Содержание

Предисловие

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

Вполне возможно, мы находимся на пороге блокчейн-революции. Эта революция началась с появлением новой экономической реальности в интернете — альтернативной валюты под названием биткойн, которая эмитируется и обеспечивается не государством, а пользователями биткойн-сети при автоматизированном достижении консенсуса между ними. Но уникальность этой валюты заключается в том, что ее пользователям не обязательно доверять друг другу. Встроенные в систему

алгоритмы саморегулирования предотвращают любые злонамеренные попытки обмана. Если быть точным, то с технической точки зрения биткойн — это цифровые деньги, обращающиеся в децентрализованной, пиринговой электронной платежной системе, основанной на публично доступной книге учета, именуемой блокчейном.

По сути — это новая форма денег, комбинирующая одноранговый обмен файлами[1*], подобно BitTorrent, и криптографическую систему с открытым ключом[2**]. С момента возникновения биткойна в 2009 году у него появился целый ряд подражателей — альтернативных криптовалют, в целом использующих тот же подход, но с некоторыми изменениями и улучшениями. Важно, что блокчейн-технология способна стать органичной экономической оболочкой сети интернет, обслуживающей онлайн-платежи, децентрализованный обмен, заработок и расходование денежных единиц, получение и передачу цифровых активов, а также создание и исполнение умных контрактов. Как средство децентрализации эти технологии могут стать следующим фундаментальным прорывом в информационных технологиях — после мейнфреймов, персональных компьютеров, интернета, мобильных и социальных сетей. Они способны коренным образом изменить жизнедеятельность человечества, как это в свое время сделал интернет.

---

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

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

Валюта, контракты и приложения блокчейн вне финансовых рынков

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

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

---

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

** DNS (англ. Domain Name System — система доменных имен) — это система, позволяющая преобразовывать символьные имена доменов в IP-адреса (и наоборот). Домен — определенная зона в системе доменных имен (DNS) интернета, выделенная какой-либо стране, организации или для иных целей. — *Прим. ред.*

генетики[3*], но новейшие экономические модели, в частности экономики совместного использования *(sharing economy)*, реализуемые такими компаниями, как, например, Airbnb и Uber, эффективно противостоят запретительным инициативам властных структур[4].

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

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

---

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

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

В качестве примера, которых в этой книге будет еще немало, можно привести использование блокчейн-технологии для регистрации и защиты объектов интеллектуальной собственности (ИС). Новая отрасль так называемого цифрового искусства *(digital art)* предлагает услуги по частной регистрации в распределенном журнале записей точного содержания любого цифрового актива: файла, изображения, медицинской записи или программного обеспечения. Блокчейн может дополнить или полностью заменить собой все существующие системы управления ИС.

Работает это следующим образом. Для начала к любому файлу применяется алгоритм, сжимающий этот файл в короткий код из 64 символов, называемый «хеш», который уникален для данного документа[5*]. Каким бы ни был размер файла — например, объем файла генома составляет 9 Гб, — на выходе получается уникальный 64-символьный хеш, не позволяющий восстановить исходный файл. Полученный хеш включается в блокчейн-транзакцию с добавлением метки времени — доказательство существования цифрового актива на тот момент. Имея исходный файл, который хранится на компьютере собственника, а не в распределенном журнале записей, всегда можно повторно вычислить его хеш и убедиться, что содержимое файла не подверглось изменению.

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

---

[*] «Хеш» или «хеш-функция»; число фиксированной длины, которое ставится в соответствие данным произвольной длины таким образом, чтобы вероятность появления различных данных с одинаковым хешем стремилась к нулю, а восстановить данные по их хешу было как можно труднее. — *Прим. ред.*

Блокчейн 1.0, 2.0 и 3.0

Многие уже начинают понимать, что благодаря своим экономическим, политическим, гуманитарным и юридическим преимуществам биткойн и блокчейн-технологии превращаются в мощнейшую подрывную инновацию, способную коренным образом изменить большинство аспектов жизни общества. Для упорядочения и удобства давайте разделим различные — существующие и потенциальные — технологические аспекты блокчейн-революции на три категории: блокчейн 1.0, 2.0 и 3.0.

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

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

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

Что такое биткойн?

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

В терминах легко запутаться, потому что слова *«биткойн»* и *«блокчейн»* могут обозначать любую из трех частей концепции:

базовую *блокчейн-технологию, протокол* и *клиента,* обеспечивающие выполнение транзакций, и собственно криптовалюту (деньги). Кроме того, эти термины могут применяться для обозначения и концепции криптовалют. Это все равно что называть термином «PayPal» сам интернет, через который работает протокол PayPal, служащий для перевода валюты PayPal. В блокчейн-индустрии эти термины часто смешиваются, поскольку пока не завершился процесс формирования общепризнанного многоуровневого стека технологий.

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

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

Биткойны создаются как вознаграждение за выполнение математических вычислений. Суть этой работы, называемой *майнингом (mining)* в том, что пользователи предоставляют свои

---

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

вычислительные ресурсы для верификации адресов и записи транзакций в реестр. В награду за участие в майнинге пользователи получают комиссию за транзакции и вновь создаваемые биткойны. Помимо майнинга, биткойны, как и любую другую валюту, можно получить в обмен на обычные (фиатные*) деньги, товары и услуги. Пользователи могут отправлять и получать биткойны с помощью *электронного кошелька* через веб-браузер или приложение, установленное на персональном компьютере или мобильном устройстве, и, в зависимости от размера транзакции, может взиматься комиссия.

Что такое блокчейн?

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

Поскольку блокчейн представляет собой реестр, любое средство просмотра, например сайт https://blockchain.info, позволяет

---

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

легко запросить транзакции, относящиеся к определенному биткойн-адресу. Так, например, в собственном электронном кошельке можно увидеть транзакцию, в которой вы получили свой первый биткойн.

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

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

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

масштабе без ограничений по форме активов, типу участников или географическому положению.

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

Связанный мир и блокчейн: пятая революционная парадигма вычислений

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

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

---

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

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

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

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

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

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

---

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

** Токен (от англ. token «знак, символ; опознавательный знак; жетон») — термин, в русском языке имеющий несколько узких значений. В данном контексте — монетовидный жетон, использующийся в качестве заменителя денег. Также под токеном понимается ключ — компактное устройство в виде USB-брелока, предназначенное для авторизации пользователя, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, надежного хранения данных. — *Прим. ред.*

Мир уже готов к всеобщим деньгам, в основе которых лежит взаимодействие в интернете. Apple Pay (использующее токены мобильное приложение электронного кошелька компании Apple) и конкурирующие продукты могут стать той поворотной точкой, с которой начнется мир полнофункциональных криптовалют, где блокчейн станет интегрированным экономическим слоем веба.

Рис. П-1. Революционные парадигмы вычислений: мейнфреймы, ПК, интернет, социальные и мобильные сети, блокчейн[8]

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

Блокчейн — революционная парадигма для «интернета людей», но она может также стать валютной основой «экономики машин». По оценкам компании Gartner, к 2020 году пространство интернета вещей будет насчитывать около 26 млрд устройств, а оборот интернет-экономики достигнет 1,9 трлн долларов[9]. Для управления транзакциями между этими устройствами потребуется «интернет денег»[10] и соответствующая криптовалюта, а микроплатежи между подключенными устройствами могут развиться в новый уровень экономики[11]. По оценкам компании Cisco, количество M2M-подключений (*machine-to-machine*, то есть связь между машинами)