Оглавление

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 (XCP), но используют блокчейн биткойна, то есть транзакции XCP 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 мира[13]. 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 бессчетное 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 действия [14].

Блокчейн решает проблему двойного расходования, объединяя технологию одноранговой 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 InterAksyon)*

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 Xapo. 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 BitMixer[15]. 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 транзакции), 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