложение клиента строится совместными усилиями большого числа различных агентов. Компания Code Valley является индустриализированным создателем программного обеспечения, в том числе построенного на базе блокчейн-технологии.

Цифровые активы компании Bitfury

Компания Bitfury Group (<http://www.bitfury.com>) начала свое существование в качестве майнера криптовалюты системы Биткойна, но со временем трансформировалась в компанию, предоставляющую полный комплекс услуг в сфере блокчейн-технологии. Она создает программное обеспечение и разрабатывает аппаратные решения для бизнеса и правительственных организаций, предназначенные для перемещения активов между блокчейн-системами.

Эта компания занимается исключительно улучшением и развитием экосистемы блокчейна системы Биткойна. Ее технологии повышают эффективность управления цифровыми активами. Также ее предложения позволяют повысить

защищенность открытых и закрытых блокчейн-транзакций с использованием аппаратных и программных решений.

Компания Bitfury обрабатывает закрытые и открытые блокчейн-транзакции. Она также помогает клиентам в отношении блокчейн-аналитики. В частности, компания Bitfury использует неизменяемую и всегда доступную для просмотра любому желающему историю транзакций в блокчейне Биткойна для проведения расширенной аналитической обработки данных по истории транзакций. Правительственные структуры используют исследования подобного типа для отслеживания криминальной активности в блокчейн-реестре системы Биткойна.

Компания Bitfury также принимает участие в разработке сети, получившей название “Lightning Network”. Эта сеть будет наложена на сеть блокчейна Биткойна, что позволит эффективно выполнять в этой системе микротранзакции.

Компания Bitfury также ведет работы по созданию регистра прав собственности. Республика Грузия в партнерстве с Bitfury создает Государственный регистр титулов земельной собственности. Все сведения о владении записываются в блокчейн-реестр с целью обеспечить хранение истории этих данных в неизменяемом виде. В развивающемся мире безопасная передача имущества будет экономически выгодна.

На ShapeShift есть любые монеты

Сайт ShapeShift (<http://www.shapeshift.io>) — это одно из самых быстрых средств обмена блокчейн-активов и криптовалют. С помощью этого сервиса пользователи могут продать цифровую валюту за считанные секунды. И при этом у них нет причин беспокоиться в отношении безопасности — здесь не требуются логины. Благодаря своим системам сайт ShapeShift существенно снижает риск похищения токенов.

Сайт ShapeShift следует жесткой политике “нет фиата”. В финансовых кругах термин *фиат* не имеет отношения к маленьким изящным итальянским автомобилям; словом “фиатный” здесь означают валюты, выпускаемые правительствами разных стран. На сайте ShapeShift посетителям не разрешается покупать криптовалюту на средства с банковских счетов или с помощью кредитных карточек. Сервисами сайта ShapeShift можно пользоваться в любом уголке мира, за исключением Северной Кореи и штата Нью-Йорк.

Использовать сервисы сайта ShapeShift очень просто. Вы заходите на сайт, определяете тип валюты, которую собираетесь обменять, и указываете тот кошелек, на котором находятся обмениваемые токены. Сайт ShapeShift обменяет токены для вас, получит их на некоторый счет, а затем отправит их в указанный вами пункт назначения.

Обменный курс, используемый на сайте ShapeShift, определяют несколько рыночных источников, и он всегда остается неизменным и независимым от кратковременных колебаний ценности обмениваемой валюты. Также есть возможность конвертировать биткойны и другую криптовалюту непосредственно на сайте ShapeShift.

Сайт ShapeShift предлагает много уникальных функций и инструментов, подобных Shifty Button и ShapeShift Lens, которые предоставляют посетителю возможность покупать предметы за любую альтернативную криптовалюту и получать и обменивать платежи в альткойнах напрямую и быстро.

Приложения машинных платежей от компании 21

Компания 21, Inc. (<http://www.21.co>) является одной из наиболее хорошо профинансированных блокчейн-компаний во всей экосистеме блокчейна с привлечением более 116 млн. долларов. Среди тех, кто вложил средства в компанию 21, можно указать такие фирмы венчурного капитала, как Andreessen Horowitz, Data Collective, Khosla Ventures, RRE Ventures и Yuan Capital.

Компания 21 создает программное и аппаратное обеспечение, которое упрощает работу с системой Биткойна по HTTP. Это позволяет осуществлять быстрые платежи по схеме “машина–машина”. Клиенты получают возможность отправлять, получать и выполнять микроплатежи по протоколу HTTP. Компания 21 также позволяет клиентам писать собственные приложения для осуществления машинных платежей в их системе.

Одним из устройств, созданных в компании 21, является встраиваемый чип для майнинга, получивший название “BitShare”. Он может быть встроен в устройство подключения к Интернету как независимый чип или интегрирован в существующий чипсет как блок IP. Компания BitShare генерирует в сети потоковый канал для цифровой валюты, предназначенный для использования в широком диапазоне приложений.

Помимо этого, компания 21 работает еще в четырех направлениях.

- » Создание загружаемых приложений, которые позволяют быстро получать биткойны в любой стране без использования банковского счета или кредитной карточки.
- » Развертывание торговой площадки, на которой можно покупать или продавать разработчикам со всего мира API обращения к системе Биткойна, а также добавлять функцию микроплатежей в биткойнах с помощью одной строки кода.

- » Разработка аналитической панели, с помощью которой можно будет вести мониторинг своих заработков в системе Биткойна, а также контролировать сетевую активность.
- » Реализация системы, которая позволяет устанавливать соединения с разработчиками и размещать свои API проведения машинных платежей.

Анонимные транзакции в системе Dash

Блокчейн-система Dash (<http://www.dash.org>) — это первая криптовалюта, выпущенная после биткойна. Создатели системы Dash поставили перед собой цель сделать транзакции в ней более конфиденциальными. (В сети Биткойна любой желающий может просмотреть историю ваших транзакций.) В результате созданная ими система Dash позволяет обеспечить полную конфиденциальность информации о ваших средствах и финансовых транзакциях. Решается эта задача за счет использования смешанного протокола, согласно которому транзакции становятся анонимными посредством перемешивания транзакций нескольких сторон и объединения потоков средств таким способом, что разделить их оказывается невозможным. Все это осуществляется в децентрализованной сети серверов, называемых *главными узлами* (masternode).

Разработчики системы Dash планируют создать первую ориентированную прежде всего на защиту криптографическую валюту с полностью закодированными биржами и закрытыми блоками транзакций. Дебитные карточки системы Dash могут приниматься по всему миру любыми банкоматами или в магазинах. Кроме того, они могут быть выпущены в различных монетарных стандартах, таких как доллары, евро или фунты.

Система Dash обладает следующими свойствами.

- » **Конфиденциальность.** Все платежи, транзакции и хранимые средства в системе абсолютно конфиденциальны, и никто не может их отследить.
- » **Быстродействие.** Использование технологии InstantX и сети главных узлов позволяет осуществлять любые транзакции в течение нескольких секунд.
- » **Защищенность.** Усовершенствованные методы шифрования и протоколы доверия делают систему абсолютно безопасной.
- » **Глобальные масштабы.** Сервис мгновенных транзакций Darksend делает систему комплексной и позволяет переводить средства в любой уголок мира быстро и анонимно.
- » **Невысокие комиссии.** Выполнение транзакции перевода денег обходится всего в несколько центов.

В системе Dash пользователям предлагают два типа кошельков — онлайн-версия кошелька и автономная версия, которую можно загрузить и установить на собственном компьютере.

Компания ConsenSys: децентрализованные приложения

Компания ConsenSys (<http://www.consensys.net>) была создана одним из основателей системы Эфириум. Она занимается созданием децентрализованных приложений, разработкой блокчейн-решений для организаций и созданием различных инструментов разработчика для экосистемы блокчейна Эфириум.

Компания ConsenSys совместно с корпорацией Microsoft работает над созданием блокчейн-системы цифровых свидетельств идентичности, проекта с открытым кодом. Это партнерство было создано в соответствии с потребностью, изложенной в документе ID2020 ООН, целью которого является сдерживание волны преступлений против человечества, осуществление которых возможно по причине отсутствия средств идентификации. План состоит в получении легальных свидетельств идентификации для каждого человека к 2020 году.

Компания ConsenSys разработала решение цифровой идентификации, получившее название “uPort” и включающее интегрированную поддержку репутационной системы и обеспечение транзакционной безопасности. Система uPort позволяет любому человеку управлять элементами своего свидетельства идентичности через портативные и стационарные устройства, имеющие доступ к среде блокчейна системы Эфириума.

Пользователи в менее развитых частях мира могут самостоятельно загружать свои свидетельства идентичности и репутации.

Приложение RepSys добавляет новые функциональные возможности к системе uPort. Оно позволяет отдельным лицам, организациям и “вещам” засвидетельствовать поведение своих контрагентов в различных типах транзакций. Его можно уподобить обзорам на сайте Amazon, но сделанным в отношении свидетельств цифровой идентичности. Система uPort поддерживает атрибуты репутации. Это могут быть как официальные элементы наподобие выдаваемых правительствами документов идентификации личности, так и страницы на сайте Facebook. Компания ConsenSys также разработала решение в отношении требования “знай своего клиента”, благодаря которому финансовые организации могут предлагать их владельцам различные финансовые услуги.

Предметный указатель

- A**
API, 113
- B**
Bitaddress, 73
- D**
DAO, 27; 31; 79; 91; 180; 247
 опасности, 81
 страхование, 207
DAPP, 79
DGB, 124
DigiByte, 124
 алгоритмы майнинга, 125
 история, 124
 криптовалюта, 124
 майнинг, 125
 сервис
 digibytegaming, 131
 DiguSign, 129
 токены, 130
Digital assets, 78
DLoc, 120
- E**
Ethereum, 27; 75
Etheria, 79
- F**
Factom, 105
 API, 113
 Factoid или FCT, 109; 114
 Harmony, 117
 консенсус, 110
 корпорация, 112
 криптовалюта, 109; 114
 назначение, 106
 помещение информации, 115
 программные продукты, 113
 протокол, 106; 108
 слои и цепочки, 107
 технология dLoc, 120
 транзакции, 109
 федеральные узлы, 114
 хранение информации, 108
 якорный блок, 111
- G**
GateHub
 Ripple, 101
GitHub, 54; 66
- H**
Hyperledger, 135; 160
 Fabric, 138
 Iroha, 142
 Sawtooth Lake, 144
 бизнес-контракты, 140
 история, 136
 цепочки поставок, 140
- I**
IoT, 30; 210
- K**
KYC, 217
- P**
Proof of Elapsed Time, 145
Proof-of-stake, 77
Proof-of-work, 29; 77; 86; 107; 109
- R**
RFID, 112; 222
Ripple, 93; 102
 Интернет ценности, 95
 доверие сторон, 98
 доверительные узлы, 98
 история, 94
 консенсус, 98
 кошелек, 101
 криптовалюта, 95; 96
 опасности, 102
 особенности, 95; 99
 отличия, 97
 протокол, 96
 финансовые операции, 95; 96
- S**
Smart Nation, 210; 227
Solidity, 78
- U**
UPort, 264
UTXO, 149
- A**
АСИК-майнер, 128
Автономные организации, 27; 79; 180
 создание, 87
Анонимные транзакции, 263
Аппаратный кошелек, 249
- Б**
Биткойн, 26; 44; 62; 64; 69; 183
 Lightning Network, 258
 бумажный кошелек, 72
 заблуждения, 67
 майнинг, 64; 70
 ограничения, 65
 опасности, 69
 протокол, 64
 раздувание сети, 76
 сообщество, 66
 транзакция, 48
Биткойн-адрес, 46
Биткойн-кошелек, 45
Битлицензия, 219
Блок, 25
Блокчейн, 15; 21; 64; 175
 DigiByte, 123
 Factom, 105; 108
 Ripple, 93; 96
 Биткойна, 61
 Эфириум, 76
 взлом, 83
 входные данные, 23
 выбор типа, 38
 в Fabric, 138
 использование как
 свидетельства, 119
 консенсус, 28
 криптовалюта, 23
 платформа
 Sawtooth Lake, 145
 полный узел, 23
 применение, 34
 реестр, 64
 сеть, 26
 смарт-контракты, 49
 создание, 56
 типы, 38
 токен, 23
 транзакция, 23
 хардфорт, 82
 хеш, 25
Блокчейн-альянс, 242
Блокчейн-платформа
 Fabric, 138; 148
 Sawtooth Lake, 144

Блокчейн-приложение, 26; 30
от IBM, 163

Блокчейн-проект, 36
план, 40

Блокчейн-протокол, 23

Блокчейн-реестр, 27

Harmony, 117

публикация данных, 248

Блокчейн-сеть, 154

закрытая, 155

частная, 54

Блокчейн-технология, 24; 43

IoT-платформа IBM, 166

Великобритания, 215

в Великобритании, 220

в Дубай, 217

в Индии, 212

в Китае, 213; 229

в Нью-Йорке, 219

в Сингапуре, 210; 216; 227

в Эстонии, 227; 228

в банковском деле, 174

возможности, 37

для Интернета, 230

доверие, 106

идентификация

личности, 184

интернет вещей, 203

ипотека, 192

перспективы, 194

источники информации, 232

страхование, 200

титульное страхование, 188

хеширование, 25

электронная почта, 230

Блокчейн-цепь

принцип работы, 23

структура, 25

типы, 22

Боковая цепочка, 258

Большие данные, 204; 213

В

Веб-сервис

Badbitcoin, 69

Bitaddress, 73

BitcoinVanityGen, 46

BitGo, 250

Blockchain, 45

Coinbase, 45

CoinWarz, 126

digibytegaming, 131

Ethereum GitHub, 86

FreeFactomizer, 115

GateHub, 101

GitHub, 54; 66; 115; 138; 170;

221; 252

Hashflare, 71

ShapeShift, 261

Slack, 138

SmartContract, 51

Харо, 45

Входные данные, 23

Вытеснение мошенниче-
ства, 183

Г

Гарантированные платежи, 182

Главный узел, 263

Гражданство, 226

Д

Дерево

Меркла, 63; 107

решений, 39

Децентрализованное приложе-
ние, 79

Доверенное авторство, 233

Доверительная среда выполне-
ния, 145

Доказательство несовершен-
ия, 185

З

Знай своего клиента, 176; 217;
256

И

Инструмент публикации, 107

Интеллектуальная собствен-
ность, 234

Интернет вещей, 30; 160; 164;
196; 203; 210; 221; 233

Ипотека, 192

Factom Harmony, 117

К

Ключ

закрытый, 45; 47

открытый, 47

Компания

21, 262

Ancun Zhengxin, 229

Bitfury Group, 260

Bitnation, 229

BitPay, 181

BitPesa, 181

Bitwage, 181

Blockcypher, 222

Blockstream, 258

Circle, 220

Cloudera, 213

CME Group, 216

Code Valley, 260

ConsenSys, 156; 264

Credits, 215

Digital Asset, 137

Guardtime, 218

KYCK!, 162

McAfee, 230

Multichain, 243

Nasdaq, 229

Peernova, 213

R3, 216; 256

Ripple, 220

база знаний, 240

RWE, 215

ShoCard, 222

Smartrac, 112; 120; 222

Tierion, 229

TZERO, 257

Wanxiang, 162

Консенсус, 28; 109

Proof of Elapsed Time, 145

Proof-of-stake, 77

Sumeragi, 142

Консорциум

Hyperledger, 135; 160

Linux Foundation, 136

R3, 137

Корпорация

Factom, 233

университет, 240

Keystone Capital, 257

Кошелек

BitGo, 250

аппаратный, 249

бумажный, 249

Краудфандинг, 76; 114

страхование, 206

Криплет, 149

типы, 151

Криптовалюта, 23; 63; 144;

246; 253

Dash, 263

DGB, 124; 126

FCT, 109

XRP, 95; 96; 99

майнинг, 64

сайт ShapeShift, 261

эфир, 84

Криптовалютная биржа, 29;

251

Bitfinex, 29; 131

компании Dash, 263

Криптография, 63

М

Майнинг, 64; 70

биткойнов, 70

облачный, 71

эволюция, 128

Майнинговая ферма, 128

Матрица взвешенных реше-
ний, 35

Мертвый капитал, 179; 197

Микроинвестиции, 180

Микроплатежи, 182; 262
Микрострахование, 201

Н

Начисление зарплаты, 180
Нотариальное засвидетельство-
вание, 196

О

Облачная платформа, 153
Azure, 153
 технология Chain, 154
Cloud Foundry, 160; 161
Облачный сервис
Azure, 147; 152
Cortana, 157
 блокчейн-
 инструменты, 156
 закрытая сеть, 155
Оракул, 150
Открытая торговля, 181

П

Пакет Iroha, 144
 мобильные приложения, 143
Перевод денег, 176
Перманентная история, 177
Пиктограммы, 17
Платформа
 Blockstream Elements, 258
 Bluemix, 160; 161; 168
 Fabric, 138; 141
 ценные бумаги и акти-
 вы, 141
 контракты Chaincode, 139
HiveMind, 244
Sawtooth Lake
 консенсус, 145
Watson, 163; 167
Покупка и продажа недвижимо-
сти, 189
Полный узел, 23; 28; 64; 85
Приложение
 Chain, 154
 Harmony, 117
 цифровой регистр, 118
RepSys, 264
Программа
 Docker, 55
 GitHub Desktop, 55
Проект
 Bletchley, 148
 криплеты, 149; 151
DigiByte
 DigiKnow, 241
Dubai Points, 218

Fabric, 138
Hercules, 214
Hyperledger, 153
Iroha, 142
OpenBazaar, 259
R3, 256
Sawtooth Lake, 144
Smart Nation, 227
Solidity, 157
TZERO, 257
Дубаи-2020, 217
Эфириум, 240
Протокол NFC, 120

Р

Радиочастотный идентифика-
тор, 112
Распределенный реестр, 206
Регулируемая песочница, 216
Реестр, 64

С

Сайт
 Bitcoin Core, 242
 Ethereum101, 240
 ShapeShift, 261
Сатоши Накамото, 62
Свидетельство идентично-
сти, 221; 231; 264
Сервис DigiSign, 129
Сертификат Кимберли, 218
Сеть
 Lightning Network, 258
 Wi-Fi, 251
 блокчейна, 26
Система
 Dash, 263
 uPort, 264
 Торренса, 188
Смарт-город, 210
Индия, 211
Смарт-контракт, 49; 80; 83;
 233; 247
 Chaincode, 139; 165
 оракул, 150
 рекомендации, 91
 смарт-обязательство, 50
 страхование, 205
Страхование, 200

Т

Технология dLoc, 120; 222
Титульное страхование, 188
Токен, 23; 28; 63
 DGB, 126
 Factoid, 114

майнинг, 64
эфир, 84
Транзакция, 23; 25
манипулирование, 103

У

Узел, 96
Университет блокчейн-
технологии, 242
Управление недвижимо-
стью, 187
Условные обозначения, 17

Ф

Фанни Мей, 192
Федеральные узлы, 114
Фиат, 261

Х

Хардфорк, 82; 83
Хеш, 25
Хеширование, 63
 дерево Меркла, 63
Холодное хранилище, 249

Ц

Централизованное дове-
рие, 205
Цифровая валюта, 175
Цифровые активы, 78; 260
Sawtooth Lake, 145

Ш

Шлюзы устройств, 167

Э

Электронное резидентство, 227
Эфириум, 27; 54; 75; 90; 153
 DAO, 79; 91
 создание, 87
DAPP, 79
uPort, 264
использование в Azure, 156
кошелек, 85; 86
майнинг, 85
протокол, 77; 78
смарт-контракты, 83; 91
сообщество, 82; 92
токены, 82
узлы, 85
эфир, 84

Я

Якорный блок, 111

Блокчейн для чайников®

Шпаргалка

Как работает блокчейн

Блокчейн представляет собой распределенную базу данных, работа которой контролируется глобальной сетью компьютеров. Информация этой базы данных распространяется и непрерывно согласовывается между компьютерами сети, — эти компьютеры называют узлами, майнерами или пирами. Но, как бы их ни называли, именно эти компьютеры создают и поддерживают свой блокчейн, проверяя и распространяя поступающие к ним данные — ту информацию, которую вводят (публикуют) пользователи сети.

Часто эти данные представляют собой сведения о перемещении криптовалюты от одного пользователя сети к другому. Например, пересылая некоторую сумму биткойнов своему другу, вы создаете и публикуете в сети Биткойна соответствующую запись. Узлы этой сети проверяют, не пересылали ли вы ранее указанную криптовалюту на другой адрес. Если все в порядке, то указанную сумму снимут с вашего счета и добавят на счет вашего друга.

Таковыми действиями узлы сети предупреждают возможность “двойной траты” криптовалюты. В случае системы Биткойна решение данной задачи обеспечивается требованием, чтобы каждый узел сети хранил собственную полную запись всей истории операций ввода данных, выполненных в этой сети за все время ее существования. Это гарантирует, что он всегда сможет проверить текущий баланс любого счета в системе, включая и ваш.

В разных блокчейнах вводимые данные необязательно должны представлять лишь информацию о перемещении криптовалюты. Некоторые блокчейн-системы позволяют публиковать в них различные данные, но за определенную плату. На содержание этих данных не накладывается жестких ограничений, в таких системах просто используется модель взимания платы за публикацию. Также эти системы позволяют получить подтверждение достоверности хранящихся в них данных без необходимости обращаться к полной истории транзакций блокчейна.

Большинство блокчейн-систем не контролируются каким-то отдельным узлом или их небольшой группой, что исключает существование в них единственной точки отказа. Все вводимые данные доступны для просмотра всей сети. Когда данные записываются в блокчейн, удалить их из него уже невозможно, они будут храниться там вечно.

Главным новшеством в блокчейнах, которое резко отличает их от обычных баз данных, является то, что их узлы непрерывно достигают соглашения о состоянии исторических данных системы за счет разделения и ограничения вводимой информации, причем без какого-либо центрального сервера или контролирующего органа.

Блокчейн для чайников®

Шпаргалка

Как работают смарт-контракты

Смарт-контракты, которые иногда называют также *чейн-кодами*, представляют собой какие-либо соглашения, которые были особым образом закодированы и помещены в блокчейн. Эти контракты в действительности являются программным кодом — просто набором операторов “если-то” и “если-то-иначе”. Код контракта встраивается непосредственно в блокчейн, что гарантирует ему неизменяемость и длительность хранения. Наиболее популярными блокчейн-платформами для создания смарт-контрактов сейчас являются Эфириум (Ethereum) и Hyperledger Fabric.

В блокчейны при сохранении в них смарт-контрактов также записываются необходимые им данные и ведутся их балансовые счета в криптовалюте, при этом фиксируется вся история связанных с ними транзакций.

У смарт-контрактов есть внутренняя память, в которой содержится их программный код. Этот код запускается, когда выполняются указанные в контракте требования и ограничения. Эти требования и ограничения могут быть внутренними или внешними по отношению к самому смарт-контракту.

Если программному коду смарт-контракта для определения, выполняются ли заданные требования и ограничения, необходим некоторый внешний источник, в нем используется *оракул* (источник знаний). Например, оракул может представлять собой источник данных о погоде; это может потребоваться, если смарт-контракт представляет собой договор страхования урожая. В этом случае сам страховой контракт может выглядеть, например, так: “Если температура опустится ниже 0° на период более одного часа, выплатить владельцу страховки 5000 долларов”.

Смарт-контракты отслеживают данные, контролируют выполнение установленных требований и ограничений и, если это так, приводят контракт в исполнение. Не существует никакого внешнего элемента или юридической системы, которая интерпретирует контракт и намерения заключивших его сторон. В данном случае закон — это программный код смарт-контракта.

Блокчейн для чайников®

Шпаргалка

Что такое криптовалюта

Криптовалюты, которые иначе называют виртуальными валютами, цифровыми валютами/деньгами или токенами, на самом деле имеют мало общего с настоящей валютой, такой как доллары, рубли или евро. Они существуют виртуально, “живут” лишь в компьютерных сетях и никак не обеспечиваются правительствами. В действительности они обеспечиваются лишь той сетью, в которой были созданы. Говоря техническим языком, криптовалюты являются лишь особыми конфиденциальными записями в базе данных. Чтобы можно было внести в эти записи какие-либо изменения, необходимо выполнение конкретных жестко заданных условий. Созданные с использованием криптографии, эти записи защищаются математикой, а не людьми.

Конфиденциальные записи помещаются (*публикуются*) в базе данных, но это база данных особого типа, распределенная в *пиринговой* (одноуровневой) компьютерной сети. Например, отправляя биткойн своему другу, на самом деле вы создаете особую конфиденциальную запись и отправляете ее в сеть Биткойна. Теперь этой сети необходимо убедиться в том, что вы не пытаетесь использовать одну и ту же запись (один и тот же токен) дважды, причем осуществляется это без обращения к какому-либо центральному серверу или контролирующему органу. В случае нашего примера сеть должна получить гарантию, что вы не отправили один и тот же биткойн поочередно двум своим друзьям.

В пиринговой сети проблема “двойной траты” (т.е. отправки одного и того же биткойна двум разным людям) в большинстве случаев решается за счет того, что у каждого равноправного узла (пира) есть собственная полная копия исторических сведений обо всех записях, сделанных в сети. Наличие полной истории позволяет получить баланс любого пользователя, включая вас. Главным нововведением в криптовалютах является тот факт, что соглашение о том, что представляет собой правильная история, достигается в сети без использования центрального сервера или какого-то управляющего органа.

Все эти конфиденциальные записи и являются реальным представлением криптовалюты.

Блокчейн для чайников®

Мини-рубрика

Что такое криптовалюта

Криптовалюта генерируется в самой сети и в большинстве случаев новые токены используются как вознаграждение для тех узлов (иначе их иногда называют *майнерами*), которые обеспечивают защиту сети и осуществляют контроль поступающих записей. Каждая сеть имеет собственный уникальный вариант процедуры генерации токенов и их распределения между узлами.

Например, в сети Биткойна узлы (в этой сети их принято называть *майнерами*) вознаграждаются за успешное создание блока, принятого и одобренного остальными узлами сети. Блок — это группа входных записей, помещаемая в распределенную базу данных. Создание каждого блока связано с поиском хеша — числового значения в заголовке блока, которое будет связывать его с предыдущим блоком цепочки базы данных. Именно отсюда возникло понятие *блокчейн*, т.е. «цепочка блоков». Блоки включают группы записей, а с помощью хешей из них образуется единая цепочка. Хеши представляют собой некий криптографическо-логический пазл. Можно представить его себе как что-то, подобное головоломке Судоку, в решении которой узлы соревнуются между собой, чтобы получить право на включение нового созданного ими блока в блокчейн.

Каждая криптовалюта имеет свои отличия, но для большинства из них будут общими следующие основные характеристики.

- **Необратимость.** После отправки криптовалюты и подтверждения этой транзакции сетью вернуть ее будет уже невозможно. Криптовалюты можно перемещать только в одном направлении, никаких возвратов платежей здесь быть не может.
- **Анонимность.** Открыть кошелек можно абсолютно анонимно, для этого не требуется какой-либо идентификатор. Однако вся процедура может иметь различную степень анонимности в зависимости от того, какой токен используется.
- **Высокая скорость работы и глобальный доступ.** Входные записи немедленно рассылаются по всей сети и получают подтверждение всего за несколько минут.
- **Принцип построения сети обеспечивает ее безопасность.** Криптовалюты используют новейшие криптографические технологии, но они пока могут находиться на ранней стадии разработки.
- **Контролируемые ресурсы, ограничиваемые сетью.**

Блокчейн для чайников®

Минифика

Безопасное хранение криптовалют

Криптовалюты привлекли к себе пристальное внимание широкой публики, но мир криптовалют сейчас очень напоминает пресловутый Дикий Запад: здесь вы найдете не только доброжелательных пионеров, всегда готовых оказать помощь и указать правильный путь, но и безжалостных бандитов, желающих отобрать у вас все, что вы имеете.

Криптовалюты наиболее уязвимы в централизованных цифровых системах, имеющих доступ к Интернету. Сюда относятся интерактивные кошельки, криптовалютные биржи, кошельки на вашем компьютере, облачные хранилища закрытых ключей (цифровых ключей, используемых для защиты ваших токенов) и мобильные приложения.

Чтобы защитить свою криптовалюту от воров, пользуйтесь *холодными хранилищами* (архивами закрытых ключей на устройствах, не имеющих доступа к Интернету). Наилучшими вариантами холодных хранилищ являются автономные аппаратные кошельки, USB-накопители и бумажные кошельки.

Поскольку криптовалюты функционируют на основе открытых блокчейн-сетей, существует множество способов, которыми кто-то может присвоить ваши деньги, проследить за вашими расходами или просто так или иначе нарушить вашу конфиденциальность. Чтобы предотвратить любые формы хищений, всегда следуйте следующим рекомендациям.

- **Используйте несколько кошельков.** Не существует никаких ограничений на количество адресов кошельков, которыми вы можете пользоваться. Некоторые считают полезным генерировать новый адрес всякий раз, когда отправляют или получают криптовалюту.
- **Храните в веб-кошельках минимально необходимые суммы.** Веб-кошельки — весьма привлекательная цель для хакеров, поэтому храните в них лишь небольшие суммы криптовалюты. Кошельки на вашем собственном компьютере также достаточно уязвимы. Поэтому крупные суммы криптовалют храните только в холодных хранилищах.
- **Обеспечьте секретность.** Не позволяйте кому-либо ознакомиться с закрытыми ключами доступа к вашей криптовалюте. Каждый, кто их узнает, получит полный (и необратимый) доступ к вашим финансам.

Узнайте о том, как блокчейн-технология меняет нашу жизнь

Блокчейн — революционная технология, положенная в основу феномена биткойна, — может оказать огромное влияние на финансовые транзакции, защиту данных и информационную целостность любого бизнеса. В этой книге рассказывается, как эта технология работает и как ваша компания может употребить всю ее мощь себе во благо. Ознакомьтесь с различными типами блокчейнов, с основными принципами работы и возможностями уже существующих блокчейн-платформ. Узнайте, какие преимущества она может принести с собой в различные сферы жизни современного мира.

В книге...

- Основы блокчейн-технологии
- Блокчейн-решения для конкретных целей
- Воздействие блокчейн-технологии
- Выбор и применение блокчейн-решений
- Десять правил использования блокчейна, которые никогда не следует нарушать

Тиана Лоуренс является сооснователем компании Factom, которая предоставляет блокчейн-решения для многих бизнес-задач, включая повышение защищенности устройств в Интернете вещей (IoT). Компания Factom входит в двадцатку наиболее влиятельных блокчейн-компаний.

 **ДИАЛЕКТИКА**

www.dialektika.com

Изображение на обложке:
©Depositphotos.com/26274295
Автор: 3dmentat

Технологии ПО/криптовалюты

ISBN: 978-5-9500295-6-1




для
ЧАЙНИКОВ®