

Мелани Свон

Блокчейн

[Купить книгу на сайте kniga.biz.ua >>>](#)

Blockchain

Blueprint for a New Economy

Melanie Swan

Beijing • Cambridge • Farnham • Köln • Sebastopol • Tokyo

O'REILLY®

[Купить книгу на сайте kniga.biz.ua >>>](http://kniga.biz.ua)

Мелани Свон

Блокчейн

Схема новой экономики



Издательство «Олимп—Бизнес»
Москва, 2017

[Купить книгу на сайте kniga.biz.ua >>>](http://kniga.biz.ua)

УДК 004:338
ББК 65.050.253
С25

*Научный редактор Виктор Фомин,
главный редактор ресурса BitNovosti.com*

Свон, Мелани

С25 Блокчейн: Схема новой экономики / Мелани Свон : [перевод с английского]. — Москва : Издательство «Олимп—Бизнес», 2017. — 240 с., ил.

ISBN 978-5-9693-0360-7

Блокчейн — это многофункциональная и многоуровневая информационная технология, предназначенная для надежного учета различных активов. Потенциально эта технология охватывает все без исключения сферы экономической деятельности и имеет множество областей применения. В их числе: финансы и экономика; операции с материальными и нематериальными активами, учет в государственных и частных организациях и организациях смешанного типа. По сути, блокчейн — это новая организационная парадигма для координации любого вида человеческой деятельности. Возможно даже, что это наше будущее, о котором полезно узнать уже сегодня. Книга адресована тем, кто интересуется финансовыми инструментами и технологическими инновациями, в частности криптотехнологиями.

**УДК 004:338
ББК 65.050.253**

Все права защищены. Воспроизведение всей книги или ее части в любом виде воспрещается без письменного разрешения издателя.

A member of: **BPR** 
Business Publishers Roundtable.com

ISBN 978-5-9693-0360-7

© 2015 Melanie Swan. All rights reserved.
© Перевод на русский язык, оформление,
издание. Издательство «Олимп—Бизнес»,
2017

Купить книгу на сайте kniga.biz.ua >>>

Оглавление

Об авторе	13
Предисловие	15
Валюта, контракты и приложения блокчейн вне финансовых рынков	17
Блокчейн 1.0, 2.0 и 3.0	19
Что такое биткойн?	20
Что такое блокчейн?	22
Связанный мир и блокчейн: пятая революционная парадигма вычислений	24
<i>Сеть биткойн-платежей для поддержки машинной экономики: M2M/IoT</i>	26
Повсеместное внедрение: доверие, удобство и простота использования	28
<i>Биткойн-культура: фестиваль Bitfilm</i>	30
Цели, методология и структура этой книги	30
ГЛАВА 1. Блокчейн: фундамент для криптовалют (Блокчейн 1.0)	35
Стек технологий: блокчейн, протокол, валюта	35
Двойное расходование и задача византийских генералов	37

Как работает криптовалюта	39
<i>Сервисы электронных кошельков</i>	
<i>и криптозащита персональных данных</i>	40
<i>Прием биткойна торговыми</i>	
<i>организациями</i>	42
Резюме: практическое использование	
Блокчейн 1.0.	42
<i>Отношение к фиатным деньгам</i>	43
<i>Правовой статус</i>	46

ГЛАВА 2. **Блокчейн: основа для контрактов**

(Блокчейн 2.0)	49
Новые возможности	49
Финансовые сервисы	53
Краудфандинг	56
Биткойн-тотализаторы	58
Умные активы	58
Умные контракты	63
Проекты Блокчейн 2.0	66
Проекты разработки кошельков	66
Платформы и API разработки блокчейна.	68
Экосистема блокчейна: децентрализованные хранение, коммуникации и вычисления	69
Ethereum: Тьюринг-полная виртуальная машина	72
<i>Counterparty повторно создает платформу</i>	
<i>умных контрактов Ethereum</i>	73
Децентрализованные приложения, организации, компании и общества: все более автономные	
умные контракты	74
<i>Децентрализованные приложения</i>	75

<i>Децентрализованные автономные организации и корпорации</i>	78
<i>Децентрализованные общества и самоограничивающиеся организации</i>	80
<i>Автоматические рынки и торговые сети</i>	81
Блокчейн как путь к искусственному интеллекту	82

ГЛАВА 3. **Блокчейн: приложения для применения за рамками финансовых областей (Блокчейн 3.0).**

Блокчейн-технология — новая и высокоэффективная модель организации деятельности	83
<i>Возможность расширения блокчейн-концепций</i>	84
<i>Фундаментальные экономические принципы: признание ценности, определение стоимости и организация обмена</i>	85
<i>Блокчейн-технология позволяет администрировать любые дискретные единицы</i>	86
<i>Блокчейн и предиктивная автоматизация с использованием больших данных</i>	87
Распределенные организационные модели, устойчивые к цензуре	88
Namescoin — децентрализованная система доменных имен	91
<i>Другие децентрализованные службы DNS и технические сложности</i>	92
<i>Свобода слова и борьба с цензурой: проекты Alexandria и Ostel</i>	93
<i>Децентрализованные DNS и цифровая идентификация личности</i>	94
Цифровая идентификация	95
<i>Нейтралитет блокчейна</i>	98
<i>Цифровой разрыв и биткойн</i>	99

Цифровая собственность: службы аттестации блокчейна (нотариальные службы, защита интеллектуальной собственности)	100
<i>Хеширование и временные метки</i>	101
<i>Доказательство существования</i>	103
<i>Ограничения</i>	105
<i>Виртуальный нотариус, Bitnotar и Chronobit</i>	106
<i>Monegraph: защита изображений в интернете</i> . . .	107
<i>Подтверждение владения цифровой собственностью как автоматическая функция</i>	109
<i>Нотариальные блокчейны как класс блокчейн- инфраструктуры</i>	110
<i>Персональные распределенные журналы мышления</i>	111
Блокчейн-правительство	113
<i>Децентрализованные управляющие службы</i>	116
<i>PrecedentCoin: решение споров в блокчейне</i>	120
<i>Гибкая демократия</i>	121
<i>Выборы со случайной выборкой</i>	124
<i>Футархия: двухэтапная демократия с голосованием и рынками прогнозов</i>	124
<i>Влияние блокчейн-правительства на социальную зрелость</i>	127
 ГЛАВА 4. Блокчейн 3.0: эффективность и координация в обществе	 129
Наука на блокчейне: Gridcoin, Foldingcoin	129
<i>Распределенные сверхпроизводительные вычисления</i>	131
<i>Глобальное здравоохранение: биткойн и борьба с инфекционными заболеваниями</i>	132
<i>Биткойн и благотворительность</i>	133
Блокчейн и геномика	133

<i>Блокчейн-геномика 2.0: секвенирование в общечеловеческом масштабе</i>	135
<i>Технологии блокчейна как универсальная модель развития</i>	137
<i>Genotecoin, GenomicResearchcoin</i>	137
Блокчейн и здравоохранение	139
<i>Healthcoin</i>	139
<i>Электронные медицинские карты</i>	140
<i>Хранилища медицинских данных в блокчейне</i>	140
<i>Службы медицинского освидетельствования в блокчейне</i>	141
<i>Контракты на предоставление медицинских услуг</i>	142
<i>Поддержка банков вирусов и хранилищ семян</i> . . .	142
Блокчейн-обучение: MOOK биткойна и умные контракты на обучение	143
<i>Learncoin</i>	145
<i>Биржи контрактов на обучение</i>	145
Научные публикации в блокчейне: Journalcoin	145
Блокчейн может не все	150
Баланс между централизацией и децентрализацией . .	151
ГЛАВА 5. Продвинутые концепции	153
Терминология и концепции	153
Валюта, токен, токенизация	155
<i>Валюты сообществ: частные деньги Хайека</i> . . .	157
<i>Валюты кампусов</i>	158
<i>Разбрасывание монет как стратегия распространения</i>	160
<i>Валюта: новые определения</i>	161
Множественность валют: монетарные и немонетарные валюты	162

Демередж валюты: побуждение к действию и перераспределение	164
<i>Расширяемость концепций демереджа</i>	167
ГЛАВА 6. Ограничения.	171
Технические сложности	171
Возможные улучшения.	176
Сложности бизнес-модели.	178
Скандалы и восприятие обществом	179
Государственное регулирование	181
Проблемы конфиденциальности персональных данных.	183
Итог: тенденции к децентрализации сохраняются.	183
ГЛАВА 7. Заключение	185
Блокчейн как информационная технология.	187
<i>Искусственный интеллект блокчейна: консенсус как механизм развития дружественного искусственного интеллекта</i>	188
<i>Обширные возможности для интеллекта</i>	189
<i>Транзакции выполняются только для дружественных ИИ</i>	189
<i>Умные контракты, действующие от имени цифрового интеллекта</i>	191
<i>Консенсус блокчейна повышает плотность информации во Вселенной</i>	192
ПРИЛОЖЕНИЕ А. Основные сведения о криптовалютах	195
Краткий экскурс в асимметричную криптографию	197

ПРИЛОЖЕНИЕ Б. Применения блокчейна — список от компании Ledra Capital.	200
ПРИЛОЖЕНИЕ В. Русскоязычные ресурсы по блокчейн-технологиям	204
Источники и примечания	205
Благодарности	228
Указатель	229

Об авторе

Мелани Свон — основатель Института блокчейн-исследований (Institute for Blockchain Studies), магистр современной философии Кингстонского университета в Лондоне и Университета Париж VIII, выпускник программы MBA по специализации «Финансы» Уортонской школы бизнеса Пенсильванского университета. Свон стажировалась в финансовой корпорации Fidelity и банке JP Morgan, в качестве предпринимателя и консультанта стартапов GroupPurchase и Prosper приобрела значительный опыт работы на новых рынках, который применила, разработав принципы оценки и учета цифровых активов в виртуальном мире для компании Deloitte. Свон стала одним из первых участников движения Quantified Self; в 2010 году она основала DIYgenomics — организацию, которая в числе первых занялась исследованиями здоровья, организуемыми по принципу краудсорсинга. Мелани Свон занимает должности преподавателя в Университете Сингулярности (Singularity University) и аффилированного научного сотрудника Института этики и новых технологий (Institute for Ethics and Emerging Technologies). Ее статьи регулярно публикуются на сайте Edge.org в разделе Annual Essay Question.

Предисловие

Блокчейн — это многофункциональная и многоуровневая информационная технология, предназначенная для надежного учета различных активов. Потенциально эта технология охватывает все без исключения сферы экономической деятельности и имеет множество областей применения. В их числе: финансы, экономика и денежные расчеты, а также операции с материальными (реальная собственность, недвижимость, автомобили и т. п.) и нематериальными (права голосования, идеи, репутация, намерения, медицинские данные, личная информация и т. п.) активами. Блокчейн создает новые возможности по поиску, организации, оценке и передаче любых дискретных единиц. По сути, это новая организационная парадигма для координации любого вида человеческой деятельности.

Вполне вероятно, мы находимся на пороге блокчейн-революции. Эта революция началась с появлением новой экономической реальности в интернете — альтернативной валюты под названием биткойн, которая эмитируется и обеспечивается не государством, а пользователями биткойн-сети при автоматизированном достижении консенсуса между ними. Но уникальность этой валюты заключается в том, что ее пользователям не обязательно доверять друг другу. Встроенные в систему алгоритмы саморегулирования предотвращают любые злонамеренные попытки обмана. Если быть точным, то с технической точки зрения биткойн — это цифровые деньги, обращающиеся

в децентрализованной, пиринговой электронной платежной системе*, основанной на публично доступной книге учета, именуемой «блокчейном».

По сути — это новая форма денег, комбинирующая одноранговый обмен файлами¹ подобно BitTorrent, и криптографическую систему с открытым ключом^{2:**}. С момента возникновения биткойна в 2009 году у него появился целый ряд подражателей — альтернативных криптовалют, в целом использующих такой же подход, но с некоторыми изменениями и улучшениями. Важно, что блокчейн-технология способна стать органичной экономической оболочкой сети интернет, обслуживающей онлайн-платежи, децентрализованный обмен, заработок и расходование токенов ценности, получение и передачу цифровых активов, а также выпуск и исполнение умных контрактов. Как средство децентрализации эти технологии могут стать следующим фундаментальным прорывом в информационных технологиях — после мейнфреймов, персональных компьютеров, интернета, мобильных и социальных сетей. Они способны коренным образом изменить жизнедеятельность человечества, как это в свое время сделал интернет.

* Одноранговый, децентрализованный или пиринговый (*англ.* peer-to-peer, P2P — равный к равному) обмен файлами — это обмен файлами в сети, основанной на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пираты. — *Прим. ред.*

** Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) — система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передается по открытому (то есть незашифрованному, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ. — *Прим. ред.*

Валюта, контракты и приложения блокчейн вне финансовых рынков

Потенциальные выгоды от применения блокчейн-технологии лежат не только в сфере экономики — они распространяются на политику и гуманитарные, социальные и научные области. Технологические возможности блокчейна уже задействуются для решения реальных общественных задач. Например, блокчейн может стать средством противостояния политическому произволу за счет внедрения децентрализованных облачных функций, которые ранее управлялись исключительно официальными организациями. Это удобно таким лицам, как Эдвард Сноуден, и таким организациям, как WikiLeaks, в связи с тем, что пожертвования на их адрес через международные платежные системы в ряде стран находятся под запретом.

Преимущества блокчейн-технологий оценили и транснациональные политически нейтральные организации, такие как ICANN* и службы DNS. Помимо ситуаций, когда общественные интересы выходят за рамки национальных границ, целые отрасли экономики смогут освободиться от избыточного регулирования и лицензирования, навязанных иерархическими структурами, лоббистами и группами влияния внутри государств. Это позволит создавать новые модели бизнеса, не отягощенные ненужными посредниками. Активно поддерживаемые отраслевым лобби изменения в законодательстве фактически запретили предоставлять рядовым потребителям новые услуги в области генетики^{3:**}, но новейшие экономические моде-

* ICANN — Internet Corporation for Assigned Names and Numbers, Корпорация по управлению доменными именами и IP-адресами. — *Прим. ред.*

** В частности, речь идет о персональной геномике — разделе науки, связанном с секвенированием и анализом генома человека. После расшифровки генотипа его можно проанализировать для определения вероятности риска заболеваний человека. — *Прим. ред.*

ли, в частности экономики совместного использования (*sharing economy*), реализуемые такими компаниями, как, например, Airbnb и Uber, эффективно противостоят запретительным инициативам властных структур⁴.

Вдобавок к экономическим и политическим преимуществам, координация, учет и безотзывность транзакций в блокчейн-технологии могут стать такой же основой для прогресса общества, какой в свое время стали «Великая хартия вольностей»^{*} или Розеттский камень. Блокчейн может служить надежным хранилищем имеющих общественную ценность записей, таких как реестры документов и событий, личных данных и активов. В такой системе каждый актив может стать *умным активом* (*smart property*).

Каждый актив в блокчейне кодируется уникальным идентификатором, по которому актив можно отслеживать, контролировать и обменивать, продавать или покупать. Это означает, что любые виды материальных (дома, автомобили и другие) и цифровых активов можно регистрировать и совершать с ними транзакции на блокчейне.

В качестве примера, которых в этой книге будет еще немало, можно привести использование блокчейн-технологии для регистрации и защиты объектов интеллектуальной собственности

^{*} Великая хартия вольностей (*лат.* Magna Carta, также Magna Charta Libertatum) — политико-правовой документ, составленный в июне 1215 года на основе требований английской знати к королю Иоанну Безземельному и защищавший ряд юридических прав и привилегий свободного населения средневековой Англии. Состоит из 63 статей, регулировавших вопросы налогов, сборов и феодальных повинностей, судоустройства и судопроизводства, прав английской церкви, городов и купцов, наследственного права и опеки. Ряд статей Хартии содержал правила, целью которых было ограничение королевской власти путем введения в политическую систему страны особых государственных органов — общего совета королевства и комитета двадцати пяти баронов, обладавшего полномочиями предпринимать действия по принуждению короля к восстановлению нарушенных прав; в силу этого данные статьи получили название конституционных. — *Прим. ред.*

(ИС). Новая отрасль так называемого цифрового искусства (*digital art*) предлагает услуги по частной регистрации в распределенном журнале записей точного содержания любого цифрового актива: файла, изображения, медицинской записи или ПО. Блокчейн может дополнить или полностью заменить собой все существующие системы управления ИС.

Работает это таким образом. Для начала к любому файлу применяется алгоритм, сжимающий этот файл в короткий код из 64 символов, называемый «хеш», который уникален для данного документа⁵. Каким бы ни был размер файла — например, объем файла генома составляет 9 ГБ, — на выходе всегда получается уникальный 64-символьный хеш, идентифицирующий, но не позволяющий восстановить исходный файл. Полученный хеш включается в блокчейн-транзакцию с добавлением метки времени — доказательство существования цифрового актива на тот момент. Имея исходный файл, который хранится на компьютере собственника, а не в распределенном журнале записей, всегда можно повторно вычислить его хеш и убедиться, что содержимое файла не подверглось изменению.

Стандартизированные механизмы правового регулирования, например договорное право, стали революционным шагом вперед для всего общества. Стандартизированные операции с интеллектуальной собственностью при помощи блокчейна могут стать следующей поворотной точкой для лучшей координации цифрового общества — по мере того, как все большая часть экономической деятельности приводится в движение идеями.

Блокчейн 1.0, 2.0 и 3.0

Многие уже начинают понимать, что благодаря своим экономическим, политическим, гуманитарным и юридическим преимуществам биткойн и блокчейн-технологии превращаются в мощнейшую подрывную инновацию, способную коренным

образом изменить большинство аспектов жизни общества. Для упорядочения и удобства давайте разделим различные — существующие и потенциальные — технологические аспекты блокчейн-революции на три категории: блокчейн 1.0, 2.0 и 3.0.

Блокчейн 1.0 — это *валюта*. Криптовалюты применяются в различных приложениях, имеющих отношение к деньгам, например системы переводов и цифровых платежей.

Блокчейн 2.0 — это *контракты*. Целые классы экономических, рыночных и финансовых приложений, в основе которых лежит блокчейн, работают с различными типами финансовых инструментов — с акциями, облигациями, фьючерсами, задатками, правовыми титулами, умными активами и умными контрактами.

Блокчейн 3.0 — это *приложения*, область применения которых выходит за рамки денежных расчетов, финансов и рынков. Они распространяются на сферы государственного управления, здравоохранения, науки, образования, культуры и искусства.

Что такое биткойн?

Биткойн — это цифровая наличность. Это одновременно цифровая валюта и онлайн-платежная система, в которой технологии шифрования обеспечивают управление генерацией денежных единиц и подтверждение перевода средств и которая работает независимо от государственных центробанков.

В терминах легко запутаться, потому что слова «*биткойн*» и «*блокчейн*» могут обозначать любую из трех частей концепции: базовую *блокчейн-технология*, *протокол* и *клиента*, обеспечивающие выполнение транзакций, и собственно криптовалюту (деньги). Кроме того, эти термины могут применяться для обозначения и концепции криптовалют. Это все равно что называть термином «PayPal» сам интернет, через который работает протокол PayPal, служащий для перевода

валюты PayPal. В блокчейн-индустрии эти термины часто смешиваются, поскольку пока не завершился процесс формирования общепризнанного многоуровневого стека технологий.

Биткойн был создан в 2009 году (точная дата — 9 января 2009 г.⁶) неизвестным лицом или группой людей, работавших под псевдонимом Сатоши Накамото (Satoshi Nakamoto). Концепция и подробности работы биткойна изложены в лаконичном и легком для чтения техническом документе «Биткойн: Одноранговая система электронной наличности»^{7:*}. Платежи в децентрализованной виртуальной валюте записываются в публичный реестр (*public ledger*), который хранится на многих — потенциально на всех — компьютерах пользователей биткойна и постоянно доступен для просмотра в интернете.

Биткойн — первая и крупнейшая децентрализованная криптовалюта. Существуют сотни других альткойнов (альтернативных криптовалют), например Litecoin или Dogecoin, но на биткойн приходится около 90% рыночной капитализации всех криптовалют, и он стал фактическим стандартом. Биткойны используются псевдонимно (а не анонимно), то есть для отправки и получения биткойнов и записи транзакций применяются биткойн-адреса — буквенно-цифровые строки длиной 27–32 символов, в чем-то аналогичные адресу электронной почты, а не личная идентификационная информация.

Биткойны создаются как вознаграждение за выполнение математических вычислений. Суть этой работы, называемой *майнингом* (*mining*) в том, что пользователи предоставляют свои вычислительные ресурсы для верификации адресов и записи транзакций в реестр. В награду за участие в майнинге пользователи получают комиссию за транзакции и вновь создаваемые биткойны. Помимо майнинга, биткойны, как

* Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. — Прим. ред.

и любую другую валюту, можно получить в обмен на обычные (фиатные*) деньги, товары и услуги. Пользователи могут отправлять и получать биткойны с помощью *электронного кошелька* через веб-браузер или приложение, установленное на персональном компьютере или мобильном устройстве. В зависимости от размера транзакции с суммы может как взиматься комиссия, так и нет.

Что такое блокчейн?

Блокчейн — это технология надежного распределенного хранения записей обо всех когда-либо совершенных биткойн-транзакциях. Блокчейн представляет собой цепочку блоков данных, объем которой постоянно растет по мере добавления майнерами новых блоков с записями самых последних транзакций, что происходит каждые 10 минут. Блоки записываются в блокчейн в линейном последовательно-хронологическом порядке. На каждом полном узле — то есть компьютере, подключенном к сети биткойна с помощью клиента, выполняющего проверку и передачу транзакций, — хранится копия блокчейна, которая автоматически загружается, когда майнер присоединяется к биткойн-сети. В реестре сохраняется полная информация обо всех адресах и балансах, начиная с генезис-блока, то есть самого первого блока транзакций, до самого последнего добавленного блока.

Поскольку блокчейн представляет собой реестр, любое средство просмотра, например сайт <https://blockchain.info>, позволяет легко запросить транзакции, относящиеся к определенному биткойн-адресу. Так, например, в собственном электронном

* Фиатные (от лат. *fiat* — декрет, указание), они же фидуциарные (от лат. *fiducia* — доверие) деньги — деньги, номинальная стоимость которых устанавливается и гарантируется государством, традиционные деньги. — *Прим. ред.*

кошельке можно увидеть транзакцию, в которой вы получили свой первый биткойн.

Блокчейн-технология считается главной инновацией биткойна, потому что именно она служит «не требующим доверия» (*trustless*) механизмом верификации всех транзакций в сети. Принципиальное новшество блокчейна заключается в его архитектуре, обеспечивающей возможности децентрализованных транзакций, не требующих доверия. Вместо того чтобы устанавливать и поддерживать доверительные отношения с партнером по транзакции (другим человеком) или сторонним участником-посредником (например, банком), пользователи полагаются на общедоступную распределенную базу данных, хранимых на многих децентрализованных узлах и поддерживаемых «майнерами-бухгалтерами». Блокчейн позволяет избавиться от «доверенных посредников» и полностью децентрализовать транзакции произвольных типов между любыми участниками в глобальном масштабе.

Технически блокчейн-технология представляет собой еще один прикладной уровень, работающий поверх существующего стека интернет-протоколов. Она привносит в интернет совершенно новое звено поддержки экономических транзакций — как моментальных денежных платежей в универсальной криптовалюте, так и более сложных и долгоживущих финансовых контрактов.

В системе, похожей на блокчейн, могут совершаться транзакции с любыми валютами, финансовыми контрактами, материальными и нематериальными активами. Более того — блокчейн может применяться не только для транзакций, но и для фиксации, отслеживания, мониторинга и совершения операций с любыми активами. По сути, мы имеем дело с громадной электронной таблицей для регистрации всех активов и учетной системой для выполнения операций с ними в глобальном масштабе без ограничений по форме активов, типу участников или географическому положению.

Тем самым блокчейн может стать средством регистрации, учета и обмена любых финансовых, материальных (имущество) и нематериальных (права голосования, идеи, репутация, намерения, медицинские данные и другие) активов.

Связанный мир и блокчейн: пятая революционная парадигма вычислений

Одна из моделей познания современного мира основывается на парадигмах вычислений. Новая парадигма возникает примерно каждое десятилетие (рис. П-1). Сначала появились мейнфреймы*, затем персональные компьютеры (ПК), а следом нашу жизнь принципиально изменил интернет. Мобильные и социальные сети стали следующей — четвертой — парадигмой. Парадигмой для нынешнего десятилетия может стать *связанный мир вычислений* (*connected world of computing*), основанный на криптографии блокчейна.

Не исключено, что именно блокчейн-технологии предстоит стать верхним экономическим слоем органично связанного мира разнообразных вычислительных устройств, в числе которых — носимые вычислительные устройства, сенсоры «интернета вещей»**, смартфоны, планшеты, ноутбуки, цифровые

* Мейнфрейм (*англ.* mainframe) — большой универсальный высокопроизводительный отказоустойчивый компьютер со значительным объемом оперативной и внешней памяти, используемый для интенсивной обработки данных, как правило, крупными компаниями и государственными организациями. — *Прим. ред.*

** Интернет вещей (*англ.* Internet of Things, IoT) — концепция вычислительной сети физических объектов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой. Организация таких сетей рассматривается как явление, способное перестроить экономические и общественные процессы, с тем чтобы частично исключить участие человека. — *Прим. ред.*

устройства самофиксации (например, Fitbit*), умные дома, умные автомобили и умный город. Но реализуемая средствами блокчейна экономика поддерживает не просто движение денег, а перенос информации и эффективное размещение ресурсов, которые эти деньги обеспечивают в масштабах экономики отдельных людей и целых компаний.

Обладая революционным потенциалом, равным потенциалу интернета, блокчейн-технология будет разворачиваться и внедряться намного быстрее благодаря повсеместной доступности интернета и мобильной связи.

Функциональность социальных и мобильных сетей четвертой парадигмы стала настолько естественной, что пользователи теперь ожидают ее от всех технологий. Так, мобильные приложения поддерживают функционал, который раньше реализовывался через веб: отметка «нравится», комментирование, включение в друзья, участие в форумах. Точно так же блокчейн-технология, относящаяся к пятой парадигме, создает у пользователей ожидание, что обмен ценностями должен быть доступен повсеместно.

Функциональность, реализованная в рамках пятой парадигмы, может выглядеть как подключенный интегрированный физический уровень вычислений со многими устройствами, поверх которого находится слой для обслуживания платежей. Но речь идет не просто о платежах, а о микроплатежах, децентрализованной бирже, зарабатывании и трате токенов, получении и передаче цифровых активов, а также о составлении и выполнении умных контрактов — то есть о полноценном экономическом слое, которого в вебе до сих пор не было.

Мир уже готов к всеобщим деньгам, в основе которых лежит взаимодействие в интернете. Apple Pay (использующее

* Fitbit — лидер рынка фитнес-гаджетов, являющихся частью более широкой темы, так называемого «мобильного здоровья». — *Прим. ред.*

токены мобильного приложения электронного кошелька компании Apple) и конкурирующие продукты могут стать той поворотной точкой, с которой начнется мир полнофункциональных криптовалют. Блокчейн при этом становится неотъемлемым экономическим слоем веба.



Рисунок П-1. Революционные парадигмы вычислений: мейнфреймы, ПК, интернет, социальные и мобильные сети, блокчейн⁸

Сеть биткойн-платежей для поддержки машинной экономики: M2M/IoT

Блокчейн — революционная парадигма для «интернета людей», но она может также стать валютной основой «экономики машин». По оценкам компании Gartner, к 2020 году пространство «интернета вещей» будет насчитывать около 26 млрд устройств, а оборот интернет-экономики достигнет 1,9 трлн долларов⁹. Для управления транзакциями между этими устройствами потребуется «интернет денег»¹⁰ и соответствующая криптовалюта, а микроплатежи между подключенными устройствами могут развиваться в новый уровень экономики¹¹. По оценкам компании Cisco, количество M2M-подключений (*machine-to-machine*, то есть связь между машинами) растет быстрее любой другой категории, прибавляя по 84%. И дело не только в оценочном трехкратном росте глобального IP-трафика в период с 2012

по 2018 год, но и в изменении его характера: в сдвиге трафика в сторону передачи мобильных данных, Wi-Fi и M2M-соединений¹². Как товарно-денежная экономика обеспечивает более качественное, быстрое и эффективное распределение ресурсов на уровне человека, так и машинная экономика предоставляет надежную и децентрализованную систему управления теми же ресурсами, но на уровне машин.

В качестве примера микроплатежей между устройствами можно привести автомобиль, который автоматически согласует скоростное прохождение шоссе в экстренных случаях, компенсируя микроплатежами неудобство, доставленное другим участникам движения. Координация воздушной доставки товаров беспилотными летательными аппаратами — еще один пример сетей микроплатежей между устройствами, где нужна балансировка индивидуальных приоритетов. Сельскохозяйственные датчики — другой пример системы, в которой экономические принципы применяются для отсеивания фоновых малозначимых данных и повышения приоритета других данных, которые подтверждаются достаточно большой группой датчиков, развернутых на местности: например, определенные параметры окружающей среды, такие как уровень влажности.

Децентрализованная модель блокчейн-технологии, предусматривающая одноранговые, не требующие доверия транзакции, на самом базовом уровне означает, что для совершения транзакций не требуются посредники. Однако возможность реализации децентрализованной модели для всех видов взаимодействий (между людьми, между человеком и машиной, между машинами) в глобальном масштабе может требовать совершенно иных структур и способов функционирования общества. Направления таких изменений пока непонятны, но существующие властные отношения и иерархии могут в новых реалиях быстро утратить свое значение.

Повсеместное внедрение: доверие, удобство и простота использования

Идеи биткойна и блокчейна новы и технически трудны, поэтому бытует мнение, что криптовалюты слишком сложны для повсеместного внедрения среди обычных пользователей. А ведь то же самое когда-то говорили об интернете — но это не стало серьезным препятствием для его распространения: не надо понимать, как работает протокол TCP/IP, чтобы отправить сообщение по электронной почте.

На заре новых технологий рядовые пользователи всегда интересуются техническими подробностями: «что это?» и «как это работает?». Приложения, основанные на технологических новациях, легко находят путь к рядовым потребителям, если они способны предложить адекватный, удобный в использовании и дружелюбный интерфейс. В частности, пользователям не обязательно видеть, а тем более вводить вручную маловразумительные буквы и цифры 32-символьного биткойн-адреса. Компании, предлагающие «общедоступный кошелек», такие как Circle Internet Financial и Харо, разрабатывают пользовательские приложения, специально ориентированные на повсеместное использование биткойна, — разумеется, это делается для того, чтобы стать «Gmail от биткойна», то есть предоставить такое же удобство и завоевать такую же долю рынка, как общеизвестная почтовая служба.

Биткойн, как платежная система, и электронные кошельки оперируют хоть и электронными, но все же деньгами, поэтому приложения для конечных пользователей должны обеспечивать повышенную защиту транзакций. Поэтому, прежде чем удобные биткойн-кошельки завоеуют массовое признание, потребуется заслужить доверие потребителей. В частности, придется решить множество вопросов обеспечения безопасности криптовалюты, в том числе: «Как сохранять свои деньги?» или «Что делать

при утере закрытого ключа или при получении в транзакции сомнительной (то есть ранее украденной) монеты?».

Специалисты блокчейн-индустрии успешно работают над решением этих вопросов, что позволит альтернативным валютам стать новым этапом развития финансовых технологий, не менее значимым, чем появление банкоматов, банковского обслуживания через интернет и Apple Pay.

Приложения для работы с деньгами, обладающие доверительно-дружественным и удобным интерфейсом, уже близки к массовому внедрению. Но вот повсеместное принятие блокчейн-приложений, выходящих за пределы исключительно денежных отношений, может оказаться намного более трудным делом. Например, казалось бы очевидный вариант — услуги виртуальных нотариусов: их будет просто находить, и они позволят легко, недорого, безопасно, надежно регистрировать интеллектуальную собственность, договоры или завещания. Тем не менее существуют социальные причины, в силу которых люди все равно будут в ряде случаев обращаться к обычным нотариусам, чтобы получить человеческий совет (и немного психотерапии) или для того, чтобы подтвердить дееспособность человека, а это может тормозить распространение технологии.

Но в целом если отрасли биткойна и блокчейна суждено будущее, то, скорее всего, развитие будет происходить поэтапно — примерно так же, как развивался интернет, который в разное время начинал привлекать различные аудитории, «подключавшиеся» к сети по разным причинам. Изначально интернет решал задачу коллективного взаимодействия в четко определенных подгруппах: среди ученых и военных. Со временем в него пришли любители компьютерных игр и развлечений, а затем «подтянулись» и все остальные. Сейчас биткойн находится на этапе участия энтузиастов или ранних потребителей, используя термин модели Эверетта Роджерса — субкультуры людей, интересующихся деньгами и идеологией.

На следующем этапе блокчейн-технологии станут осваивать те социальные группы, для которых она сможет решать реальные практические проблемы, — например, люди из стран с введенной интернет-цензурой. Для них особое значение будет иметь существование децентрализованной системы доменных имен (DNS) на основе блокчейна. На рынке интеллектуальной собственности блокчейн-технологии можно задействовать для регистрации патентов, с ее помощью можно коренным образом изменить судопроизводство, связанное с интеллектуальной собственностью: управление объектами ИС, доступ к ним и установление их принадлежности.

Биткойн-культура: фестиваль Bitfilm

Один из индикаторов масштаба принятия новой технологии обычными людьми — ее след в массовой культуре. Возможно, фестиваль Bitfilm, в котором участвуют фильмы, посвященные биткойну, может стать первой ласточкой внедрения криптовалют в массовое сознание. Фильмы, отобранные для фестиваля, по-своему интерпретируют биткойн и рассказывают о его влиянии. Фестиваль впервые прошел в 2013 году и получил продолжение в конце 2014 — начале 2015 года в Берлине (где находится штаб-квартира Bitfilm), Сеуле, Буэнос-Айресе, Амстердаме, Рио-де-Жанейро и Кейптауне. Естественно, Bitfilm позволяет зрителям голосовать за понравившийся фильм биткойнами. Фестиваль продюсирует компания Bitfilm. Другое направление деятельности компании — создание роликов, рекламирующих блокчейн (рис. 2).

Цели, методология и структура этой книги

Отрасль блокчейн находится на начальной стадии развития — стадии бурного роста и инноваций. Принципы, терминология, стандарты, основные участники, нормы и отношение к тем или