

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)	83
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
Namesoip — 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>Monograph: 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: MOOC 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. Продвинутое 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

Блокчейн: фундамент для криптовалют (Блокчейн 1.0)

Стек технологий: блокчейн, протокол, валюта

Термин «биткойн» (Bitcoin) может ввести в заблуждение, поскольку биткойном принято считать три разные вещи.

Во-первых, биткойн — это базовая платформа блокчейн-технологии.

Во-вторых, биткойном называется работающий на основе этой базовой технологии протокол, описывающий, как именно происходит перевод активов в цепочке блоков.

В-третьих, биткойн — это цифровая криптовалюта, самая первая и самая популярная из известных на сегодня криптовалют.

В таблице 1-1 показано, чем различаются эти понятия. Нижний уровень — это базовая блокчейн-технология. Блокчейн как цепочка блоков транзакций — это распределенный, общедоступный и совместно используемый всеми узлами сети реестр или журнал записей, содержащий данные о транзакциях. Журнал обновляется майнерами и отслеживается всеми желающими, но при этом никем не контролируется. Он подобен

гигантской общедоступной таблице, которая периодически обновляется и подтверждает уникальность цифровых операций перевода денежных средств.

Средним уровнем стека является протокол — пакет программ, который переводит средства путем внесения транзакций в блокчейн (журнал записей). Наконец, третий уровень — это сама валюта под названием «биткойн», в транзакциях и на биржах используется обозначение *BTC* или *Btc*. Среди сотни криптовалют биткойн — не только самая первая, но и самая популярная. Среди прочих следует отметить Litecoin, Dogecoin, Ripple, NXT, и Peercoin. Перечень и котировки основных альткойнов можно найти на сайте <http://coinmarketcap.com/>.

Таблица 1-1. Уровни стека блокчейн-технологий на примере биткойна

Криптовалюта	Биткойн (BTC), Litecoin, Dogecoin
Биткойн-протокол и клиент	Программы, выполняющие операции
Блокчейн биткойна	Базовый децентрализованный журнал записей

Важно понимать, что общая структура любой современной криптовалютной системы формируется всеми тремя уровнями (блокчейн, протокол и валюта). Каждая монета представляет собой одновременно валюту и протокол, она может иметь собственный распределенный журнал записей или использовать распределенный блокчейн биткойна. Например, криптовалюта Litecoin использует Litecoin-протокол, работающий с блокчейном Litecoin, — по сути, это клон биткойна, в котором слегка изменены некоторые функции.

Отдельный блокчейн означает, что у монеты имеется собственный децентрализованный журнал записей с такой же структурой и форматом, что и распределенный журнал записей биткойна.

Другие протоколы, например Counterparty, имеют собственную валюту (ХСР), но используют блокчейн биткойна, то есть транзакции ХСР регистрируются в распределенном журнале записей биткойна. Таблицу с описанием характеристик проекта Crypto 2.0 можно найти по адресу: http://bit.ly/crypto_2_0_comp.

Двойное расходование и задача византийских генералов

Даже если оставить в стороне потенциал использования биткойна и блокчейн-технологии, биткойн, безусловно, является серьезным фундаментальным прорывом в области информатики — результатом 20 лет исследований в области цифровых валют и 40 лет исследований в области криптографии, над которыми работали тысячи ученых всего мира¹³. Биткойн стал решением давней проблемы цифровых наличных денег — проблемы двойного расходования (*double-spend problem*). До появления криптографии блокчейна цифровую наличность (*digital cash*)*, как и любой другой цифровой актив, можно было бесконечно копировать — как, например, мы можем сегодня бесчисленное количество раз копировать вложение в электронной почте. При этом без специального посредника невозможно было подтвердить, что та или иная партия денег не была уже израсходована ранее. Функцию посредника выполняла доверенная третья сторона: банк или платежная система вроде PayPal, которая хранила журнал записей, гарантирующий, что каждая единица

* Цифровая наличность (*англ.* digital cash) или электронная наличность (*англ.* e-cash, electronic cash) — термин, который в настоящее время широко используется в платежных системах. Название связано с возможностью совершать электронные платежи аналогично оплате обычными наличными: без обязательного посредничества третьего лица. Первые криптографические протоколы электронной наличности были предложены в 1983 году Дэвидом Чаумом и Стефаном Брэндсом. — *Прим. ред.*

цифровых денег может быть потрачена только один раз, тем самым предотвращая двойное расходование.

Проблема двойного расходования аналогична давно сформулированной математической проблеме — так называемой «Задаче византийских генералов»*, суть которой состоит в том, что несколько генералов перед сражением, не доверяя друг другу, должны как-то согласовать свои действия¹⁴.

Блокчейн решает проблему двойного расходования, объединяя технологию однорангового обмена файлами BitTorrent и шифрование с открытым ключом, тем самым создавая новый вид цифровых денег. Собственность на монеты регистрируется в открытом журнале записей и подтверждается криптографическими протоколами и сообществом майнеров. Блокчейн не требует доверия в том смысле, что в процессе транзакции пользователю нет нужды доверять контрагенту или посреднику. Необходимо лишь доверять системе — программной реализации блокчейн-протокола.

«Блоки» в блокчейне представляют собой группы транзакций, которые последовательно записываются в журнал учета транзакций, то есть «добавляются в цепочку». Распределенные журналы записей можно свободно просматривать с помощью браузеров блоков, размещенных на специализированных интернет-сайтах; например, для распределенного журнала записей биткойна — *www.blockchain.info*. Чтобы просмотреть поток транзакций пользователя, нужно ввести его биткойн-адрес, например *1DpZHXi5bEjNn6SriUKjh6wE4HwPFBPvfx*.

* В вычислительной технике под «Задачей византийских генералов» понимают мысленный эксперимент, призванный проиллюстрировать проблему синхронизации состояния систем в случае, когда коммуникации считаются надежными, а процессоры — нет. В криптологии — это задача взаимодействия нескольких удаленных абонентов, которые получили приказы из одного центра. Часть абонентов, включая центр, могут быть противниками. Нужно выработать единую стратегию действий, которая будет выигрышной для абонентов. — *Прим. ред.*

Как работает криптовалюта

Биткойн — это цифровые наличные деньги, с помощью которых можно покупать и продавать товары через интернет. Цепочка добавленной стоимости биткойна формируется несколькими группами: разработчиками, майнерами, биржами, сервисами обработки платежей, операторами интернет-кошельков и конечными пользователями/потребителями. Для начала работы с криптовалютой пользователю требуется лишь биткойн-адрес, секретный ключ и программа-кошелек. Биткойн-адрес — это идентификатор вроде номера счета, на который другие пользователи могут отправлять биткойны, а секретный ключ — это криптографический ключ, с помощью которого можно отправлять полученные биткойны другим пользователям. Для того чтобы оперировать биткойнами, программа-кошелек устанавливается на компьютере или смартфоне (см. рис. 1-1). При этом не нужно открывать никакого «расчетного счета» в какой-либо компании или банке — после установки программа автоматически генерирует связку из секретного ключа и биткойн-адреса, и вы можете сразу же



Рисунок 1-1. Приложение — электронный биткойн-кошелек и перевод биткойнов (изображение предоставлено разработчиками электронного биткойн-кошелька и InterAktyon)

распоряжаться средствами, привязанными к данному адресу. Кошелек может содержать копию блокчейна — записи всех транзакций, когда-либо выполненных с данной валютой. Это позволяет самостоятельно верифицировать любые транзакции в рамках децентрализованной системы Биткойн. Практические аспекты обслуживания альткойн-кошельков подробнее описаны в Приложении А.

Сервисы электронных кошельков и криптозащита персональных данных

Криптозащита персональных данных — это новая обширная область знаний. Проблема обеспечения защиты персональных финансовых активов и транзакций в блокчейне весьма актуальна.

Обычным потребителям незнакомы многие особенности блокчейн-технологии и криптозащиты персональных данных — например, необходимость создавать резервную копию кошелька. Сохранение секретного ключа в электронном кошельке на собственном компьютере дает полную финансовую независимость, но также означает невозможность обратиться в службу поддержки для «восстановления пароля». Потеря секретного ключа влечет за собой потерю биткойнов. В этом плане блокчейн-технология пока еще не готова к повсеместному использованию. Данную проблему пытаются решить ориентированные на пользователя биткойн-стартапы вроде Circle Internet Financial и Харо. Можно разработать стандартизированное приложение или сервис для создания резервных копий (например, если биткойн-кошелек был установлен на потерянных, украденных, вышедших из строя или обновленных смартфонах/ноутбуках/планшетах). Такой сервис помог бы пользователям управлять своими секретными ключами и их резервными копиями, чтобы они могли самостоятельно решить свою проблему или обратиться к сторонним специалистам.

Еще один элемент защиты персональных данных, который рекомендуют специалисты, — это *койн-миксинг* — «перемешивание» своих монет с транзакциями других пользователей для достижения максимальной конфиденциальности транзакций. Эту задачу решают такие сервисы, как Dark Coin, Dark Wallet и BitMixer¹⁵. По мере роста рынка альтернативных криптовалют будет также расти спрос на унифицированный электронный кошелек, который способен работать более чем с одной криптовалютой. Сегодня для большинства сервисов на основе блокчейна требуется установка отдельного кошелька, так что можно просто забить свой смартфон разнообразными электронными кошельками.

Несмотря на то что на сегодня реализация криптовалют громоздка и неэффективна, они обладают множеством важных преимуществ в области криптозащиты персональных данных. Вот одно из таких преимуществ — блокчейн представляет собой *push-технологию* (пользователь самостоятельно инициирует каждую транзакцию), а не *pull-технологию* (как в случае с кредитной картой или банком, когда персональные данные пользователя хранятся в файле и используются во время каждой авторизации). Когда создавались технологии кредитных карт, безопасность интернет-платежей вообще не стояла на повестке дня, в то время как при создании блокчейн-технологий она находится в центре внимания.

Pull-технологии не могут обойтись без централизованных хранилищ персональных данных, которые становятся все более уязвимыми для хакерских атак. Вот лишь некоторые из недавних примеров масштабных атак с целью хищения персональных данных, от которых пострадали миллионы пользователей: Target, ChaseBank и Dairy Queen. Возможность оплаты биткойнами услуг десятков тысяч торговцев, принимающих криптовалюту (например, Microsoft, Overstock, New Egg, и Dell Computer; см. <https://bitpay.com/directory#/>), означает, что