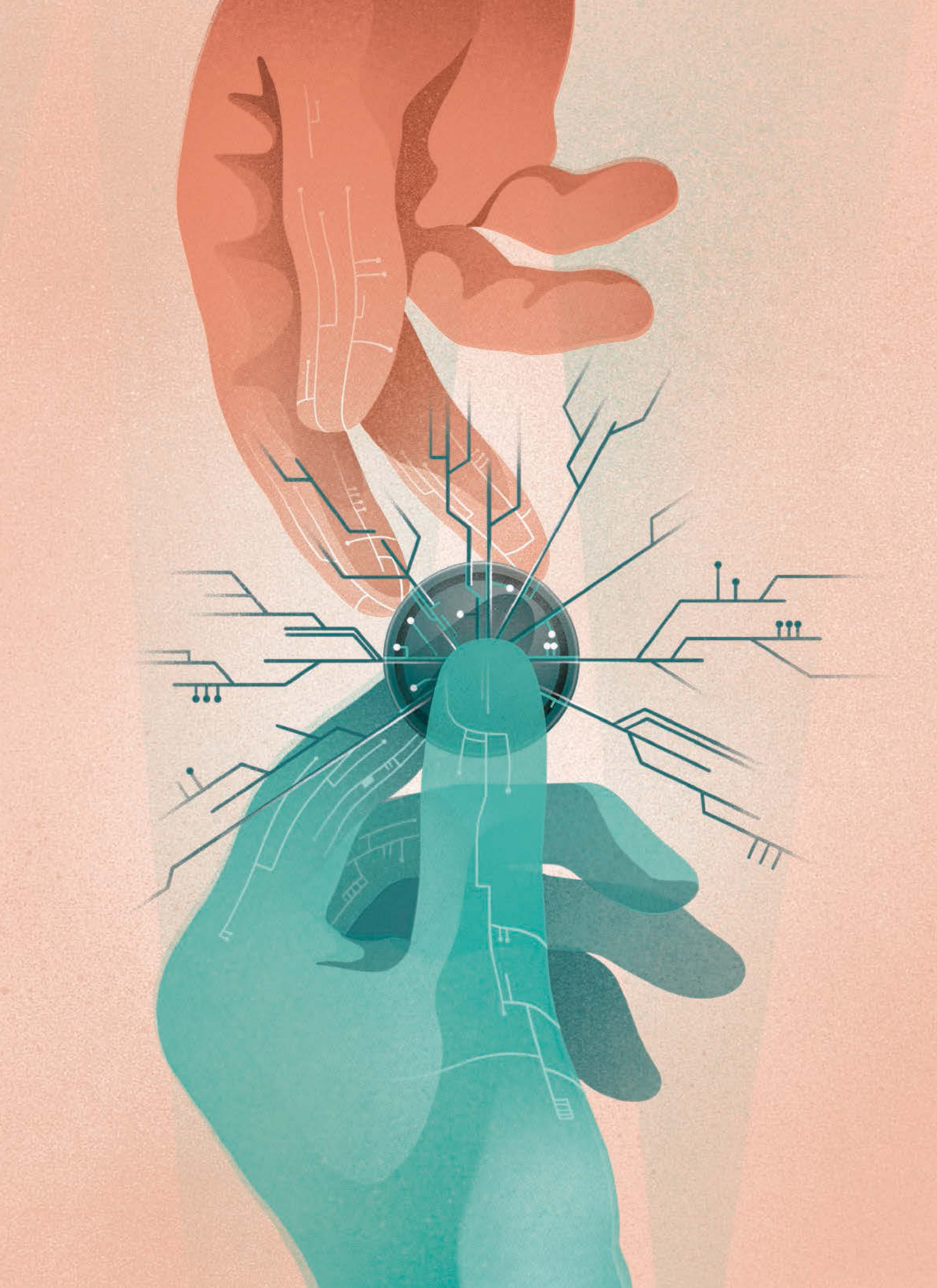


БУДУЩЕЕ ДЕНЕГ

СПЕЦИАЛЬНЫЙ РЕПОРТАЖ

Биткоин был только началом. Механизмы, обеспечивающие доверие без участия людей-посредников, могут исправить самые большие недостатки финансовых систем, но в то же время заставляют задуматься. Готовы ли мы к миру, в котором любой актив — от валюты до персональных данных — можно продать и отследить в нестираемом реестре? Вдруг технология, разработанная для того, чтобы лишить могущества банки и правительства, наоборот даст им беспрецедентный контроль?

Illustrations by Borja Bonaque

БУДУЩЕЕ ДЕНЕГ

СРЫВАЯ БАНК

НОВЫЕ ФИНАНСОВЫЕ СИСТЕМЫ МОГУТ ОСТАНОВИТЬ КОНЦЕНТРАЦИЮ БОГАТСТВА И УВЕЛИЧИТЬ УЧАСТИЕ ПРОСТЫХ ЛЮДЕЙ В ЭКОНОМИКЕ — НО ТОЛЬКО ПРИ ИСПОЛЬЗОВАНИИ С ОСТОРОЖНОСТЬЮ

АЛЕКСАНДР ЛИПТОН И АЛЕКС «СЭНДИ» ПЕНТЛЕНД

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Современная финансовая система стала угрожающе сложной. Увеличение прозрачности могло бы снизить риски, но для этого необходимо моделировать процесс денежного обращения с таким уровнем детализации, который недоступен существующей технологии.
- Новые технологии, такие как цифровые валюты, теперь позволяют имитировать каждую сделку и трансакцию. С помощью этих инструментов можно создать более эффективные финансовые сети и децентрализовать контроль над деньгами. Люди смогут обмениваться непосредственно друг с другом, не завися от банков.
- Радикальные перемены вполне возможны, но возникает и множество сомнений. Такие цифровые сети, если они правильно сконструированы и ответственно используются, только способствуют росту справедливости и ответственности. Но настолько же легко они могут привести и к крайней степени централизованного контроля.

ОБ АВТОРАХ

Александр Липтон (Alexander Lipton) — основатель и главный исполнительный директор лабораторий *StrongHold Labs* и член группы *Connection Science* в Массачусетском технологическом институте. Ранее он работал на руководящих постах в Банке Америки и одновременно был приглашенным профессором в Оксфордском университете и Королевском колледже Лондона. В 2000 г. он получил первую премию *Quant of the Year*.

Алекс «Сэнди» Пентленд (Alex "Sandy" Pentland)— профессор Массачусетского технологического института, член Национальной академии США, один из самых цитируемых авторов в сфере информатики. В 2011 г. журнал *Forbes* назвал его одним из семи самых влиятельных специалистов по данным. Его последняя книга — «Социальная физика» (*Social Physics*, 2015).

Это произошло более 5 тыс. лет назад. Одним весенним днем в городе-государстве Ур в Месопотамии чужеземный купец обменял свои товары на большой мешок серебра. Торговец не захотел везти серебро домой, так как знал, что вернется в Ур в конце сезона сбора урожая, чтобы купить зерно. Вместо этого он отправился в местный храм, где хранились ценности, и попросил жреца сохранить серебро.

Вскоре к жрецу обратился племянник и попросил денег взаймы. Молодой человек хотел купить семена, чтобы вырастить собственный урожай. Просьба растрогала жреца, и он одолжил племяннику немного серебра, рассудив, что возместит недостачу из собственных средств или займет у друзей, если юноше не удастся вернуть долг ко времени, когда серебро понадобится владельцу. Использовав долгосрочный договор с купцом-чужестранцем для выдачи краткосрочной ссуды племяннику, жрец удвоил количество коммерческих трансакций, используя дважды одни и те же деньги. Иными словами, он изобрел частичное банковское резервирование.

Из археологических данных мы знаем, что примерно так развивались события в Месопотамии, и это серьезно изменило финансовую среду в двух направлениях. Во-первых, увеличилась производительность труда, так как племянник теперь мог купить семена. Во-вторых, появился риск: юноша мог не вернуть деньги вовремя.

Несколькими тысячелетиями позже поддерживаемые государством центральные банки, появившиеся в Европе XVII в., соединили деятельность по «удваиванию расходов» с взиманием налогов. Короли занимали деньги у купцов, чтобы вести войны или строить дороги, а также платить оружейникам, поставщикам и войску. Деньги начинали циркулировать, стимулируя хозяйственную деятельность и принося прибыль, и на каждом этапе их количество увеличивалось вдвое или более. Короли обычно возвращали ссуды, взимая налог на прибыль. Так появилась модель денежного обращения, знаменующая начало современной банковской системы.

В упрощенном виде современное денежное обращение можно представить следующим образом: сначала фирмы берут кредиты в частных банках, таких как *JPMorgan Chase* или *HSBC*, для оплаты труда сотрудников и на другие расходы. На этом этапе создаются деньги. Затем потребители оплачивают товары, производимые фирмами, или депонируют деньги в банках в виде сбережений. И, наконец, фирмы используют полученные ими денежные средства для возврата долга банкам и цикл завершается. На этом этапе ссуженные деньги ликвидируются, но процент (процентные деньги) остается в системе навсегда. Так частные банки дают старт экономике, создавая деньги «из воздуха». Право банков на подобную деятельность частично регулируют центральные банки, устанавливающие предельные величины капитала и ликвидности, которыми должны обладать частные банки на постоянной основе, чтобы осуществлять операции по кредитованию.

Если бы все было так просто. К сожалению, в связи с обращением денег перед обществом встают фундаментальные проблемы. Во-первых, неизбежно появляется горстка миллиардеров, распоряжающихся основной частью мирового

богатства. Кроме того, удручающе часто деньги создаются с использованием заемных средств, но при этом риски оценивают недостаточно или не заботятся о них вообще. Вот так и случаются финансовые кризисы, такие как в 2008 г.: банкиры и политики подстегивали высокий спрос на ипотечные кредиты, который сопровождался интенсивным ростом объемов создаваемой денежной массы и еще более значительным увеличением рисков.

Может показаться очевидным, что причина возникающих сложностей — сам процесс денежного обращения. Однако корень проблемы не в этом. Создание денег за счет заемных средств оправданно, если оценивать присущие этому процессу риски и управлять ими, а одновременно пресекать сосредоточение богатства в одних руках. Тем не менее сегодня переплетение различных факторов, таких как быстрый рост численности населения, всемирная торговля и использование мощных компьютеров, делает систему слишком сложной для управления и регулирования, не говоря уже о понимании.

Еще больше тревожит, что преобладающая структура управления макроэкономической деятельностью опирается на устаревшие парадигмы. Например, в моделях, которые обычно используются для регулирования денежной эмиссии и процентных ставок, частные банки рассматриваются как простые посредники. При этом игнорируется тот факт, что сами по себе банки — это большое, активное и создающее деньги звено. У банков есть собственные интересы и стратегии, направленные на получение прибыли, с чем, в основном, и связана непрозрачность системы. Неудивительно, что ипотечный кризис 2008 г. было трудно предвидеть.

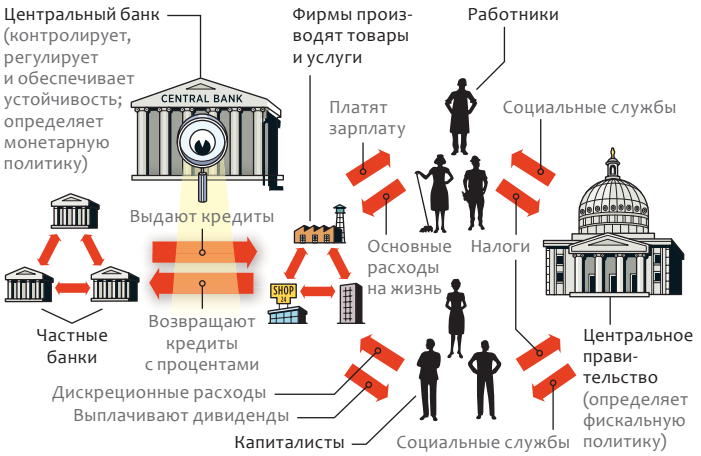
Чтобы по-настоящему понять современную сверхсложную систему денежного обращения, необходимо смоделировать ее в беспрецедентных деталях. Выполнению подобной колоссальной задачи долго препятствовали ограничения технологий. Но большие данные, а также появление цифровых валют и цифровых контрактов в конце концов изменят это. Вместо использования средних исторических показателей для оценки вероятных изменений в любой экономической системе наконец появится возможность

Три типа финансовых систем

Современное денежное обращение стало слишком сложным, чтобы в нем разобраться. Новые блокчейн-технологии, такие как составляющие основу сети *Bitcoin*, делают систему децентрализованной и более ясной. Разрабатываются новые сети.

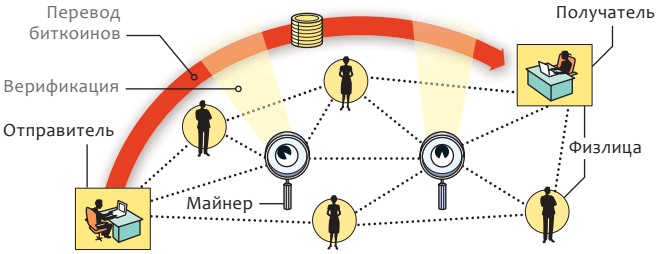
Частичное банковское резервирование (современное денежное обращение)

Банки создают деньги «из воздуха», когда выдают кредиты фирмам. Фирмы платят зарплату работникам и выплачивают дивиденды. Население покупает у фирм товары и услуги. Когда кредиты возвращают, «созданные» деньги ликвидируются, но процент остается в системе постоянно.



Пиринговая сеть *Bitcoin*

Трансакции совершаются между пользователями, без посредников. Они транслируются публично и записываются в блокчейне. Согласование обеспечивают случайные валидаторы. Биткоин не имеет стоимости, поэтому его цена от природы нестабильна.



Пиринговая сеть *Tradecoin*

Как и в сети *Bitcoin*, трансакции совершаются между пользователями напрямую и открыто записываются в блокчейне. Но согласование обеспечивают назначенные валидаторы. Ценность трейдкоина обеспечена спонсорскими активами, так что его цена относительно стабильна.

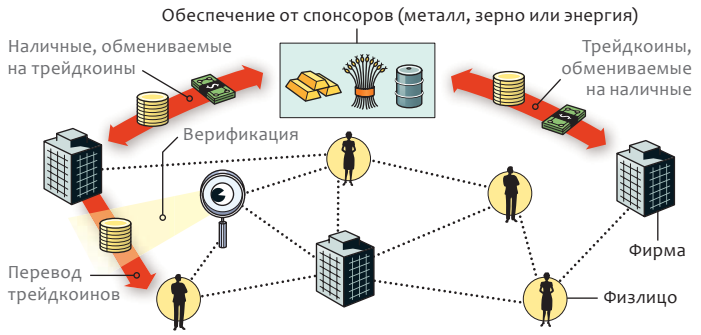


Illustration by Peter and Maria Hoey

полностью сымитировать каждую отдельную сделку и трансакцию и проанализировать все потенциальные результаты. В перспективе это достижение основательно изменит функциональность и идеологию глобальной финансовой системы и повысит — или понизит — экономическую безопасность.

Появление цифровых валют

Новые технологии, позволяющие перестроить нашу финансовую систему, начали бурно развиваться только в последние десять лет. Почти все слышали о биткоине, но это лишь часть многообещающей индустрии финансовых технологий, вокруг которой много суеты и спекуляций. Что важно знать: ключевое изобретение — распределенный реестр — это база данных, к которой имеют доступ и которой управляют множество пользователей. Именно эта технология сделала возможным появление криптовалют — цифровых валют, защищенных шифрованием, таких как биткоин. Составляющая основу этой технологии структура данных называется «блокчейн» (*blockchain*, «цепочка блоков») и представляет собой серию последовательно зашифрованных блоков. Для надежности и безопасности блоки согласованно обновляются посредством различных проверочных механизмов с участием людей и компьютеров.

Сами принципы блокчейна и распределенных реестров не новы: блокчейн, например, обычно задействован при переходе власти, земли или иной собственности из рук в руки. Новшество заключается в одновременной реализации двух концепций в защищенной от взлома компьютерной системе, которая применима для решения различных практических задач. Новые технологии распределенных реестров на базе блокчейнов позволяют создавать цифровые валюты, гораздо более эффективные, чем американский доллар, и даже более эффективные, чем биткоин.

Такие инструменты дают возможность осуществлять мониторинг и анализ трансакций на мельчайшем уровне, поэтому наконец можно разобраться в денежном обращении. Имея четкое представление о происходящем, мы научимся распознавать предупредительные сигналы среди триллионов записанных в реестре трансакций и поступать соответствующим образом, чтобы повысить стабильность и безопасность системы. Подобный мониторинг в режиме реального времени представляет собой более надежный механизм и в рамках общества в целом. Во время финансового кризиса 2008 г. бюрократических возможностей не хватало, чтобы заниматься персональным ущербом, причиненным десяткам миллионов человек. В результате регуляторы сосредоточились на помощи небольшой группе крупных банков, оставив в стороне обычных людей, которые пострадали больше всего.

Краткая история денег

VII в. до н.э.
В Лидии начали чеканку стандартных монет.

XIV в.
Торговые банки, такие как принадлежавшие семейству Медичи, расширяют участие в международных финансах, торговле и производстве.

XVII в.
Выдавая ссуды из депонированных денежных средств, банки стимулировали экономику, одновременно создавая новые источники риска, которые постоянно приводят к местным кризисам и даже всеобщим депрессиям. Появляются центральные банки, совмещающие банковскую деятельность с взиманием налогов.

XVIII в.
В результате развития существовавшей ранее системы, когда циркулировавшие деньги слабо регулировались резервами драгоценных металлов, появляется золотой стандарт. Это снижает риск.

XX в.
Золотой стандарт замещается Базельскими соглашениями, в которых говорится, что владение высоколиквидными (легко продаваемыми) активами практически равноценно владению золотом.

По мере того как расширяется область применения этой быстро развивающейся технологии, путаница растет. Поскольку в настоящее время биткоин — самый известный (некоторые сказали бы: печально известный) вид цифровой валюты, вернемся немного назад, чтобы изучить его происхождение и недостатки и понять, чем он отличается от других более перспективных современных криптовалют. Система *Bitcoin* — это пиринговая *(peer-to-peer)* электронная платежная система, работающая без центрального органа *(для расчетов используется одноименная криптовалюта — биткоин. — Примеч. пер.)*. К системе может присоединиться любой желающий, что можно рассматривать одновременно и как сильную, и как слабую сторону. Пользователи совершают финансовые трансакции напрямую, без участия посредников. Эти трансакции записываются в публичном распределенном реестре на базе блокчейна и теоретически видны всем участникам. Со времени появления в 2009 г. цена биткоина возросла на несколько порядков, превратив его в любимую криптовалюту спекулянтов.

Потенциал биткоина огромен. Сторонники биткоина — в основном технически подкованные идеалисты и либертарианцы, но также и некоторые преступники — ожидают, что он станет мировой валютой и в конечном итоге вытеснит национальные валюты, которыми, по их мнению, легко манипулировать. Некоторые энтузиасты даже полагают, что биткоин — это электронная версия золота, вероятно, забыв, что стабильность золота обеспечивается как его физическими свойствами, так и миллиардами заинтересованных лиц и что в цифровом мире обычно на смену хорошим технологиям приходят совершенные.

Система создавалась таким образом, чтобы полномочия распределялись между множеством майнеров, но за счет слияния в гигантские пулы малое число групп стало достаточно могущественным, чтобы контролировать всю систему *Bitcoin*

На самом деле биткоин — это не первая и, скорее всего, не последняя крупная цифровая валюта. Кроме того, существуют также серьезные логистические ограничения. Например, в системе *Bitcoin* в секунду обрабатывается примерно семь трансакций, тогда как среднее число обрабатываемых трансакций *Visa* за то же время — 2 тыс. Помимо прочего, майнинг — процесс, с помощью которого узлы сети криптовалюты конкурируют, чтобы безопасно добавлять новые трансакции в блокчейн, — связан с потреблением огромного количества электроэнергии. В странах с дорогой электроэнергией майнеры могут разориться на платежах за электричество для вычислительных мощностей. Хотя точная цифра неизвестна, полагают, что *Bitcoin* потребляет столько же электроэнергии, сколько *eBay, Facebook* и *Google* вместе взятые. Кроме того, система создавалась таким образом, чтобы полномочия распределялись между множеством майнеров, но за счет слияния в гигантские пулы малое число групп стало достаточно могущественным, чтобы контролировать всю систему *Bitcoin*. Вот вам и технология *peer-to-peer*!

Использование биткоина также ограничено. Сущность денег определяется характером их использования (функции денег): для осуществления сделок (как средства платежа), как средства накопления и как счетной единицы. Поскольку в отличие от доллара США (и других определяемых правительством законных платежных средств) цена биткоина крайне нестабильна, его трудно использовать на повседневной основе. Криптовалюты биткоин и эфир (еще одна основная цифровая валюта) не обеспечены реальными активами или даже обязательствами правительства, следовательно, они имеют исключительно спекулятивный характер. Проще говоря, это ненастоящие деньги: цена того, что не имеет стоимости, может быть какой угодно. Некоторые энтузиасты рассматривают отсутствие реальной стоимости у биткоина как его достоинство и заявляют, что в будущем все деньги станут подобными биткоину. Это маловероятно как по техническим, так и по политическим причинам.

Тем не менее биткоин как первая успешная децентрализованная цифровая валюта — это впечатляющий прорыв. Передовая технология и главные принципы нерегулируемой пиринговой финансовой системы, положенные в основу биткоина, предлагают практические решения серьезных проблем. Конечно, это только один из вариантов применения распределенных реестров на базе блокчейна. Все-таки блокчейн — это технология, а не особая идеология, и не стоит ее связывать с доктриной биткоина или мотивами, по которым технология применяется или будет применяться. Наряду с возможностью решить существующие проблемы нашей финансовой системы эта

технология также может и усугубить их. Если же принять во внимание, что контроль над деньгами (а именно над созданием как существующих, так и будущих денег) — это ключевой элемент власти, то уже сейчас можно увидеть, какие субъективные риски таил ящик Пандоры, открытый данной технологией.

Рассмотрим ситуацию с центральными банками основных резервных валют, такими как Федеральная резервная система США (ФРС США) и Банк Англии. Часто доверие к финансовой организации связано с ее размерами — чем крупнее, тем большего доверия заслуживает, однако эти игроки доказали, что такой подход — серьезное заблуждение. ФРС США и Банк Англии то и дело выбирают способы сделать простых людей еще беднее: понижая стоимость собственных финансовых обязательств за счет инфляции, сдерживая процентные ставки и т.п. Недавно они начали тестировать отрицательные процентные ставки и рассматривать вопрос об отказе от наличных денег.

Еще больше тревожит, что некоторые центральные банки обсуждают возможности перевода всей валюты в электронную и учета покупок непосредственно в реестре. Это может привести к исключению частных банков из процесса и дать правительству абсолютный контроль над экономикой. Это означает также, что у правительства будут данные обо всем, что вы покупаете, в том числе и о том, что вы намеренно, чтобы не оставлять документальных следов, оплатили наличными. Вероятность подобного развития событий все возрастает, а такие страны, как Китай, Великобритания, Сингапур и Швеция, уже объявили о наличии планов по изучению и потенциальному воплощению такой стратегии. Отсюда напрашивается вывод: несмотря на то что сама технология умышленно децентрализована, ее можно использовать для создания централизованно управляемых систем.

Криптовалюты следующего поколения, такие как трейдкоин, могут значительно уменьшить помехи в системе мировой торговли, даже среди хаоса в современных политике и экономике. В итоге господство основных валют, таких как доллар, может ослабнуть и финансовая система США могла бы стать более эффективной

К более стабильной финансовой системе

Разумеется, изобретение блокчейна и распределенного реестра не искоренит такие проблемы, как финансовые кризисы и нездоровая инфляция (по крайней мере, в ближайшем будущем), но оно способствует появлению законной альтернативы крупным и могущественным игрокам. Технология позволяет формировать специализированные системы мировых валют, которые до этого не обладали достаточными масштабами, надежностью или политической стабильностью, чтобы стать конкурентоспособными. Вот почему на следующем этапе естественным будет объединение не обладающих богатством развивающихся экономических систем или большого числа отдельных граждан для формирования альтернативы центральным банкам.

Имея в виду такую возможность, наша лаборатория в Массачусетском технологическом институте работает над созданием электронной валюты, пригодной для широкомасштабного использования в деловых операциях. Валюта под названием трейдкоин будет нестираемо регистрироваться в блокчейне и всегда будет привязана к корзине базовых активов, таких как зерно, электроэнергия или полезные ископаемые, что позволит стабилизировать ее стоимость и повысить доверие общества. Ключевая идея в том, что для широко используемой валюты необходимы как доверие людей, так и эффективные торговые системы.

Цифровой трейдкоин на базе распределенного реестра позволит альянсам малых государств, предприятий, коммерсантов, кредитных союзов и даже фермеров сформировать активы, достаточные для обеспечения крупной ликвидной валюты, которая потенциально станет такой же надежной или по крайней мере такой же эффективной, как национальные валюты, используемые Всемирным банком и Международным валютным фондом. Таким образом, члены альянса трейдкоина будут в какой-то степени защищены от эгоистической политики крупных игроков. Криптографическая структура позволяет намного легче, безопаснее и дешевле стать участником международной торговли. Если члены альянса географически и политически разделены, то они больше защищены от рисков дефолта, чем если бы за их

спиной стояло единственное большое сообщество. Именно так и появился в 1694 г. Банк Англии — как торговый альянс.

Принципы, лежащие в основе трейдкоина, фундаментально отличаются от принципов криптовалют, подобных биткоину, которые не обеспечены реальными активами и не задействуют альянсы. В сети трейдкоина за счет использования заранее одобренной сети различных доверенных «валидаторов» также исключен энергоемкий процесс майнинга. Участники могут выбирать серию выполняющих валидацию узлов сети, различающихся настолько, что никто не сможет подкупить 51% валидаторов сразу. В результате получается быстрый, полностью масштабируемый, надежный и экологически чистый финансовый инструмент. В нем сочетаются самые современные технологии с очень старой идеей золотых монет, которые имеют подлинную ценность и поэтому пользуются достаточным доверием, чтобы применять их далеко от места происхождения.

Такие валюты, как трейдкоин, могут стать даже более безопасными, чем используемые сегодня, поскольку их можно разрабатывать таким образом, что детали денежного обращения становятся очевидными для осуществления надзора. Надзор со стороны заинтересованных сторон до сих пор необходим, подобно тому как Корпорация по управлению доменными именами и *IP*-адресами *(ICANN)* контролирует интернет или регуляторы, такие как Совет управляющих Федеральной резервной системы, осуществляют надзор за банковской системой США. Надзорные органы будут учитывать простую отчетность, ведущуюся в распределенном реестре, поэтому мы сможем более надежно моделировать и предсказывать риски. В настоящее время такая прозрачность невозможна, потому что доступ к деталям финансовых трансакций и контрактов ограничен. Однако если бы такая система существовала в 2008 г., то она бы зафиксировала экстремальную концентрацию некоторых трейдеров вокруг производных ценных бумаг, обеспеченных ипотечными ценными бумагами, и смоделировала в деталях последствия изменения стоимости жилья. Тогда на месте скрытых комплексов безнадежных ипотечных сделок были бы яркие красные флажки.

Мы приняли вызов, связанный с необходимостью повышения прозрачности. Например, мы разрабатываем в качестве пилотных системы программного обеспечения «доверенной сети» для финансовых компаний Евросоюза и США. Они позволят записывать и «проигрывать» трансакции и контракты между разными сторонами, не раскрывая информацию и не нарушая конфиденциальность. Это программное обеспечение также служит основой для трейдкоина. Мы изучаем возможность пилотного запуска двух типов валюты трейдкоин: первый предназначен для международной торговли и обеспечивается альянсом малых государств, а второй обеспечивается фермерами для использования на товарных рынках. Сейчас мы ведем набор членов альянса для апробации идеи.

Поразительно, что впервые появится мировая цифровая валюта, в значительной степени устойчивая к эгоистичной политике богатых центральных банков, контролирующих большую часть денег. Несомненно, в ближайшее время вероятно появление целого ряда новых альтернатив, и некоторые смогут подняться настолько, чтобы конкурировать с крупнейшими резервными валютами. Появление возможности разработать полностью понятные денежные системы означает, что мы способны в перспективе создать инструменты для минимизации рисков, недопущения кризисов и обеспечения свободы от вмешательства правительств и чрезмерно могущественных корпораций. Поскольку такая валюта будет конвертируемой и обеспеченной обычными активами, у нее будет реальная начальная стоимость. Это значит, что подобные валюты менее подвержены спекулятивным атакам и будут устойчивы к политическим манипуляциям и инфляции, вызванной проблемами одного государства.

Криптовалюты следующего поколения, такие как трейдкоин, могут значительно уменьшить помехи в системе мировой торговли, даже среди хаоса в современных политике и экономике. В итоге господство основных валют, таких как доллар, может ослабнуть и финансовая система США могла бы стать более эффективной. Существует надежда, что такие распределенные системы, обеспеченные широкими коалициями различных игроков, принесут миру бóльшие открытость, ответственность и справедливость.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ

- The Macroeconomics of Central Bank Issued Digital Currencies. John Barrdear and Michael Kumhof. Staff Working Paper No. 605. Bank of England, July 2016.
- Modern Monetary Circuit Theory, Stability of Interconnected Banking Network, and Balance Sheet Optimization for Individual Banks. Alexander Lipton in International Journal of Theoretical and Applied Finance, Vol. 19, No. 6, Article No. 1650034, September 2016.
- Trust::Data: A New Framework for Identity and Data Sharing. Edited by Thomas Hardjono, David Shrier and Alex Pentland. Visionary Future, 2016.

БУДУЩЕЕ ДЕНЕГ

МИР, СОЗДАННЫЙ БИТКОИНОМ

ПЕРВАЯ КРУПНАЯ ЦИФРОВАЯ ВАЛЮТА ПОЗВОЛИЛА НАМ УВИДЕТЬ НОВЫЙ ФИНАНСОВЫЙ ПОРЯДОК, КОТОРЫЙ СКОРЕЕ СТАВИТ ВОПРОСЫ, ЧЕМ ДАЕТ ОТВЕТЫ

ДЖОН ПАВЛУС

ОБ АВТОРЕ

Джон Павлус (John Pavlus) — писатель и кинематографист, в сферу интересов которого входят вопросы науки и техники. Его статьи публиковались в журналах *Bloomberg Businessweek*, *MIT Technology Review* и в сборниках *The Best American Science and Nature Writing*. Живет в Портленде, штат Орегон.

Биткоин, криптовалюты, смарт-контракты. Сегодня уже многие наслышаны о быстро меняющейся экосистеме финансовых технологий. Сотни центральных банков поддерживают развитие новаторской технологии блокчейн, а инвесторы вкладывают в нее миллиарды. Тем не менее, согласно результатам опроса, проведенного в 2017 г. компанией *PricewaterhouseCoopers (PwC)*, только 24% специалистов в сфере мировых финансовых услуг указали, что они «очень хорошо» или «хорошо» знакомы с этой технологией. Большинство обычных людей даже если и разбираются в этой технологии, то не уверены, законно ли ее использование. Ярые сторонники блокчейна утверждают, что он способен перевернуть всю экономическую систему. Другие, такие как исследователь блокчейна из Корнеллского университета Эмин Гюн Сирер (Emin Gün Sirer), предупреждают, что в то время как техническая сторона блокчейна «удивительная и прорывная, много всякой чепухи вокруг». Как разобраться в нюансах и в том, что такое блокчейн?

Все началось с Сатоши Накамото (Satoshi Nakamoto) — миллиардера-отшельника *(или, возможно, группы лиц. — Примеч. пер.)* с вымышленным именем. В октябре 2008 г. через скрытый список интернет-рассылки Накамото опубликовал статью, в которой описал подробности проекта первого в мире блокчейна — публичной базы данных, распределенной на тысячах компьютерах и синхронизируемой ими в течение каждых десяти минут, доступной каждому и при этом полностью защищенной от взлома. Цель проекта — обеспечить децентрализованный, «непробиваемый» протокол для новой цифровой валюты, которую Накамото назвал «биткоин».

До того момента основная проблема, связанная с пиринговой электронной наличностью, была в том, что никто не мог надежно предотвратить использование такой наличности дважды. Блокчейн-технология все изменила, так как каждый перевод биткоинов записывался в распределенном реестре — своего рода электронной таблице, которая благодаря законам математики и шифрования нерушима и даже более надежна, чем, например, высеченная в камне. Журнал *The Economist* прозвал ее «машиной доверия».

Технология, ставшая основой биткоина, быстро его переросла и превратилась в движущую силу неистового периода инноваций. Блокчейн можно рассматривать как основу для хранения любых данных, для которых требуется надежный источник: финансовых историй, документов о собственности, документов, удостоверяющих личность. Этот «глобальный регистр», как называет его Дон Тапскотт (Don Tapscott), соавтор книги «Технология блокчейн. То, что движет финансовой революцией сегодня» *(Blockchain Revolution)*, — чистая доска. Но, как любая несовершенная технология, блокчейн может использоваться и во зло, поэтому некоторые неистово «бьют по тормозам». Далее представлен путеводитель по цифровому ландшафту, навязанному нам Сатоши Накамото (кем бы он ни был).

Illustrations by Peter and Maria Hoey

Основные понятия

КРИПТОВАЛЮТА — цифровая валюта, основанная на математических алгоритмах шифрования, которые используются для контроля над способом и временем создания валютных единиц и для обеспечения безопасного перевода платежей.

ПИРИНГОВАЯ СЕТЬ *(peer-to-peer (P2P) network)* — децентрализованная сеть компьютеров, то есть такая, в которой любые компьютеры могут взаимодействовать друг с другом напрямую, без участия центрального сервера или другого администратора. Идея стала популярной после запуска в конце 1990-х гг. сети *Napster* для обмена музыкальными файлами.

УЗЕЛ СЕТИ — компьютер, подсоединенный к *P2P*-сети. В настоящее время к сети *Bitcoin* подключены тысячи компьютеров по всему миру.

РАСПРЕДЕЛЕННЫЙ РЕЕСТР — реестр зарегистрированных с временными метками трансакций, который одновременно распространяется, копируется и верифицируется посредством согласования множеством разных компьютеров в *P2P*-сети. Если каждый узел сети имеет идентичную копию реестра, то фальсифицированные записи или искаженные версии легко обнаружить.

БЛОК — группа записей об отдельных трансакциях в блокчейне. В сети *Bitcoin* новые блоки добавляются к цепочке каждые десять минут.

ХЕШИРОВАНИЕ — криптографический метод, в котором используется математическая функция для преобразования любого объема данных в уникальную строку буквенно-цифровых символов фиксированной длины — значение хеш-функции. Таким образом, создается легко проверяемый цифровой отпечаток хешированных данных. Даже если единственный бит исходных данных изменить или исказить, то отпечаток в хеш-функции будет радикально отличаться, поэтому легко обнаружить ошибки или подделку. Хеш (результат хеширования) имеет одностороннюю направленность: из отпечатка нельзя воссоздать или извлечь исходные данные.

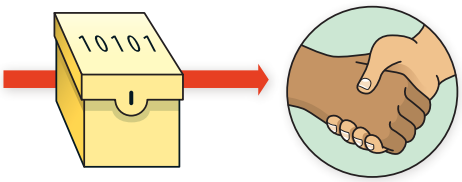
МАЙНИНГ — процесс, посредством которого узлы сети криптовалюты конкурируют за право безопасно добавить блоки трансакций в блокчейн. Валютные единицы служат вознаграждением и, следовательно, материальным стимулом для обеспечения безопасности. Майнинг включает загрузку последней версии трансакций блокчейна для верификации и последующее использование метода прямого перебора для случайного поиска решения сложного математического пазла, созданного посредством хеширования. Первый узел сети, решивший задачу, «добывает» этот блок, добавляя его к блокчейну, и требует полагающееся вознаграждение. Узлы сети контролируют люди, но соревнование не имеет ничего общего с мастерством: просто чем больше чистая вычислительная мощность, которую задействует майнер, тем больше вероятность найти решение — процесс, который называется доказательством выполнения работы *(proof of work)*.

Как работает блокчейн

Как цифровая валюта или любые данные надежно передаются в децентрализованнй сети, полной незнакомцев, у которых вообще нет оснований доверять друг другу? За счет генерации постоянного реестра трансакций, который ни один участник сети не может изменить.

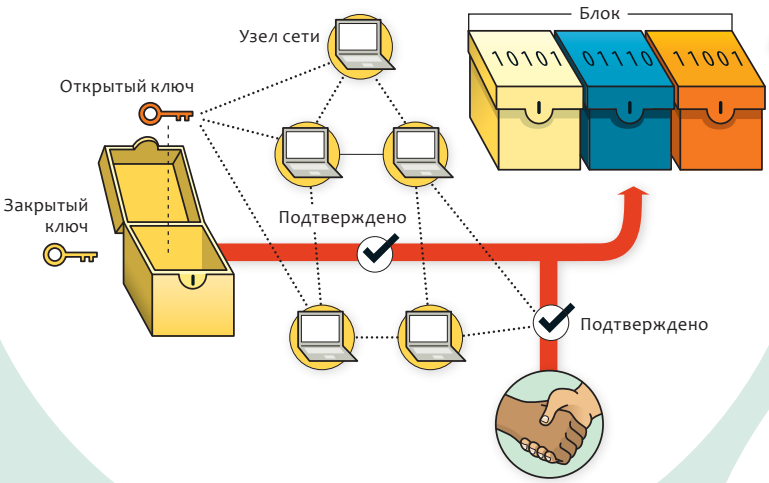
1

Трансакция в блокчейне начинается, когда одна из сторон соглашается отправить данные другой стороне. Данные могут быть разными, но поскольку суть блокчейна — создание неизменяемой, поддающейся проверке записи об обмене, обычно данные представляют какой-нибудь ценный актив. Наиболее часто передаются единицы криптовалюты или другие финансовые инструменты, контракты, документы или записи о праве собственности, медицинская информация или другие персональные данные.



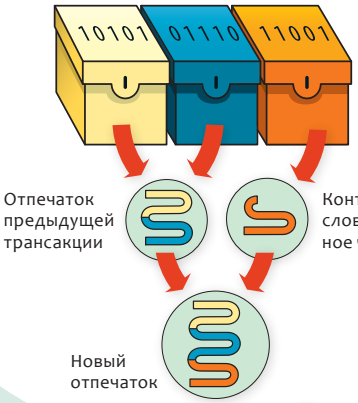
2

Трансакция транслируется для верификации в пиринговой сети компьютеров, управляющей блокчейном. Каждый узел сети имеет в распоряжении процедуру для подтверждения подлинности трансакции. (В трансакциях биткоинов, например, сеть проверяет, действительно ли осуществляющие платеж обладают заявленным количеством биткоинов.) Когда сеть приходит к согласию, алгоритмы «упаковывают» подтвержденную трансакцию вместе с другими недавно подтвержденными трансакциями в блок.



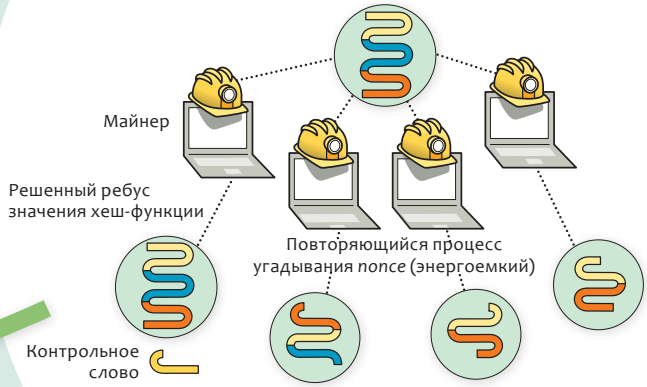
3

Программа создает «отпечаток» для нового блока посредством хеширования содержащихся в блоке данных вместе с двумя другими элементами информации: отпечатком предшествующего блока и непредсказуемого случайного числа, называемого *nonce (ключ, используемый только один раз в криптографически защищенной связи. — Примеч. пер.).*



4

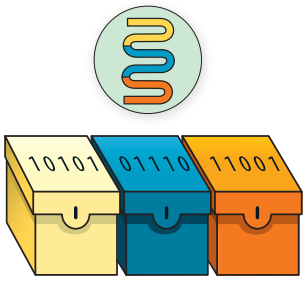
Специальные узлы сети (майнеры) начинают соревноваться друг с другом за право добавить новый блок к блокчейну. Их компьютеры методом проб и ошибок снова и снова выполняют утомительный комплекс вычислений, связанных с хешем, пытаясь сгенерировать решение, удовлетворяющее произвольному правилу, определенному сетью. (В блокчейне сети *Bitcoin* майнеры ищут решения — значения хеш-функции, — которые начинаются с определенного количества нулей.) Тот, кто первым завершит этот процесс доказательства выполнения работы и найдет математическое решение, успешно «добывает» этот блок, получая финансовое вознаграждение.



В КАЧЕСТВЕ АЛЬТЕРНАТИВЫ. Доказательство выполнения работы — энергоемкий процесс, поэтому в некоторых новых блокчейнах вместо этого используется сеть предварительно одобренных узлов-«валидаторов», которые удостоверяют трансакции через альтернативный процесс — подтверждение доли. Поскольку этот процесс не опирается на сложные вычисления хеша, требуется намного меньше вычислительной мощности (и намного меньше электричества).

5

Подтвержденный блок добавляется в блокчейн с цифровым отпечатком, в котором также математически закодированы подтвержденные отпечатки всех предшествующих блоков. Такие вложенные отпечатки с добавлением каждого нового блока усиливают безопасность блокчейна, потому что изменение даже одного бита информации на любом участке блокчейна радикально меняет отпечаток не только одного блока, но и каждого последующего в цепи.



О БЛОКЧЕЙНЕ ПРОСТЫМИ СЛОВАМИ:
ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

1

БИТКОИН И БЛОКЧЕЙН — ЭТО ОДНО И ТО ЖЕ?

Нет, но их легко перепутать, так как и о том и о другом стало известно в 2008 г., когда Сатоши Накамото опубликовал статью, описывающую, как совместно реализовать две концепции. Биткоин — это один из видов криптовалюты. То, что называется «блокчейн», представляет собой технологию, благодаря которой возможно существование биткоина: это инфраструктура, которую можно использовать для отслеживания разного вида трансакций. Технология блокчейн существует без биткоина, но не наоборот. Биткоин можно рассматривать как вид программы, работающей в блокчейне, наподобие веб-сайтов, работающих в интернете.

2

ОТКУДА ПОЯВЛЯЕТСЯ ЦЕННОСТЬ КРИПТОВАЛЮТЫ?

Одни эксперты полагают, что такая криптовалюта, как биткоин, имеет ценность из-за ее безопасности (блокчейн биткоина никогда не взламывали — пока) или из-за математически заданного «дефицита» (фиксированное предложение 21 млн биткоинов означает, что они никогда не обесценятся за счет печатания новых денег). Другие считают, что биткоину присуща внутренняя стоимость, так как майнинг — это утомительная работа, делающая сеть сильнее, то есть, иными словами, ценность заключается в объеме работ. А что насчет криптовалют, где майнинг не требуется? По мнению Кристиана Каталини (Christian Catalini) из Массачусетского технологического института, «ценность появляется из договоренности. Мы все соглашаемся, что криптовалюта имеет ценность». С этой точки зрения у криптовалют больше общего с социальными сетями, чем с центральными банками. «Деньги — это средство, с помощью которого общество следит за системой сдерживания и уравновешивания, — говорит Каталини. — Если криптовалюты станут более удобным средством отслеживания информации, то их ценность гарантирована независимо от того, представляют ли они физические активы или просто числа».

3

БЛОКЧЕЙН — ЭТО НОВЫЙ ВИД ИНТЕРНЕТА?

Не совсем так, поскольку блокчейну требуется интернет для поддержки и управления пиринговой сетью. Необходимо также отметить, что когда в быту говорят о блокчейне, почти всегда имеют в виду специальную систему, внедренную Накамото как средство обеспечения биткоина. Биткоин-блокчейн стал первой системой распределенного реестра, не нуждающейся в центральном сервере или организации для обеспечения работы. И он остается одним из самых больших: на ноябрь 2017 г. в биткоин-блокчейне содержалось более 130 Гб (140 млрд байт) информации, и с каждой новой трансакцией его размер увеличивается. Но это количество информации все же не сравнится с объемом данных в интернете, который измеряется иоттабайтами (10^{24}, или септиллионы байт).

4

БЛОКЧЕЙН — ЭТО ЗАКОННО?

Да. Но децентрализованный характер и ассоциация с биткоином, который используется и в незаконных трансакциях, таких как продажа оружия и наркотиков, создают блокчейнам незаслуженную репутацию «вне закона». Блокчейны можно использовать для разных целей, плохих или хороших, так же как *Facebook*, электронную почту или другие интернет-технологии.

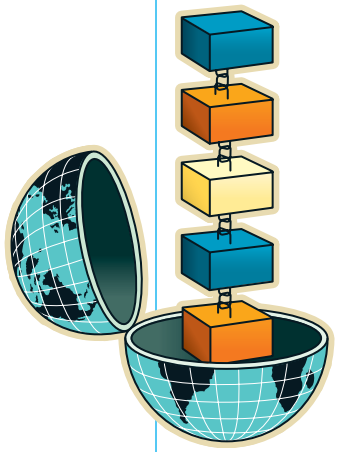
5

НАСКОЛЬКО БЕЗОПАСНЫ И НАДЕЖНЫ КРИПТОВАЛЮТЫ?

Поскольку криптовалюты — это не что иное, как программное средство, их надежность, по словам Каталини, исследователя из МТИ, «обеспечивается кодовой базой». Любой может сгенерировать криптомонеты и получать деньги за счет их продажи через первичное размещение — даже Пэрис Хилтон поддержала распространение непонятных токенов. Но это не совпадение, что две самых популярных криптовалюты, биткоин и эфир, были созданы специалистами по компьютерному программированию. При этом даже валюты с впечатляющей технической надежностью могут быть рискованными. В *DAO* — децентрализованной автономной организации, работающей с *Ethereum* и стоившей в 2016 г. свыше $100 млн, — «была ошибка» (по сдержанной оценке Каталини), которая позволила хакерам вывести из системы криптовалюту эфир на $50 млн.

10%

общемирового валового внутреннего продукта, согласно прогнозам Всемирного экономического форума, к 2025 г. будут аккумулированы в системах на базе блокчейна.



КТО ИСПОЛЬЗУЕТ БЛОКЧЕЙН-ТЕХНОЛОГИЮ?

Это технология используется не только киберлибертарианцами и не только в финансовой сфере. Вот неполный список.

- **ФИНАНСОВЫЕ ИНСТИТУТЫ.** Международные банки и инвестиционные институты исследуют и внедряют блокчейн-проекты, иногда объединяясь в консорциумы. С 2012 г. успешно работает *Ripple* — система на базе блокчейна для осуществления международных трансакций между банками. Стартапы, такие как *Bloom*, намерены задействовать блокчейны для кредитной отчетности, надеясь прекратить утечку данных, как случилось при взломе *Equifax*.
- **ПРАВИТЕЛЬСТВА.** В штатах Делавэр и Иллинойс распределенные реестры используются для свидетельств о рождении. В Вермонте закон разрешает использование блокчейн-технологии для удостоверения подлинности юридических документов. В Дубае блокчейны задействованы во многих административных услугах, таких как получение лицензий. В 2016 г. в Тунисе на базе блокчейн-технологии начался выпуск цифровой версии национальной валюты — *e*-динара.
- **ПРЕДПРИНИМАТЕЛИ В СФЕРЕ ТЕХНОЛОГИЙ.** Сеть *Ethereum*, разработанная скорее для поддержки новых прикладных программ, чем для экосистем цифровой наличности наподобие биткоина, функционирует как *AppStore* для блокчейн-стартапов. Сотни новых проектов и фирм работают на этой платформе. Так, *WePower* позволит домохозяйствам продавать и покупать возобновляемую энергию (вырабатываемую, например, установленными на крыше солнечными батареями) непосредственно друг у друга.
- **ПРАВООБЛАДАТЕЛИ.** Британская певица Имоджен Хип основала *Mycelia* — технологичный инкубатор, который отслеживает метаданные, связанные с музыкальными произведениями, исключив посредников, таких как *iTunes*.
- **НЕКОММЕРЧЕСКИЕ ФОНДЫ И ГРУППЫ ПОМОЩИ.** Фонд *BitGive* совершенствует отчетность, связанную с благотворительными пожертвованиями. Мировая продовольственная программа ООН рационализирует способы отслеживания и доставки помощи сирийским беженцам в Иордании.
- **ВУЗЫ.** Забудьте о бумажных дипломах: проект *Blockcerts* обеспечит доступ к любым документам о профессиональном образовании и сделает их более надежными.
- **КОМПАНИИ ПО УПРАВЛЕНИЮ АКТИВАМИ.** Находящаяся в Лондоне компания *Everledger* специализируется в индустрии бриллиантов и осуществляет регистрацию свойств и происхождения каждого драгоценного камня. Отслеживаются также вина высшего качества и произведения искусства.
- **ЖУРНАЛИСТЫ.** Чтобы защититься от фейковых новостей, *Civil* предоставляет платформу для независимых журналистов, защищенную от внешнего влияния и поддерживаемую читателями.
- **ОБЫЧНЫЕ ЛЮДИ.** Для работников-мигрантов, которые отправляют деньги своим семьям, использовать биткоины дешевле, чем *Western Union*, поэтому сейчас приблизительно 20% международных денежных переводов между Южной Кореей и Филиппинами осуществляется в биткоинах.

77%

мировой индустрии финансовых услуг, согласно прогнозу *PwC*, будут использовать блокчейн как часть производственной системы или процесса к 2020 г.

БИТКОИН — ЭТО БУДУЩЕЕ ИЛИ ОДНОДНЕВКА?

Биткоин — наиболее популярная мировая цифровая валюта, но крайне рискованная. Многие финансовые эксперты указывают на его легендарную неустойчивость: стоимость биткоина выросла более чем в десять раз с 2016 г., но всего за две недели в сентябре 2017 г. цена упала на 40% — и опять быстро восстановилась и превысила прежний уровень. (Кто знает, сколько будет стоить биткоин, когда вы прочитаете это.) По мнению других экспертов, из-за технических ограничений сети (медленная обработка трансакций) вкупе с непомерными расходами на майнинг биткоин превращается в финансовую бомбу замедленного действия. «Мы не уверены в биткоине», — говорит Чарли Моррис (Charlie Morris), директор по инвестициям фирмы *NextBlock Global*, инвестирующей в блокчейн-технологии.

Биткоин узаконил основы экономики мировой криптовалюты. Но следующий крупный «альткоин» (альтернатива биткоину), вероятно, более устойчив: криптовалюта эфир более похожа на «блокчейн-актив», как называет его Моррис, чем на наличные деньги, и используется для поддержания и безопасности сети *Ethereum*. По аналогии с арендой виртуальных серверов в облаке *Google* разработчики, желающие создавать программные приложения с использованием блокчейна *Ethereum*, должны оплачивать доступ в токенах эфира. Чем больше используется *Ethereum* в качестве основной платформы, тем более стабильной и ценной становится криптовалюта эфир. Велика вероятность, что появятся новые валюты и платформы: соревнование только началось.

ЗАЧЕМ ИСПОЛЬЗОВАТЬ КРИПТОВАЛЮТУ ВМЕСТО НАЦИОНАЛЬНОЙ ВАЛЮТЫ?

Представьте, что за стодолларовую банкноту можно купить товаров только на $50. В Венесуэле, где официальная валюта обесценивается, такой сценарий — реальность. «Каждый год вы теряете около половины чистого дохода из-за гиперинфляции, — говорит венчурный капиталист Моррис. — Люди думают: "Как это прекратить?" И покупают биткоины».

Почему же непонятная криптовалюта, ценность которой как законного платежного средства государством не гарантирована, кажется более надежным выбором, чем более традиционные, обладающие ценностью товары, такие как золото? С одной стороны, для простых людей конвертировать венесуэльские боливары в биткоины намного проще — это может сделать любой, у кого есть доступ в интернет. Поскольку биткоины не имеют физической формы, их не надо прятать где-то в ненадежном месте (под матрасом или, как в Венесуэле, на счете в банке). Конечно, цена биткоина тоже нестабильна. Но в то время как курс боливара резко падает, стоимость биткоина по крайней мере стремится вверх. В стране, где, по прогнозам МВФ, уровень инфляции в 2018 г. превысит 2300%, вложения в биткоины кажутся оправданным риском.

В Зимбабве столкнулись с противоположной проблемой. После того как страна отказалась от собственной валюты в пользу доллара США, теперь экономика зависит от импорта валюты, которой не хватает. В настоящее время биткоины получили настолько широкое распространение, что их принимают к оплате даже торговцы автомобилями.

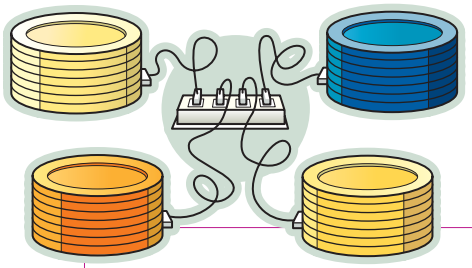
ОЗНАЧАЕТ ЛИ ЭТО КОНЕЦ НАЛИЧНЫХ ДЕНЕГ?

Может показаться, что напечатанные деньги ожидает та же судьба, что и газеты. Но эксперты утверждают, что до конца наличных еще далеко. «Мы все еще используем огромное количество наличности для оплаты таких услуг, например, как морские международные грузоперевозки, — говорит Винай Гупта (Vinay Gupta), главный исполнительный директор *Mattereum*, юридической фирмы по сопровождению смарт-контрактов. — Система не настолько непригодна, чтобы люди были готовы ее уничтожить». Проблема биткоина и эфира в том, что, хотя они и могут выполнять функции средства накопления или денежной единицы, криптовалюты не везде принимаются в качестве законного платежного средства, чтобы конкурировать с наличными деньгами.

В таких местах, как Кения, где редко у кого есть обычные банковские счета, а такие сервисы «мобильных денег», как *M-Pesa*, сделали хранение и перевод денег с помощью телефона более простыми, чем обмен наличных, криптовалюты могли бы пригодиться. Но для майнинга требуются мощные процессоры — необычный ресурс в Африке, где недорогих простых мобильных телефонов продается больше, чем смартфонов, и немногие среди населения имеют персональные компьютеры. Теоретически вычисления, необходимые для обеспечения безопасности трансакций в блокчейне, можно проводить с использованием «вашей старой *SIM*-карты *Nokia*», — говорит Гупта. И все же живые деньги не исчезнут в ближайшем будущем.

3 4 5

3 4 5



БЛОКЧЕЙН — ЭТО НОВЫЙ ВИД ИНТЕРНЕТА?

БЛОКЧЕЙН — ЭТО ЗАКОННО?

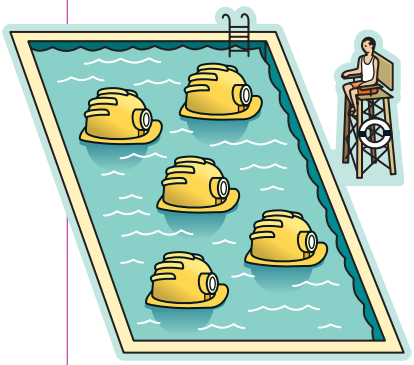
НАСКОЛЬКО БЕЗОПАСНЫ И НАДЕЖНЫ КРИПТОВАЛЮТЫ?

ЧТО СЛУЖИТ ИСТОЧНИКОМ ЭНЕРГИИ ДЛЯ КРИПТОВАЛЮТ?

То, что криптовалюты не имеют физического воплощения, не означает, что их использование ничего не стоит. Намеренно трудоемкий процесс, в ходе которого добываются новые биткоины, — добавление новых трансакций в реестр — требует, чтобы вся пиринговая сеть циклически проходила через бессчетное количество случайных вычислений для подтверждения трансакций в блокчейне. Для этого необходима энергия.

Сколько энергии? Начнем с количества вычислений. В конце 2017 г. хешрейт (единица вычислительной мощности) сети *Bitcoin* составлял около 10 эксахешей (10 млн трлн вычислений) в секунду. Оценить точный объем потребляемой энергии на основе этого показателя невозможно, так как в децентрализованной сети нельзя учесть вклад индивидуальных узлов. По заслуживающей доверия оценке, сеть *Bitcoin* ежегодно потребляет около 27 ТВт электричества — примерно столько же, сколько Ирландия. То есть только для производства биткоинов в год требуется 11 млн т угля, при сжигании которого в атмосферу выбрасывается 29 млн т диоксида углерода. Для снабжения сети *Bitcoin* солнечной энергией необходимо задействовать больше половины мощности, производимой для коммунального хозяйства гелиоэлектростанциями США в год.

Создатель *Ethereum*, Виталик Бутерин, теперь переводит блокчейн-сети на другой механизм подтверждения (валидации) — доказательство владения (*proof of stake*), — который не опирается на майнинг. Маловероятно, что в более крупной и более децентрализованной сети *Bitcoin* в ближайшее время будет сделано то же самое. Но Винай Гупта, разрабатывавший стратегию блокчейна в Дубае, считает, что жадность, побуждающая майнеров превращать киловатты в криптовалюту, в конце концов заставит их решать эту масштабную проблему. Венчурный капиталист Чарли Моррис полагает, что как только рыночная устойчивость криптовалют, базирующихся на механизме доказательства владения, будет подтверждена, «майнинг станет лишь всплеском в истории. Люди будут говорить: "Помните, как это было нелепо?"».



ГДЕ НА САМОМ ДЕЛЕ ПРОИСХОДИТ МАЙНИНГ?

71%

биткоинов добывается в Китае, на втором месте находится Индия (4%). Совет: не пытайтесь «майнить» дома, самостоятельно. Сейчас в этой деятельности господствуют гигантские майнинговые пулы, такие как в Китае, так что вероятность добыть блок одиночным узлом сети составляет 1 к 8 млн. Одиночные операторы потратят намного больше на счета за электроэнергию, чем заработают. Хотите заняться майнингом как хобби? Присоединяйтесь к публичным майнинговым пулам.

ЧТО ЛЮДИ ДУМАЮТ О БЛОКЧЕЙНЕ?

62% американцев уверены, что криптовалюты используются для незаконных покупок, или вообще не знают, для чего они используются (по данным опроса *YouGov*, проведенного в 2017 г.).

59% глобальных потребителей, опрошенных в 2017 г. *HSBC*, никогда не слышали о блокчейн-технологии; 80% тех, кто слышал о технологии, не понимают, что это такое.

39% руководителей высшего звена в крупных компаниях США отметили, что они знают мало или совсем не знают о технологии блокчейн (по данным исследования *Deloitte*, проведенного в 2017 г).

КАК ЭТА ТЕХНОЛОГИЯ БУДЕТ ИСПОЛЬЗОВАТЬСЯ В БУДУЩЕМ?

Каждый, кто полагается на технологию блокчейн, — футурист по определению. Когда технология распределенных реестров пройдет стадию страховочных колес, что можно создать с ее использованием?

- **САМОУПРАВЛЯЕМЫЕ САМОСТОЯТЕЛЬНЫЕ МАШИНЫ.** Пока вы на работе или спите, ваша машина будет ездить сама по себе, не работая на *Uber*. Смарт-контракты на базе блокчейна за счет автоматизации двух базовых функций — подбора машины для пассажира и содействия в осуществлении платежей — могут исключить посредников, таких как *Uber* или *Lyft*, из сферы совместного использования автомобилей. Вашу долю в долевой собственности на машину также можно будет выражать в токенах криптовалюты.
- **ПОРТАТИВНЫЕ МЕДИЦИНСКИЕ ДАННЫЕ.** По словам Брайана Белендорфа (Brian Behlendorf), исполнительного директора проекта *Hyperledger* фонда *Linux Foundation*, та же технология, что позволяет двум не обязательно доверяющим друг другу людям обмениваться биткоинами, может обеспечить безопасность медицинской информации, предоставив контроль пациентам. Пациенты получат «кошелек здоровья» со своими данными и историями болезней. Врач может обратиться к реестру и запросить данные о вашей группе крови, отправив на телефон пользователя запрос о доступе. «Вы получаете контрольный след, отражающий, кому была предоставлена информация, и можете удалить данные после окончания лечения», — говорит Белендорф.
- **ГЛОБАЛЬНЫЙ СУПЕРКОМПЬЮТЕР.** Подсоединение ваших устройств к тысячам других в пиринговой системе — и применение блокчейна для получения платы за их использование — станет финансовым стимулом для поддержания всемирного децентрализованного суперкомпьютера. Пока вы спите, ваши портативный компьютер и телефон смогут арендовать ученые, например для проверки моделей. Так уже работает проект *Golem*. «Вычислительная мощность множества простаивающих портативных компьютеров намного больше, чем у центров обработки и хранения данных, — говорит Гупта. — Проекты в сфере искусственного интеллекта и моделирования климата можно ускорить тысячекратно».

В ЧЕМ ЗАКЛЮЧАЮТСЯ ОГРАНИЧЕНИЯ И ОПАСНОСТИ БЛОКЧЕЙНА?

«Блокчейн предоставляет основу, которую, с учетом определенных допущений, очень трудно изменить постфактум, — говорит исследователь блокчейна Эмин Гюн Сирер. — Но это не значит, что все события, фиксируемые в блокчейне, подлинны и желательны. Если кто-то, взломав мой компьютер, украдет мои криптомонеты и попытается их использовать, я очень захочу отменить эту трансакцию. И тогда неизменяемость блокчейна становится преградой». Кроме того, легко перепутать теоретическую неизменяемость блокчейна с настоящей безопасностью данных: публичные блокчейны, такие как *Ethereum* и *Bitcoin*, на самом деле не кодируют информацию. Брайан Белендорф из фонда *Linux Foundation* в своих выводах заходит еще дальше: «Реестры нельзя использовать для хранения персональных данных или конфиденциальной информации, даже в закодированной форме. Потому что мы знаем: все, что будет зашифровано сегодня, через 40–50 лет расшифруют с помощью более совершенной технологии». Некоторые сторонники блокчейна говорят о нем как о панацее для любых социальных проблем, связанных с доверием, но это безрассудный оптимизм. Об ограничениях блокчейна в качестве спасителя общества читайте на следующей странице.

КАК РЕГУЛИРОВАТЬ ДЕЦЕНТРАЛИЗОВАННУЮ СИСТЕМУ?

Учитывая, что репутация децентрализованных цифровых валют сходна с репутацией Дикого Запада, легко предположить, что они были созданы для устранения или ухода от финансового регулирования. Но это не совсем верно. На самом деле у биткоина полно правил, просто они установлены и навязаны исходным кодом (и коллективной активностью пиринговой сети), а не правительством или финансовыми институтами. «Совершенно новое в биткоине — это стремление избежать общественного управления в сфере ведения учета», — говорит Патрик Мерк (Patrick Murck), юрист, исследователь политики и регуляции блокчейна из Центра Беркмана — Кляйна по изучению интернета и общества при Гарвардском университете. Заявленное предназначение *Ethereum* — поддержка внедрения автономных смарт-контрактов — исключительно регулятивная сфера. Блокчейн, вероятно, и есть не что иное, как регулирование: математически заданная система правил, определяющая, что можно и нельзя делать с записями в базе данных.

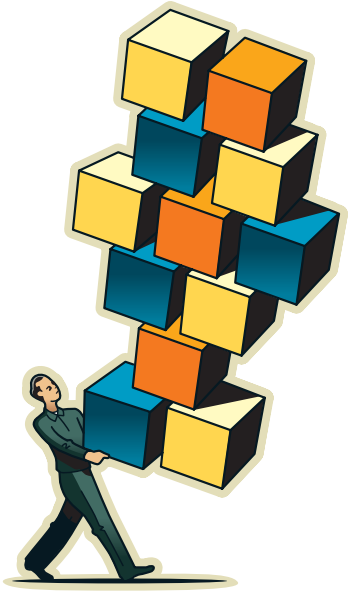
Важная составляющая в сфере финансового регулирования, децентрализованного или нет, — кто осуществляет регулирование и как. «В децентрализованной системе негде применять регулирование, но как только в этой системе вновь появятся посредники (третьи стороны), следом появится и регулирование», — говорит Мерк. В 2013 г. Китай ввел запрет на использование криптовалют в банковской системе, а в сентябре 2017 г. запретил использование биткоинов в качестве местных кредитных орудий обращения. США и Япония переходят к регулированию криптовалютных бирж и *ICO* (первичного размещения монет) с такой же бдительностью, как и в области торговли акциями и инвестиционной банковской деятельности.

Одно из применений блокчейна в будущем — обеспечение безопасности записей с цифровыми личными данными, и, по мнению венчурного капиталиста Чарли Морриса, могут появиться новые криптовалюты, в которых личные данные будут сочетаться с финансовой информацией. У таких криптовалют не будет анонимности биткоина (по оценкам Морриса, лишь нескольких сотен человек честно платят налоги с принадлежащих им биткоинов). Но когда электронные деньги становятся общедоступными, необходимость компромисса между ощущением безопасности и стабильностью может сделать надзор приемлемым или даже желательным. Мерк говорит: «Если я отдаю вам в распоряжение какую-то собственность, будь то биткоины или тряпичные куклы, и доверяю совершать с ней сделки, тогда ваша деятельность или уже регулируется, или скоро будет регулироваться».

В БЛОКЧЕЙНЕ МОЖЕТ ПРОИЗОЙТИ СБОЙ?

До настоящего времени блокчейн биткоина (первый и на сегодня самый крупный и широко используемый) никогда не был скомпрометирован или взломан. Но это не значит, что каждый блокчейн по определению неуязвим. «Совершенных технологий не бывает», — говорит Эмин Гюн Сирер, соруководитель *Initiative for Cryptocurrencies and Contracts (IC3)*. Рассмотрим три вида «дыр» (уязвимостей) в броне блокчейна.

АТАКА 51%. Безопасность сети криптовалют на базе блокчейна обеспечивается за счет двух безграничных ресурсов: скорости и жадности майнеров. Но теоретически возможно получить контроль и над тем и над другим. Для разрушения механизма согласования в блокчейне хакерам понадобилось бы «прибрать к рукам» большинство узлов сети. Это позволило бы им контролировать, как и какой блок добывать. Они смогли бы изменять направление новых трансакций и, таким образом, удвоить траты цифровой валюты. Или хакеры могли бы препятствовать подтверждению трансакций, выполняемых другими людьми. Пиринговая сеть биткоина, состоящая из тысяч узлов по всему миру, вряд ли станет жертвой такой атаки. Но более мелкие альткоины находятся в зоне риска: в 2016 г. сеть *Krypton* подверглась атаке группы под названием «Команда 51». Уязвимы даже блокчейны, в которых не используется майнинг, потому что они, как предупреждает Гюн Сирер, полагаются на «допущение, что большинство узлов в их сети безвредны».



СТАРЫЙ ДОБРЫЙ ЧЕЛОВЕЧЕСКИЙ ФАКТОР. Пытаться скомпрометировать сам блокчейн — все равно что пытаться горы свернуть. Но любые конструкции, возведенные на базе блокчейна или примыкающие к нему, по-прежнему уязвимы. В 2014 г. *Mt. Gox*, биржа биткоина (посредник, позволяющий людям конвертировать традиционные валюты, например доллары, в биткоины), в результате плохого управления и из-за дефектного кода потеряла 850 тыс. биткоинов, стоивших в то время $620 млн. И, наконец, блокчейны — это всего лишь распределенные реестры без службы технической поддержки, так что, если ваш кошелек полон криптовалюты и вы потеряли пароль, почти наверняка эти деньги исчезнут. Ирония в том, что некоторые держатели криптовалюты хранят распечатки своих кодов доступа (или даже саму валюту на *USB*-диске) в банковских ячейках, то есть на консервации.

«РАЗДУВАНИЕ» БЛОКЧЕЙНА. Это скорее не уязвимость, а естественный результат слишком хорошей работы блокчейнов. В связи с тем, что каждый новый блок обязательно повторно подтверждает предшествующий, каждый узел сети, осуществляющий валидацию, должен иметь копию самой последней версии всей цепочки, чтобы работать с каждой новой трансакцией. Блокчейн биткоина уже стал громоздким, поскольку его размер превышает 130 Гб и постоянно увеличивается. Более гибкий реестр *Ethereum*, который может работать как платформа для более сложных трансакций, таких как смарт-контракты, еще больше, чем реестр биткоина. Если все начнут его использовать, то с нагрузкой будут справляться только высокопроизводительные суперкомпьютеры? Это может эффективно децентрализовать сеть, но при этом свести к нулю саму идею распределенного реестра.

ЭВОЛЮЦИЯ ДОВЕРИЯ

КОНЕЧНЫЙ СОЦИАЛЬНЫЙ ЭФФЕКТ БЛОКЧЕЙН-ТЕХНОЛОГИИ ЗАВИСИТ ОТ ТОГО, КТО КОНТРОЛИРУЕТ НАШУ ЦИФРОВУЮ ЛИЧНОСТЬ

НАТАЛИ СМОЛЕНСКИ

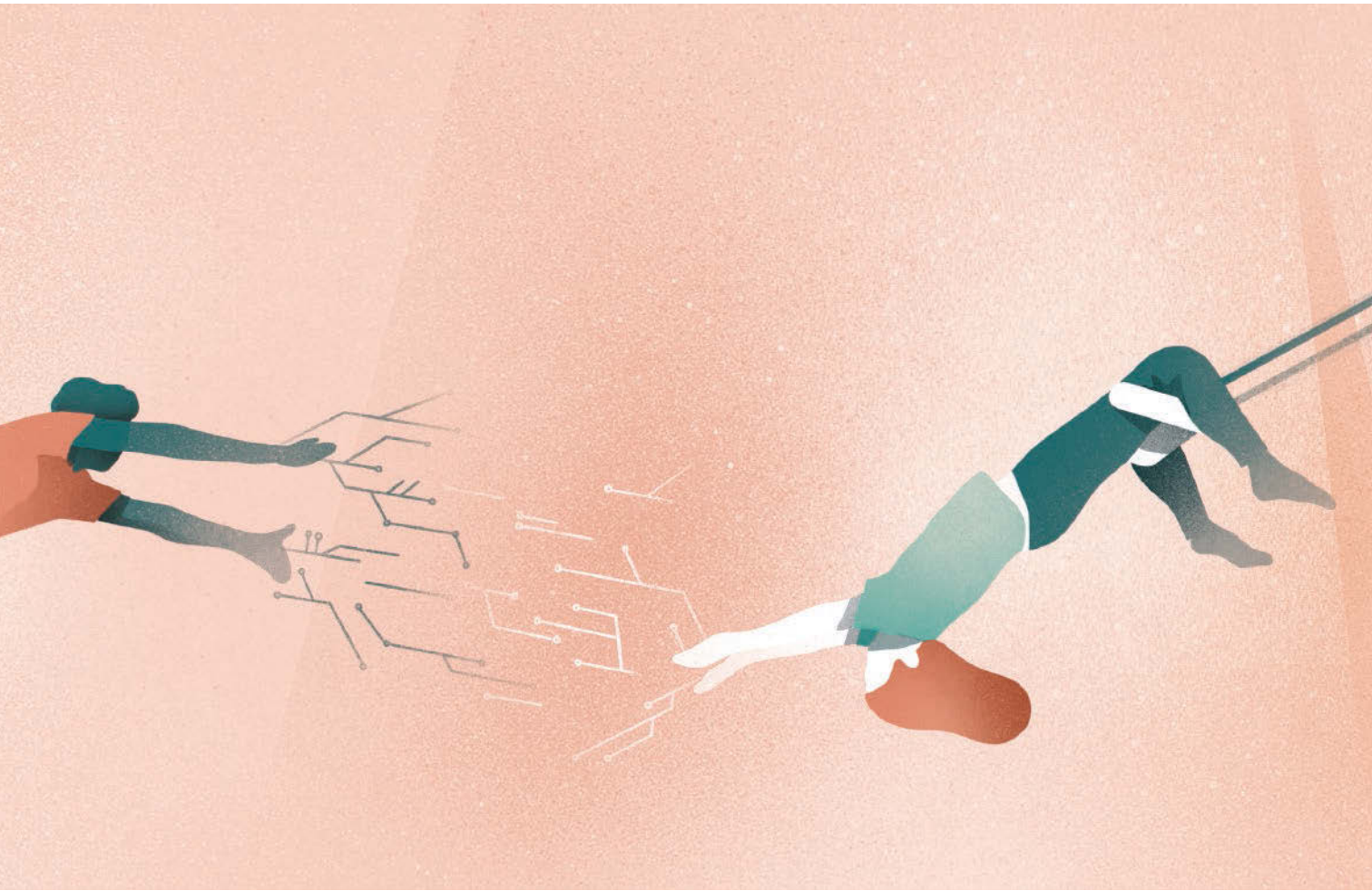
ОБ АВТОРЕ

Натали Смоленски (Natalie Smolenski) — культурный антрополог, исследует проблемы взаимодействия личности, технологий и правительства. Она возглавляет отдел развития компании *Learning Machine*, которая занимается разработкой приложений для выпуска и удостоверения официальных записей в блокчейне с использованием открытого стандарта *Blockcerts*.

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Банки и правительства потерпели целый ряд неудач в обеспечении доверия к международной экономике, особенно в последние несколько десятков лет. Обычные люди стали настороженно относиться к централизованной власти и ищут альтернативы.
- Биткоин (и блокчейн-технология в целом) позволяет передать функцию обеспечения доверия от организаций-посредников, таких как банки, машинам. Использование этой технологии могло бы полностью исключить эксплуатационные практики из финансовой системы, а не сдерживать их с помощью наказания.
- Блокчейны открывают возможности как для предоставления людям большей свободы, так и для обеспечения надзора и контроля в беспрецедентных масштабах. Как эта технология в конечном итоге будет использоваться, зависит от того, как программное обеспечение будет управлять цифровой личностью.

Для того чтобы принимать участие в современной мировой экономике, обычные люди должны согласиться на невыгодную сделку: их жизнь открыта для государств, банков и корпораций, тогда как поведение и закулисная деятельность могущественных игроков остаются скрытыми. Границы между потребителем и гражданином стали необратимо размытыми. Подобное взаимодействие, когда только одна сторона извлекает пользу, — серьезная структурная проблема. Социолог из Гарвардского университета Шошана Зубофф (Shoshana Zuboff) называет это явление надзирающим капитализмом. Сами институты, чьей привилегией стало обеспечение



социального доверия, — банки и правительства — во всем мире не справляются с этой задачей, особенно в течение жизни тех, кто моложе 35 лет.

Финансовый кризис 2008 г. и его последствия выявили своего рода беспомощность окружающего мира. Большинство дошедших до суда разбирательств закончились не реальными судебными сроками для высокопоставленных банкиров, а выплатами издержек заинтересованным лицам. Это убедило многих в том, что богачи и власть имущие находятся в сговоре. Проблемы кроются гораздо глубже, чем просто в негативных последствиях безнадежных ипотечных кредитов. Анализ базы данных за 2007 г. со списком из 37 млн компаний и инвесторов по всему миру выявил, что 1% таких компаний контролирует 40% системы и большинство в этом 1% составляют финансовые институты. За последние 30 лет во многих странах доходы от инвестиций стали основным источником экономического роста, намного опережая рост доходов населения и делая верхушку, состоящую из богатых людей, еще богаче. Тем временем 2 млрд людей до сих пор лишены банковского обслуживания и исключены из далеко не идеальной системы, в принципе облегчающей доступ к капиталу. Не существует единого мнения о том, следует ли и как изменить эти тенденции, чтобы повысить экономическое равенство и участие людей в экономике, не нарушая личную независимость.

Так мы подходим к историческому моменту, когда недоверие к власти и богатству обращается против самих основ экономической жизни, которые имеют всеобщий и меняющийся характер. Если и возникает побуждение отказаться от этих основ в знак протеста, то существует также и понимание, что это способ экономически навредить самим себе. Подобные ограничения заставили специалистов по технологиям во всем мире искать

альтернативные варианты, способные повысить уровень доверия и сделать его взаимным. Неслучайно первая успешная цифровая валюта, биткоин, «вышла на сцену» в 2009 г.: она представляет собой реакцию на растущее желание открытости, доступности и расширения прав.

Конечно, биткоин представляет собой валюту, обращение которой происходит посредством блокчейна — новой цифровой инфраструктуры, функционирующей как распределенный реестр, в котором трансакции подтверждаются в результате математического согласования, а не людьми. Блокчейн открывает новые возможности для прямого обмена и прав личной собственности, касающихся не только денег, но и любого цифрового актива.

О биткоине — и вообще о блокчейнах — часто говорят как о ненадежных. Но это не совсем точно. Скорее теперь доверяют не людям, а криптографической системе, к тому же обладающей материальными стимулами для участия в сети. Иными словами, происходит деперсонализация доверия. Сначала это может показаться парадоксом. Разве доверие во всех его формах в некоторой степени не связано с людьми? В ходе истории в связи с глобальной миграцией и торговлей сети доверия расширялись от маленькой группы людей, в которой все друг друга знают, до сообществ, в основном состоящих из незнакомцев и врагов. Чтобы занимать новые территории, кормить растущее население, вести войны, строить империи и обмениваться знаниями, люди используют «технологии доверия», прошедшие частично перекрывающиеся стадии эволюции. Этапы эволюции доверия: родство и дарение подарков, разделение труда, ведение учета (рождение кредита и долга), иерархия, обращение денег, универсализация религий и, совсем недавно, банковская деятельность.

В начале XXI в. доверие вступило в следующую стадию эволюции. Сами банки, которые выступали гарантами современного капитализма, действуя как надежные агенты, обеспечивающие доверие, стали препятствием для его развития. В современной финансовой системе политика и закон стремятся сдерживать практику эксплуатации за счет наказания. В будущем использование блокчейнов поможет просто исключить такую практику.

Конструкция из блокчейна

Протокол консенсуса биткоина, определяющий стимулы и требования, выполнение которых необходимо для участия в сети, исключительно хорошо поддерживает распределенную, открытую пиринговую систему управления. Трансакции в такой сети открыты, хотя и выполняются под псевдонимами, сама сеть имеет открытый код и поддерживается глобальным сообществом основных разработчиков-добровольцев. В блокчейне биткоина также не хранятся персональные данные: вместо учетных записей в качестве адресов используются пары из открытого и закрытого ключей.

Однако трансакции на базе блокчейна легче прослеживаются, чем наличные деньги. Следовательно, если пара ключей будет привязана к конкретной личности, сетевой анализ может помочь полиции выследить преступников. Это противоречит предположению, что криптовалюты больше пригодны для преступной деятельности, чем другие виды валют. Фактически вновь появляется призрак надзирающего капитализма. Интересно, что свойства блокчейнов позволяют использовать их как для предоставления людям большей свободы, так и для осуществления надзора и контроля на беспрецедентном уровне. Как блокчейны будут использоваться, зависит от архитектуры «программного стека» — протокола блокчейна и уровня приложений, то есть от архитектуры обработки цифровых личных данных.

Что касается протокола, то важно понимать, что блокчейн можно разработать по-разному. В общем случае термин «блокчейн» используется для описания типа системы, в которой единственная, универсальная запись трансакций копируется, хотя не существует абсолютного согласия в вопросе о том, каков набор необходимых характеристик. Сейчас существует несметное множество блокчейнов, сконструированных для решения различных задач.

Например, публичный блокчейн *Ethereum* выполняет роль всемирного распределенного компьютера под названием *Ethereum Virtual Machine*. В его «цепочке» хранятся смарт-контракты, которые исполняются при удовлетворении оговоренных в них условий. В отличие от сети *Bitcoin* пользователи, больше всего инвестировавшие в сеть, получают возможность совместной валидации новых блоков. У пользователей, нарушающих правила, криптовалюта автоматически конфискуется.

Некоторые блокчейны разработаны для сообществ с более высоким уровнем доверия среди пользователей. Такие «разрешенные» блокчейны в основном полагаются на центральный орган, предоставляющий определенным пользователям доступ к системе, так что они могут выступать в качестве валидаторов трансакций. В подобных сетях соблюдение правил пользователями обеспечивается скорее за счет повышения дисциплины под наблюдением центрального органа, чем материальными стимулами. Главный пример такой сети — *Ripple*, блокчейн, специально разработанный для осуществления трансакций между банками. *Enterprise Ethereum Alliance* состоит из почти 200 корпоративных членов, которые разрабатывают общедоступный инструментарий, позволяющий фирмам создавать собственные лицензионные версии на базе блокчейна *Ethereum*.

Одну из инициатив, подобных блокчейну, называют распределенными реестрами, поскольку

в них отсутствуют одна или несколько базовых характеристик блокчейнов. Их использование обычно разрешено, многие из трансакций также держатся в тайне. *R3 Corda* — крупный распределенный реестр, разработанный консорциумом банков для содействия достижению консенсуса в области финансовых соглашений.

Разрешенные блокчейны и распределенные реестры появились отчасти для того, чтобы включить в сеть определенного рода проверку личности валидаторов и лиц, осуществляющих трансакции. (В протоколе блокчейна биткоина намеренно отсутствует подтверждение личности.) Именно в вопросах, касающихся личных данных, и будет реализована социальная характеристика блокчейнов как «освободителя» или «угнетателя». Чем легче соотнести чьи-то трансакции с конкретной личностью и чем более централизованы и контролируемы извне цифровые личные данные, тем больше возможностей для роста количества злоупотреблений.

Перспективы и опасности

Обыкновенные люди не могут пользоваться непосредственно блокчейном, так же как и интернетом. Вместо этого применяются программные приложения, которые позволяют использовать базовый блокчейн тем или иным способом. Именно на уровне приложений царят скрытый беспорядок и зачастую недобросовестность. История биткоина омрачена ситуациями с биржами криптовалют и провайдерами кошельков, которые оставили слабые места в безопасности своих приложений, что привело к взломам, наделавшим много шума, и обвинениям в хищении. В случае с сетью *Ethereum* уязвимости привели к похищению или утрате миллионов долларов в криптовалюте эфир, и пользователи практически ничего не смогли сделать. В общем, использовать для хранения цифровых активов на базе блокчейна любое приложение, разработанное доверенной третьей стороной, все еще крайне небезопасно.

Вот в чем главная ловушка блокчейнов: общество не будет ими пользоваться без «дружественных» приложений. Но в приложениях, удобных для пользователя, часто такая простота достигается через централизацию, то есть воспроизведение условий контроля, которые блокчейны пытаются обойти.

Тем не менее если блокчейны станут широко применяться, то некоторая корреляция между трансакциями и личными данными необходима. Возможно, идентификация не потребует полного раскрытия информации о том, кто вы. Как доказывают некоторые представители биткоин-сообщества, нынешняя навязчивая идея о проверке идентичности неуместна. Все, что, в общем-то, требуется знать, — соответствуют ли действительности конкретные данные о вас. Вам правда больше 21 года? Действительно ли вы получили кандидатскую степень в Массачусетском технологическом институте? Вы гражданин США? Мотивационные структуры надзирающего капитализма приучили нас верить, что для существования в этом мире необходимо отказаться от удаления персональных данных. Изменение этой исходной предпосылки — один из самых радикальных эффектов, который могут иметь блокчейн-технологии.

Представьте, например, будущее электронного голосования. Счетная комиссия должна коррелировать подсчитанные голоса с зарегистрированными избирателями, чтобы отметить, что человек проголосовал. Но этот процесс необязательно должен идентифицировать человека перед комиссией: достаточно просто подтвердить, что избиратель зарегистрировался для участия в этих выборах, и после того как тот проголосует, зафиксировать, что он отдал свой голос, не связывая голос с избирателем.

Проекты, которые минимизируют распространение так называемой информации, соотносимой с личностью, все еще редко встречаются, отчасти потому, что их нелегко «монетизировать», то есть превратить информацию как в традиционную валюту, так и в «валюту» в виде персональных данных. Одним из таких проектов стал *Blockcerts* — серия свободных справочных библиотек, разработанная Медиалабораторией Массачусетского технологического института и фирмой *Learning Machine*, где работает автор статьи. *Blockcerts* позволяет людям хранить свои цифровые активы в личном кошельке на собственном мобильном устройстве. Документы, выданные человеку, не ассоциируются с каким-то личным профилем, если получатель не пожелает сделать это. Все коды общедоступны, их целостность можно проверять. Коды может использовать любой желающий для разработки собственных приложений для отправки, хранения, распространения и подтверждения официальных документов. Такой заявительный подход — шаг к тому, что некоторые в пространстве цифровой идентичности назвали «самовластная личность», подразумевая, что люди обладают административным контролем над собственными данными.

Блокчейны — это действительно взрывная технология доверия. Но если при разработке приложений на базе блокчейна не учесть цифровую независимость личности, то ничто в принципе не помешает относиться к людям как к множеству объектов в цепочке, каждое движение и деятельность которых записываются, причем, возможно, постоянно. Создание цифровой личности, чье существование не зависит от правительств и корпораций, — следующий серьезный вызов, который бросают нам блокчейны, и они же могут помочь с ним справиться. ■

Перевод: С.М. Левензон