ЛОРАН ЛЕЛУ

БЛОКЧЕЙН ОТ А ДО Я

С ПРЕДИСЛОВИЕМ УИЛЬЯМА МОГАЙАРА, АВТОРА КНИГИ «БЛОКЧЕЙН ДЛЯ БИЗНЕСА»

«Огромная благодарность Лорану за то, что он сумел расширить границы нашего понимания блокчейна, так как обучение — это сложная, но благородная задача».

Annotation

Французский бестселлер, доступно объясняющий, что такое Блокчейн, где применяется эта технология, как она связана с криптовалютой и кто ее создатель. Для ее чтения и понимания не нужно обладать никакими специальными знаниями – все описано очень просто и внятно и, что самое важное, правильно.

Лоран Лелу

Блокчейн от А до Я. Все о технологии десятилетия

Blockchain: La révolution de la confiance Laurent Leloup

Blockchain © 2017 Groupe Eyrolles, Paris, France

Предисловие

Блокчейн – лучший инструмент нынешнего десятилетия. Тем не менее, общество по-прежнему не понимает эту технологию до конца и не знает, в чем причина проблем, стоящих на пути ее окончательного успеха.

Вот почему так важна работа Лорана Лелу, которую он провел для написания этой книги, – она помогает нам понять принципы блокчейна и разобраться в его многочисленных особенностях.

Хотя эта книга станет отличным подспорьем для тех, кто хочет понять принципы блокчейна, ее одной будет недостаточно, ведь читателю необходимо научиться «думать в стиле блокчейн». Чтобы реально проникнуть в суть блокчейна, вам необходимо постоянно проявлять любопытство к этой теме, поскольку с первого захода понять все до конца вам вряд ли удастся.

Блокчейн можно без преувеличения назвать многоцелевым проектом. В зависимости от того, кто вы и чем занимаетесь, блокчейн способен предложить вам то, что нужно. К примеру, для разработчиков программного обеспечения блокчейн является наиболее интересной средой с момента появления языка Java в 1995 году. Для бизнеса блокчейн стал мощным катализатором реинжиниринга бизнес-операций и внешних связей. Предпринимателям блокчейн позволяет создавать стартапы, не боясь начинать новое дело с небольшим числом клиентов.

Блокчейн – это не просто объект, продукт, тенденция или некая возможность. Блокчейн состоит из нескольких частей, некоторые из которых работают вместе, а другие – самостоятельно и независимо. Благодаря этой модульности блокчейн имеет бесконечное множество вариантов использования.

Развитие блокчейна несет в себе огромные перспективы. Эта книга покажет вам, что теория блокчейна схематична, и вы быстро сможете преодолеть разрыв между теорией и практикой применительно к

реальным проектам (прежде всего вашим) и устранить препятствия на пути к успеху.

Идея блокчейна простая, но мощная – она заключается прежде всего в новаторском подходе. Речь здесь идет не только о том, как создать лучшую сеть, банк или обеспечить более качественное обслуживание. Развитие блокчейна зависит от того, что делают люди, и влияют на это не только его технические характеристики. Распространение блокчейна происходит постепенно, начиная с разработчиков и стартаперов. За ними следуют люди, связанные с 1Т-бизнесом, а за ними – компании, которые открыли для себя огромный потенциал блокчейна. Далее блокчейном заинтересуется широкая общественность, которая потребует изменений, и, наконец, организации, которые до этого сопротивлялись изменениям.

Но, чтобы добраться до этого этапа, нужно больше пользователей приложений блокчейна, больше самих приложений и гораздо больше разработчиков. В долгосрочной перспективе большинство пользователей не будут знать или понимать, что в программном обеспечении или сервисе, которым они пользуются, присутствует блокчейн. Мы и сегодня оцениваем возможности приложения по его достоинствам и удобству, а не потому, что оно работает на основе базы данных и основано на той или иной технологии.

Так же как экономика Интернета, блокчейн создаст новую экономику, и мы не должны упускать из виду этот потенциал. Криптотехнологическая экономика будет экономикой, основанной на децентрализованном доверии, как в политическом плане, так и в плане цифровой архитектуры. Блокчейн обеспечит всем равный доступ и уменьшит высоту барьеров для всех участников.

Распространение и обмен информацией – ниша, изначально занятая Интернетом, тогда как функцией блокчейна является передача ценностей. Вот основная суть того, что вам следует знать о блокчейне, – и почти все, что следует из базовой идеи. Несмотря на порожденное им смятение и беспокойство, мы должны помнить, что по сути своей блокчейн – это перспективная технология. Как и в случае с любой перспективой, нужно время, чтобы она приблизилась. Но, чтобы выполнить все эти обещания, нам понадобятся миллионы людей, разбирающихся в технологии

блокчейна, миллионы бизнес-лидеров и миллионы активных пользователей. Поскольку постепенное развитие блокчейна можно наблюдать на протяжении всей истории существования Интернета, нужно не оглядываться назад, а быстрее устремиться вперед.

Огромная благодарность Лорану за то, что он сумел расширить границы нашего понимания блокчейна, так как обучение – это сложная, но благородная задача.

Уильям Могайар[1]

Введение

Когда в октябре 2015 года в журнале The Economist вышла статья под заголовком «Блокчейн, трастовый механизм», Интернет и социальные сети очень быстро и массово подхватили и распространили ее.

Из этого можно сделать вывод, что в конце 2015 года слово «блокчейн» еще не достигло той известности, которой оно может похвастаться сегодня. Так что даже такой солидный журнал, как The Economist, вынес на обложку утверждение, что блокчейн является механизмом создания доверия и лежащая в основе биткойна технология изменит принципы работы всей современной экономики.

Такое заявление могло пробудить интерес у любого издания, и долго ждать не пришлось – в течение следующих нескольких часов, а затем и дней, многочисленные блоги, газеты, журналы и другие средства массовой информации одно за другим стали перепечатывать и цитировать «громкую статью» с более или менее точным описанием технологии блокчейна, биткойна и других криптомашин. Но главное к тому моменту уже произошло – намечающаяся динамика и эффект разорвавшейся бомбы после статьи, напечатанной в The Economist, сделали свое дело.

С октября 2015 года напор выдаваемой СМИ информации на тему блокчейна практически не упал, а количество ежедневно создаваемых новых проектов по технологии блокчейн, цифровых валют и других *распределенных реестров* выросло феноменально.

У этой статьи в солидном журнале был по меньшей мере один большой плюс: с нее началось обсуждение блокчейна, биткойна, криптовалют и распределенного консенсуса, а кроме того, она начала готовить людей к пробивной технологии, названной Доном Тапскоттом «революционной» и уберизирующей «Убер», «наивысшей уберизацией»[2], как заявил Филипп Эрлен в своем интервью.

С тех пор появилось не так много новых проектов: масса рекламы, но

мало конкретных достижений, кроме нескольких опытных образцов, находящихся в процессе разработки. Но – скажете вы – разве этого недостаточно для технологии, только начинающей свой жизненный путь?

На самом деле, самое важное, о чем следует помнить после всей этой горячечной раскрутки в средствах массовой информации, это то, что, по словам Людвига Сигела, автора статьи, опубликованной в журнале The Economist, то новое, что привносит блокчейн, это не деньги… но доверие.

Следует понять, что блокчейн – революционная технология, которая разрушит многие бизнес-модели, полностью трансформирует экономику и общество и принесет в качестве научно-технической новинки… что? Доверие.

Мы сейчас оказались на переправе – давление в СМИ снизится до обычного, начнет расти мастерство специалистов; предприятия, сначала крупные, а затем средние, будут оснащены соответствующими технологиями; проекты, использующие блокчейн, начнут множиться; технология будет развиваться; проснутся инвесторы, и в конце концов мы получим общее для всех представление об этой технологии – мы будем смотреть на мир с позиций доверия. Именно это и обещает нам блокчейн.

После появления Интернета в 1990-х, а затем блокчейна биткойн, созданного Сатоси Накамото[3], поколения X и У[4] показали нам возможности социальных сетей с их прозрачностью.

Интернет упустил шанс поставить человека в основу своей технологии, и теперь именно блокчейн может обеспечить нам власть и свободу.

Глава 1

Что такое блокчейн?

Тот, кому не хватает знаний, постоянно мечется, меняя направление своего движения.

Реми Белло

Демистификация блокчейна

Определение

Дать опередеделение блокчейну в нескольких словах нелегко, поскольку каждый читатель, опираясь на свой образ мышления, свои достижения и опыт, будет воспринимать те или иные формулировки по-разному.

Ниже я приведу несколько определений, которые по нарастающей позволят вам лучше понять, что же такое блокчейн.

Упрощенное: Блокчейн – это большая бухгалтерская книга, или журнал (гроссбух), куда каждый может вносить записи и который каждый может прочитать, разбросанный по огромному количеству компьютеров во всем мире.

Базовое: Блокчейн – это программный продукт, который позволяет хранить и преобразовывать величины или данные при помощи Интернета защищенным и прозрачным способом, не имея при этом центрального управляющего органа.

Буквальное: Блокчейн описывает цепочку блоков (числовых контейнеров), в которых хранится информация самого разного вида: транзакции, контракты, документы о собственности, произведения искусства и т. д.

Обобщенное: Блокчейн – это технология, использующаяся в транзакционных приложениях нового поколения, которая, благодаря алгоритму коллективного консенсуса и распределенному децентрализованному «гроссбуху», создает доверие, ответственность и прозрачность среди всех участников.

Техническое: Блокчейн – это технология организации базы данных,

опирающаяся на Интернет и полностью использующая все его достоинства, включающая открытый протокол и способность к расчетам и шифрованию. Эту распределенную базу данных транзакций можно сравнить с бухгалтерской книгой, в которой каждая новая транзакция записывается следом за предыдущими без возможности изменить или уничтожить предшествующие записи. Эта книга активна, составлена в хронологическом порядке, распределена, проверяема и защищена от фальсификации системой распределения доверия (консенсусом) между участниками системы (узлами).

Можно также предложить определение, которое суммирует то, что было сказано выше: Блокчейн – это распределенная база данных транзакций, которую можно сравнить с огромным децентрализованным и распределенным гроссбухом, где, благодаря Интернету, прозрачно защищены и автономно хранятся и преобразовываются величины и данные, при этом центральный контролирующий орган отсутствует. Эта книга активна, составлена в хронологическом порядке, распределена, проверяема и защищена от фальсификации при помощи системы распределения доверия (консенсуса) между участниками (узлами). Каждый участник сети обладает актуальной копией этого «гроссбуха» (в квазиреальности[5]), содержимое которого все время синхронизируется со всеми остальными участниками.

Таким образом, блокчейн:

• позволяет автоматизировать транзакции, не привлекая при этом третьей стороны;

• является системой распределенного консенсуса и доверия;

• представляет собой инфраструктуру, обеспечивающую подтверждение подлинности и нотаризацию[6].

Основные принципы блокчейна

Основные принципы, на которых базируется блокчейн, следующие:

 *Распределенный гроссбух,* или *регистр 2.0,* построен по принципу книги учета и распределен между всеми участниками.

 *Децентрализация и отказ от посредничества:* Блокчейн не контролируется никаким центральным органом, в этой доверительном системе отношений между двумя участниками нет третьих лиц.

 *Консенсус:* Факт принятия транзакции или отказа от нее является результатом распределенного консенсуса, а не решения некоего централизованного института.

 *Неизменность и устойчивость*: Невозможно изменить или уничтожить записи.

 *Распределенное доверие и прозрачность:* Разделяются данные, операции и консенсус.

Другими словами: работа с использованием механизма коллективного консенсуса, а также использование огромной открытой книги учета, децентрализованной и разделенной между участниками, влекут за собой *доверие, прозрачность и чувство общности.*

Таким образом, у блокчейна могут выявляться специфические технические особенности использования его с теми или иными приложениями.

Технология блокчейна может менять правила игры: меньше централизации, меньше власти, больше разделения. Таким образом, блокчейн несет в себе инфраструктуру распределенного алгоритмического доверия, или *консенсус по требованию.*

Именно благодаря этим свойственным инфраструктуре аспектам многочисленные наблюдатели сравнивали блокчейн с Интернетом, но в результате пришли к выводу, что он превзойдет Интернет.

От Интернета к блокчейну

Чтобы проиллюстрировать это высказывание, проведем сравнение:

 Интернет позволяет автоматизировать связи (и установление связей и отношений), в то время как блокчейн позволяет автоматизировать транзакции, упраздняя третьих лиц.

 Интернет – это система децентрализованной публикации, в то время как блокчейн – это система распределенного доверия.

 Интернет – это инфраструктура публикаций, в то время как блокчейн – это инфраструктура подтверждений прав доступа.

Мы можем подвести итог периода 1994–2015 годы (периода, в который происходило основное развитие Интернета и блокчейна) следующими примерами:

 1994 год, Интернет:

- Межличностное общение;
- Автоматическая публикация;
- Электронная коммерция;
- Социальные сети.

 2015 год, блокчейн:

• Децентрализация и доверие;

• Оборот ценностей без посредничества.

Таким образом, между Интернетом и блокчейном нет никаких противоречий. Имеет место лишь развитие технологий (можно сказать, революция, см. главу 4), недавно достигшее своего пика.

Как работает блокчейн?

Для создания и работы блокчейна необходимы реестр (строка блоков, например биткойн), шифрование с ключами для защиты сделки, алгоритм (на основе консенсуса) для проверки транзакций, а также одноранговая сеть[8], чтобы все заработало. Вы добавляете участников, и это, если вкратце, все необходимые элементы.

Возьмем для примера блокчейн биткойн, процесс образования которого, а также основные принципы и способ функционирования мы рассмотрим в следующей главе, и опишем его функционирование, разбив на четыре этапа:

 Этап 1: Два участника согласовывают условия транзакции (передачу денег, активы, финансовые документы и т. д.).

 Этап 2: Журнал «сканируется» членами сети. Посредством анализа его хронологии члены сети удостоверяются, что продавец действительно обладает заявленными активами или фондами, которые он продает.

 Этап 3: Если все в порядке, транзакция подтверждается и добавляется в последний блок цепи.

 Этап 4: Журнал распространяется среди всех участников сети. Его распространенность обеспечивает его защищенность. Для фальсификации транзакции необходимо было бы изменить журналы у всех членов (узлов) сети.

Таким образом, чтобы получить статус достоверной, каждая сделка должна быть подписана с помощью асимметричной криптографии[10]

(закрытый ключ/ открытый ключ).

Следовательно, для осуществления транзакции в блокчейне типа биткойн необходимы три вида информации:

• личный ключ дебетового адреса;

• общий ключ кредитового адреса;

• сумма транзакции.

Биткойн-адрес представлен в формате АБСМ[11]с помощью специализированного кодирования 58 буквенно-цифровых символов: это цифры, а также заглавные и строчные буквы, за исключением букв и цифр I, I, O и O, которые Сатоси Накамото исключил, так как в некоторых шрифтах они выглядят одинаково. Первый созданный адрес имел вид: 1A1zP1eP5QGefi2DMPTfTL5SLmv7Divfna44.

(Например, мой биткойн-адрес выглядит так: 112BekzNCw8xEfwtpwDgKr3zEfUgyuxUZV.)

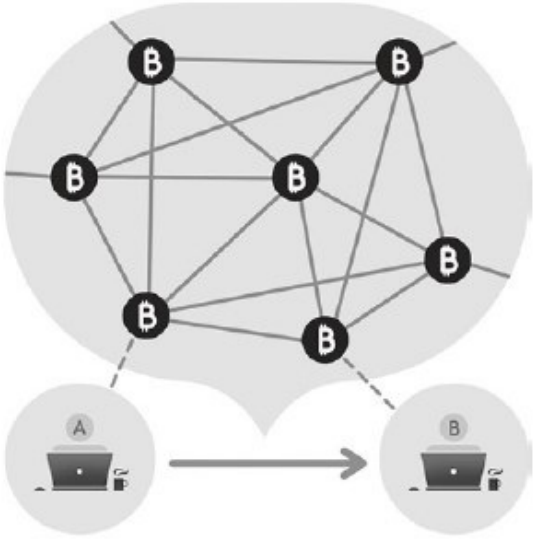
Широкая публика понемногу открывает для себя биткойн, криптовалюту и, в конечном счете, блокчейн. Но люди в основном не слишком хорошо понимают, что собой представляет эта система и для чего она служит. По правде говоря, шумиха в СМИ вокруг их использования и отсутствие популяризации этой новой технологии не способствуют лучшему пониманию.

Таким образом, наши дни вполне можно сравнить со временем рождения Интернета – тогда общественность услышала о революционной технологии, не понимая толком принципов ее работы, но при этом отлично ощущая ее воздействие на экономику и общество.

«Блокчейн похож на Интернет до появления браузеров»: сегодня, когда мы перемещаемся от сайта к сайту или осуществляем транзакции с помощью ПК или смартфона, нам нет необходимости понимать, что такое Интернет и как он работает. То же самое произойдет и с блокчейном, когда им начнут широко пользоваться и будут разработаны удобные интерфейсы.

Классическая система:
централизованная с третьей контролирующей стороной

ПРОТИВ



Система блокчейна:
распределенная и без третьего доверенного лица

Для чего это нужно?

Банковская деятельность – первый задействованный сектор

Блокчейн – это абсолютно новое, децентрализованное, безопасное и прозрачное решение, позволяющее хранить информацию, обмениваться ею, определять ее подлинность и проверять ее, причем цена всех этих действий достаточно невысока. Все выполняется самим пользователем, поэтому в сделке не требуется участие третьего доверенного лица. Именно в отсутствии стороннего доверенного лица и состоит основная инновация и оригинальность блокчейна.

В настоящее время мы знаем всего о нескольких способах его использования, но, похоже, возможностей применения блокчейна очень много, причем в самых разных областях экономики и общества. И эти возможности будут множиться с появлением все более новых технологий блокчейна.

Целью создания блокчейна биткойн (2009) было не служение миру финансов, а напротив – его замена. С течением времени банки начали осознавать тот факт, что эта технология может нарушить их бизнес-модель и представляет собой одновременно и угрозу, и возможность.

Филипп Эрлен[12] в своем интервью газете «Ле Монд», в котором рассматривались возможные применения технологии блокчейна в банковской и финансовой сферах, заявил: «Блокчейн – это высшая форма уберизации. Даже уберизированные услуги в Интернете могут быть улучшены с его помощью: Uber, Airbnb… они платят инженерам, компьютерщикам».

Начиная с октября 2015 года, СМИ во Франции начали говорить о

приближающейся технологической революции, о технологии, которая перевернет самые основы бизнеса, финансовой деятельности и даже общества. Начался ажиотаж в средствах массовой информации, футуристы и прочие провидцы предлагали свой взгляд на грядущие изменения, предрекая великие разрушения и революционные потрясения.

С появлением биткойна и шума в СМИ, развернувшегося вокруг новой, преобразующей мир технологии, банкам и другим финансовым учреждениям оказалось непросто пренебречь этой информацией. Тем более что технология блокчейна, как оказалось, позволяет мгновенно осуществлять сделки с минимальными издержками и без обращения к централизованному органу управления.

Казалось, что технология блокчейна наконец готова изменить, помимо прочего, и мир банковских операций за счет снижения рисков контрагентов и, как следствие, потребности в собственных средствах, сокращения расходов на инфраструктуру сети и компьютерный персонал, а также благодаря экономии на обработке информации.

Учитывая перспективу столь значительной и быстро реализуемой экономии и возможного разрушения привычных схем, очень многие банки присоединились к R3CEV[14] (или, как его чаще называют, R3), запущенному в сентябре 2015 года, для того чтобы исследовать эту технологию и развивать собственную «частную» цепочку блоков без биткойн-валюты и ее блокчейна. В результате в апреле 2016 года R3 запустил свое решение, названное Corda.

Другой консорциум, созданный в форме содружества проектов, был запущен в декабре 2015 года и получил название Hyperledger. Он был инициирован некоммерческим консорциумом компаний Linux, IBM и Digital Asset Holdings[15]. Вот некоторые из участников, которые объединились в этот проект: Accenture, ANZ Bank, Cisco, CLS, Credits, Deutsche Börse, DTCC, Fujitsu Limited, IC3, IBM, Intel, J. – P. Morgan, London Stock Exchange Group, Mitsubishi UFJ Financial Group, R3, State Street, SWIFT, VMware, Wells Fargo, Сбербанк…

Затем во Франции начали появляться новые варианты развития технологии блокчейна и примеры ее использования: «В ближайшем

будущем мы добьемся большего упорядочения финансового законодательства по кассовым бонам и создадим минибоны[16], чтобы экспериментировать с блокчейном», – заявил Эммануэль Макрон в июне 2016 года. Этот эксперимент, первый в своем роде во Франции, позволяет демократизировать технологию формирования блоков и может стать первым случаем ее применения на государственном уровне.

Таким образом, обещанное светлое будущее под влиянием блокчейна уже выходит за рамки финансов. Похоже, следующей его целью будет страхование, а затем блокчейн постепенно или быстро (история покажет) распространится на все сегменты экономики и общества.

Некоторые области, имеющие потенциал для применения блокчейна

Вот краткий список некоторых областей применения блокчейна[17]:

 Финансы (платежи, проходящие мгновенно и практически бесплатно между двумя сторонами);

 Страхование (микроконтракты, микроплатежи, групповое страхование, более эффективное управление идентификацией клиентов и связанных с ними данных, сертификация происхождения товара);

 Государство (прозрачная и безопасная система голосования, сбор налогов, кадастры);

 Электронная коммерция (простые и безопасные платежи в Интернете);

 Интернет вещей;

 Промышленность (управление подключенными объектами и автономизация объектов для совершения сделок);

 Идентификация отпечатков пальцев;

 Логистика (управление процессами и контрактами посредством алгоритмических процессов);

 Питание (отслеживание информации, относящейся к партии продуктов, от сбора до упаковки);

 Интеллектуальная собственность (статьи, фотографии, музыка, иллюстрации);

 Сделки с недвижимостью в странах, где нет земельного кадастра;

 Аутентификация произведений, предметов, ценностей;

 Обучение (проверка подлинности дипломов);

Здравоохранение (отслеживание медикаментов, обеспечение безопасности медицинских данных, управление данными пациентов);

 Энергетика (умные сети, умные здания, умные города);

 Децентрализованные автобазы.

Таким образом, сообщил Лука Компарини, по мнению IBM, технология блокчейна находится в зачаточном состоянии и еще не соответствует потребностям банковского сектора. Среди основных проблем можно выделить «масштабируемость» и отсутствие конфиденциальности транзакций, что при нынешнем состоянии дел исключает возможность использования блокчейна. Тем не менее, инженеры IBM проанализировали ситуацию и сообщили, что использование блокчейна не ограничивается только банковским сектором, но распространяется «на все

сферы B2B, где IBM занимает ключевые позиции».

Помимо этого, можно добавить еще один важный момент, который должен быть в банковских проектах со множеством участников: во взаимодействии систем должны иметься гарантии, позволяющие гармонизировать сделку. При существующей неоднородности банковских систем этого не происходит.

Глава 2

Блокчейн сегодня

Секрет преобразований заключается в умении сосредоточить свою энергию для создания нового, а не для борьбы со старым.

Дэн Миллман

Теперь рассмотрим различные варианты блокчейна, возникшие один за другим и породившие экосистему, которую мы знаем сегодня. Начнем с блокчейна биткойн и истории его возникновения.

Блокчейн биткойн

Немного истории

Первоначально биткойн являлся улучшением концепции b-money (придуманной Вэй Даем в 1999 году, в которой серверы должны были внести гарантийный взнос в нечетко раскрытый механизм) и технологии bitgold (описанной в 2005 году Ником Сабо[19]и продвигавшей идею использования доказательств на основании расчетов). Но прежде чем продолжить, следует ввести два термина для лучшего понимания следующих разделов.

1. Асимметричная криптография, или шифрование с открытым ключом / закрытым ключом. Это метод шифрования, который противопоставляется симметричной криптографии. Основным принципом асимметричного шифрования является наличие двух ключей (которые пользователь «создает» сам).

2. Распределенная система – это набор автономных объектов вычисления (компьютеры, КПК, процессоры и т. п.), которые связаны между собой и могут сообщаться по сети. Мы могли бы привести в качестве примера физическую сеть машин с несколькими различными процессами, обращающихся к одной и той же машине.

1977–2005 годы: период до появления биткойна и его изобретателя

 1977 год: первое описание шифрования RSA[20], в котором используется открытый ключ для шифрования конфиденциальных данных и закрытый ключ для их расшифровки.

 1979 год: Ральф Меркле[21] изобрел механизм сжатия «дерево

Меркле». Он используется для эффективного и безопасного хранения и проверки больших объемов данных и используется в протоколе биткойн, чтобы вычислить корень Меркле всех операций, содержащихся в блоке данных.

 1990 год: американский математик Дэвид Шаум изобрел DigiCash – электронную валюту (централизованную и собственную) на основе криптографических протоколов.

 1992 год: Скотт Ванстоун (Certicom) предложил алгоритм ECDSA (Elliptic curve digital signature algorithm), который использует более короткие ключи и позволяет выполнять операции подписи и шифрования быстрее, чем RSA.

 1994 год: Ник Сабо выдвинул идею смарт-контракта, или умного договора (см. в этой главе на страницах, посвященных блокчейну Ethereum).

 18 июня 1996 года: NSA публикует доклад под названием «Как производить валюту: криптография анонимных электронных наличных».

 1997: Адам Бэк изобрел HashCash – систему подтверждения выполнения работы на базе идеи, выдвинутой Синтией Дворк и Мони Наором в докладе, опубликованном в 1993 году, Pricing via Processing or Combatting Junk Mail. Позднее Адам Бэк станет первым партнером Сатоси Накамото.

 1998 год: банкротство DigiCash. Вэй Дай выдвигает идею цифровой наличности на основе регистра, распределенного по рассылочной ведомости The Cypherpunks.

 1999 год: Шон Фэннинг в сотрудничестве с Napster изобрел технологию peer to peer (P2P), (равный равному, одноранговую). Платформа обмена аудиофайлами Napster работала с центральным сервером (farm), который играл роль центрального реестра всех файлов, принадлежащих участникам или запрашиваемых ими (равными партнерами). В этой централизованной системе сформировалась единая точка отказа (Single Point of Failure – SPOF) платформы Napster, и сайт был закрыт ФБР в 2001 году за нарушение прав интеллектуальной собственности.

 2000 год: Том Пеппер и Джастин Франкель разработали Gnutella – первую полностью распределенную платформу для передачи данных файлов P2P.

 1998–2005 годы: Ник Сабо разрабатывает проект BitGold – децентрализованную цифровую валюту, основанную на устойчивых к фальсификации цепочках подтверждений о завершении работы, в которой были использованы многие элементы, в конечном счете вошедшие в биткойн: автоматическое проставление даты и времени, электронные подписи, открытые ключи… Однако система оказалась слишком уязвимой для атак.

 2004 год: разработка Ripplepay – попытка создать децентрализованную валютную систему.

2007–2010 годы: появление блокчейна биткойн и его валюты биткойн

Кто такой Сатоси Накамото? Немного истории.

 В 2007 году Сатоси Накамото, таинственная фигура, стоящая за изобретением биткойна, заявил, что он начал работу над этой технологией.

 19 августа 2008 года: Сатоси Накамото зарезервировал доменное имя bitcoin.org.

 31 октября 2008 года: было объявлено о появлении биткойна. Сатоси Накамото опубликовал статью *Bitcoin: A Peer-to-Peer Electronic Cash System,* в которой представил метод решения криптографической задачи, над которой многие бились в течение нескольких десятилетий, – проблемы двойной оплаты, или задачи византийских генералов. Эта проблема мешала двум контрагентам обмениваться активами, в частности деньгами, без участия доверенного лица.

 3 января 2009 года: создается первый блок (исходный блок).

 12 января 2009 года: первая биткойн-транзакция.

 Февраль 2009 года: Сатоси Накамото распространяет первую версию программы Bitcoin на сайте P2P Foundation и создает первые биткойны.

 2009 и 2010 год: Сатоси Накамото разрабатывает и создает биткойн и программное обеспечение Bitcoin-Qt.

 Середина 2010 года: разработчики и сообщество Bitcoin постепенно теряют контакт с Сатоси Накамото.

 12 декабря 2010 года: Накамото написал последнее сообщение на форуме Bitcointalk. Незадолго до исчезновения Накамото назначает Гэвина Андресена преемником, передав ему доступ к проекту Bitcoin на SourceForge и копию аварийного ключа – уникальный личный криптографический ключ, позволяющий смягчить последствия

потенциальной атаки на системы биткойна – например, в случае обнаружения уязвимостей, позволяющих задним числом изменить операции, или захвата более 51 % узлов сети (см. врезку, посвященную этому вопросу, далее). Операторы узлов сети могут при получении предупреждения оповестить своих пользователей либо остановить все регистрации сделок.

Определение

Термин «биткойн» происходит от сокращения двух английских слов: bit – единица информации в двоичном коде и coin – монета. Биткойн одновременно обозначает информационный протокол (биткойн) сети Интернет и единицу расчетов (биткойн), используемую в этой платежной системе.

Блокчейн биткойн – это свободная и открытая технология, работающая в одноранговой сети (peer-to-peer или P2P), без центральной власти (без посредства финансового учреждения). Эта технология позволяет обмениваться объектами (биткойнами или BTC), записывая каждую транзакцию (с автоматической фиксацией даты и времени) в большую бухгалтерскую книгу (ledger), в которой невозможно никакое изменение.

Управление транзакциями и создание биткойнов поддерживаются коллективно сетью, и конструкция этого управления является открытой; никто не владеет и не управляет цепочкой блоков биткойн, и каждый может присоединиться к ней. Благодаря нескольким уникальным свойствам биткойн делает возможными различные перспективные варианты использования, которые не могут быть охвачены современными платежными системами.

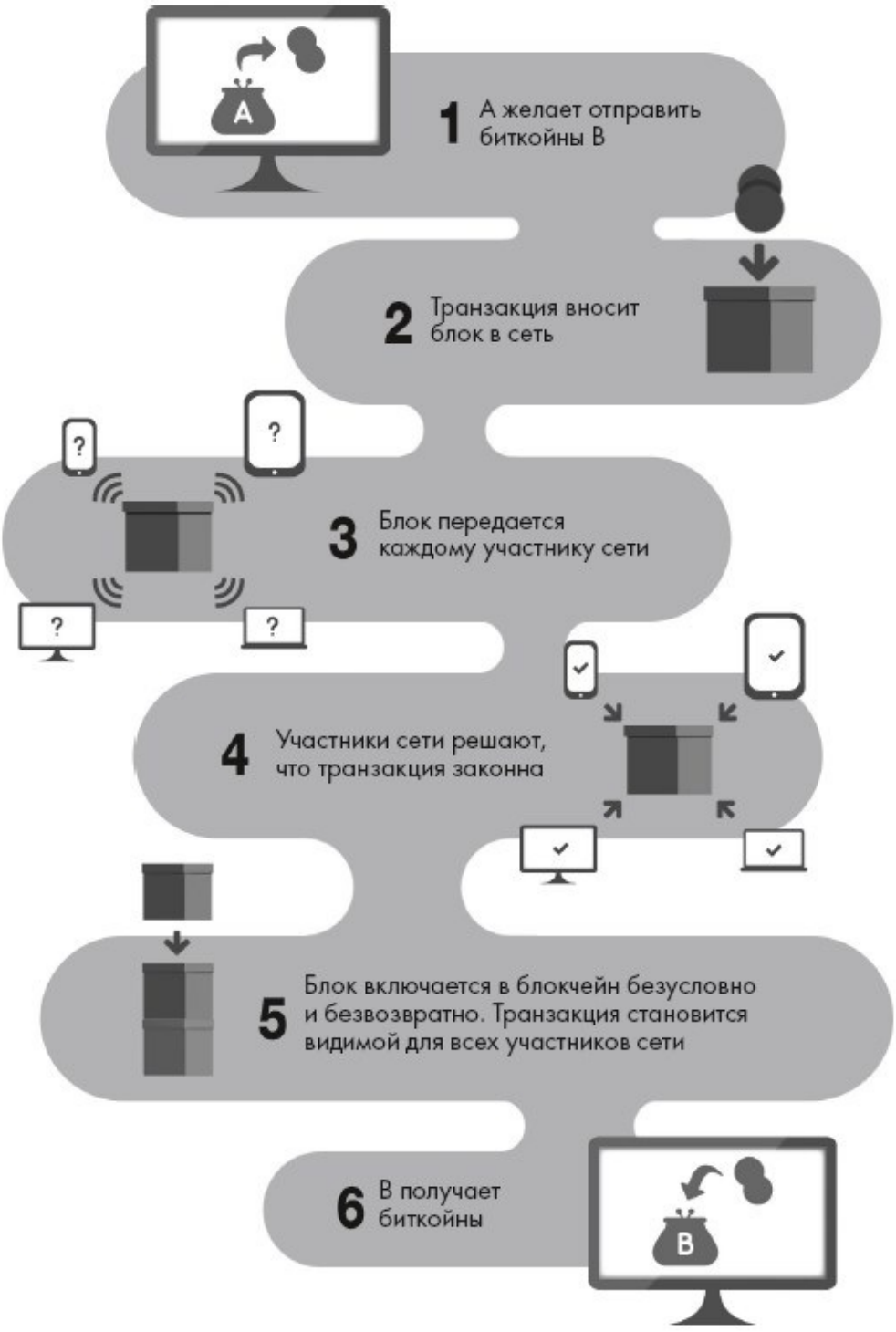
Биткойн-валюта, в отличие от других валют, не является воплощением государственного органа, банка или компании, и каждый биткойн идентифицируется в книге учета при помощи истории всех сделок, в которых он участвует с момента ее создания.

Принцип функционирования

Блокчейн биткойн опирается на криптографический протокол, в частности, для того чтобы:

• с одной стороны, решить проблему, называемую «двойной расход», которая до сих пор мешала появлению такого рода валют (А дает Б, убедившись, что он не дал параллельно С);

• с другой стороны, гарантировать невозможность подделать идентификаторы заинтересованных сторон и ценность биткойнов, содержащихся в электронных кошельках.



Функционирование блокчейна биткойн можно разделить на следующие четыре этапа:

- два участника договариваются о сделке;

• с помощью блокчейна сделка шифруется и утверждается на основе консенсуса (подтверждение выполненной работы / майнинг, см. ниже);

• далее сделка вписывается, а затем блокируется в последнем блоке блокчейна;

• на последнем этапе цепочка блоков реплицируется на всех узлах (участниках) сети.

Доступ к сети

Биткойн – это одноранговая сеть: участники образуют одноранговую сеть, общаясь посредством Интернета. Когда новый компьютер пытается подключиться к сети, его первая задача – найти другие подключенные к ней компьютеры.

После того как компьютер будет подключен, второй шаг – скачать базу данных всех операций, осуществлявшихся с момента запуска проекта, транзакций, заключавшихся в передаче определенного количества биткойнов с одного счета на другой.

Учетная запись идентифицируется биткойн-адресом, который схематически аналогичен номеру счета в банке.

Помимо пунктов обмена валюты, существуют и другие решения, например, платформы для депонирования, односторонние торговые точки и физический обмен в автоматах.

Транзакции

Чтобы стать законной, каждая транзакция должна быть подписана (в криптографическом смысле этого термина) при помощи асимметричного шифрования или шифрования с двойным ключом (открытым и закрытым).

На входе транзакция получает ссылку на предыдущую транзакцию, которая подтверждает тот факт, что упомянутые в сделке средства реальны, а на выходе она производит один или несколько биткойн-адресов с соответствующими приписанными к ним суммами. Входы и выходы любой транзакции всегда сбалансированы.

Тем не менее, эта новая транзакция не сразу определяется как допустимая, так как она должна сначала быть включена в реестр сделок (блоков), который состоит из набора блоков транзакций. Транзакции, переданные в незакодированном виде, признаются действительными при помощи соответствующих закодированных подписей, которые визируют сделку. В настоящее время ежедневное количество таких сделок быстро растет. Например, в июне 2016 года ежедневный объем подобных сделок составлял около 200 тысяч, а в конце ноября 2016 года их число дошло почти до 300 тысяч.

С другой стороны, с позиции числа транзакций в секунду блокчейн биткойн менее эффективен, чем более привычные технологии. Это нередко объясняется тем, что сеть биткойн ограничена в силу своей конструкции. Она способна обработать максимум около семи транзакций в секунду, в то время как максимальная мощность платежной сети Visa составляет 56 тысяч транзакций в секунду.

Кошелек или бумажник

Блокчейн биткойн устроен принципиально иначе, чем банковские учреждения, в которых клиент может иметь несколько счетов со всеми сведениями, касающимися истории каждого счета. Блокчейн хранит след каждой сделки, но в нем нет баланса счета пользователей. Следовательно, действуя подобным образом, восстановить ваши данные невозможно.

Пользователи владеют кошельком или бумажником, который содержит «адреса», связанные с парой ключей, работающих с помощью системы асимметричного шифрования (открытый ключ / закрытый ключ). Обратите внимание, что закрытый ключ хранится в кошельке, а открытый ключ записывается в блокчейне и, следовательно, неприкосновенен. Поэтому, как и в реальной жизни, не следует терять свой кошелек…

Стоимость биткойна

Стоимость биткойна плавает и определяется экономической ситуацией и валютным рынком. Правила организации денежной эмиссии определяются только компьютерным кодом свободного программного обеспечения биткойн.

При создании блокчейна биткойн его создатель Сатоси Накамото записал в протокол (набор правил, которые определяют работу сети), что будет создан всего 21 миллион биткойнов. Этот потолок был установлен в либертарианском духе для предотвращения инфляции стоимости биткойна.

Вот несколько биткойн-единиц:

• 1 биткойн = 1000 миллибиткойнов;

• 1 биткойн = 1000 000 микробиткойнам или битам;

• 1 биткойн = 100 000000 сатоси.

В результате количество биткойнов ограничено 21 миллионом единиц, и каждый биткойн делится до восьмого десятичного знака. Таким образом, наименьшая сумма, которая может быть передана, – 0,00000001 (10-8) биткойна – она названа в сообществе биткойн «сатоси» в честь изобретателя этой валюты.

Обратите внимание, что в период с 3 января 2009 года, когда впервые были задействованы 50 биткойнов в транзакции, фиксирующей временное происхождение всех последующих операций, до конца ноября 2017 года стоимость биткойна выросла почти с 0 до более 8000 долларов США.

Биткойн: майнинг или консенсус

В блокчейне биткойн, чтобы добавить транзакцию и создать новые биткойны, вы должны задействовать консенсус. Это называется майнинг.

Этот процесс предполагает, что отдельные люди будут вознаграждены сетью за свои услуги. Майнеры обрабатывают транзакции и обеспечивают безопасность сети с помощью специализированного оборудования, а в обмен получают новые биткойны.

Таким образом, некоторые пользователи (узлы) используют свои вычислительные мощности (CPU[22]) для того, чтобы верифицировать, сохранять и обеспечивать безопасность транзакций в блокчейне.

Можно определить этот механизм как своего рода «победитель получает все» – это означает, что при каждой сделке тысячи майнеров запускают вычисления, но только один находит решение, которое делает ее действительной.

Таким образом, чтобы быть утвержденным и зарегистрированным в сети, каждый блок должен быть результатом машинного и алгоритмического консенсуса, и этот процесс называется *proof of work* (PoW), или подтверждение выполнения работы. Для сведения: сложность меняется каждые 2016 блоков.

Сеть пытается назначить сложность таким образом, чтобы всемирной вычислительной мощности требовалось ровно 14 дней, чтобы сгенерировать 2016 блоков. Поэтому сложность растет вместе с мощностью сети.

Майнинг – это протокол (алгоритм[23]) распределенного и децентрализованного консенсуса, заключающийся в дешифровке данных или математических вычислений (именно поэтому и говорят о криптовалюте или криптодевизах, так как для того, чтобы их произвести, необходимо пройти процесс дешифровки).

В этот момент нашей демонстрации важно уточнить, что майнеры участвуют не только в верификации транзакций.

Проблема энергопотребления

Биткойн потребляет много энергии. Механизму консенсуса, *proof of work* (доказательству выполнения работы), который наиболее часто используется в существующих системах, для работы требуется очень много электроэнергии; самая важная сеть, биткойн, будет потреблять столько же электроэнергии, сколько, к примеру, потребляет Ирландия.

В течение нескольких лет целый ряд исследователей, а также журналисты и критики блокчейна биткойн, убежденные банковским лобби, заявляли, что майнинг биткойнов является безумной тратой энергии[25]. А что в действительности?

Проблема византийских генералов

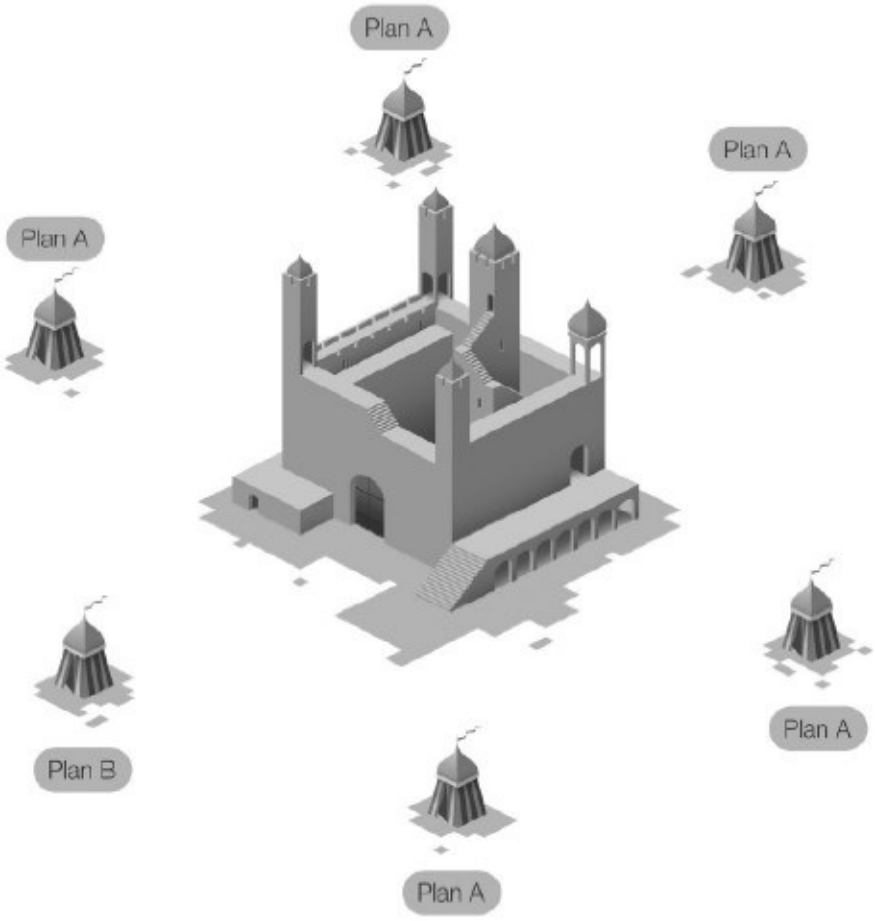
Определение

Проблема, или теория, византийских генералов – это математическая метафора, в которой рассматривается проблема пересмотра безотказности средств связи и целостности собеседников. Речь идет о том, как и в какой степени можно принимать информацию, источник или канал передачи которой выглядит подозрительно.

Чтобы решить эту проблему, мы должны использовать определенные стратегии (в данном случае – алгоритм). Эта проблема впервые была глубоко проработана в статье «Проблема византийских генералов», опубликованной в 1982 году[26].

Блокчейн и проблема византийских генералов

Вот как выглядит проблема: генералы, каждый из которых командует отдельной армией, должны координировать свои действия, чтобы осадить город. Генералы общаются с помощью надежных курьеров, но некоторые из генералов оказались предателями и стремятся к тому, чтобы сорвать план нападения (византийская ошибка, таким образом, представляет собой сбой, заключающийся в предоставлении недостоверной или противоречивой информации). Таким образом, нападение может сорваться, если генералы не придут к консенсусу.



Таким образом, нужно найти алгоритм, чтобы убедиться, что лояльные генералы смогут все же договориться и согласовать план битвы. Следует координировать доверительные отношения с помощью сообщений, написанных и подписанных (без возможности подделки), которые генералы передают друг другу, делясь намерениями со всеми генералами. Таким образом, мы возвращаемся к консенсусу *proof of work.*

Технология блокчейна предоставляет первое и, возможно, единственное решение проблемы византийских генералов. Таким образом, вероятно, впервые в истории человечества удается создать и сохранить реестр, открытый для широкой публики и достаточно безопасный для каждого.

Алгоритм византийских генералов[28]**, или отказоустойчивость**

Устойчивость к византийским сбоям, или *Byzantine Fault Tolerance*

(BFT), – это способность системы продолжать функционировать, в ряде случаев в сокращенном объеме, не выходя полностью из строя, когда часть ее компонентов работает неправильно.

Исторически эту систему отказоустойчивости разработали военные во время холодной войны для обеспечения непрерывной работы сложной замкнутой сети, в данном случае сети ARPA[29].

Говоря языком информатики, поскольку алгоритмы родились не одновременно с технологией блокчейна, а в 1970-х годах, проблема византийских генералов – это абстрактное представление класса программ, активизирующих ряд участников, таких как процессоры в компьютере, компьютеры в сети, роботы на заводе или узлы в цепочке (с блоками или без них).

Таким образом, в области распределенных вычислений, и в частности в блокчейнах, ответные действия на сбои будут обеспечены Paxos[30] и Tendermint[31] – семействами протоколов, позволяющими находить консенсус в сети с ненадежными узлами и, таким образом, способными справляться со сбоями.

Биткойн: майнеры и вознаграждения

В теории все в мире могут быть майнерами, так было при запуске блокчейна. Но на практике при экспоненциальном увеличении числа транзакций майнинг – занятие для предприятий, в основном базирующихся в регионах, где стоимость электроэнергии ниже.

В блокчейне биткойн блок в настоящее время содержит 1000 транзакций с ограничением на размер в 1 мегабайт (средний размер блоков колеблется между 600 и 700 Кб), или около семи транзакций в секунду. Когда майнер собирается подтвердить блок транзакций, он получает 25 новых биткойнов, которые создаются каждые десять минут.

В блокчейне биткойн, существующем с января 2009 года, наградой за решение блока было от 50 биткойнов, но она автоматически уменьшалась в два раза каждые 210 тысяч блоков (около четырех лет): сегодня майнеры получают 12,5 биткойнов за блок с 2021 года 6,75 BTC и т. д.

Сегодня несколько мегапулов (GHASH. IO, Ant-Pool, BW.COM, F2Pool…) имеют монополию на добычу биткойнов. Достаточно посмотреть на сайт blockchain. info в столбце «передано через», чтобы понять, какому пулу удался подвиг получения биткойнов за последние блоки (цифры указаны в процентах).

АТАКА НА 51 %

Атака на 51 % возникает, когда отдельный человек или группа людей контролируют более половины вычислительной мощности, отданной под майнинг. Он (они) может отвергнуть или утвердить сделки, а также и выполнять двойные траты[32]. Действительно, узлы сети (в блокчейне биткойн, например) признают в качестве законной самую длинную цепочку, которая будет написана группой майнеров, обладающей самой большой вычислительной мощностью.

Если бы такая атака состоялась, то, вполне вероятно, что сеть быстро опознала бы этот факт.

В настоящее время большая часть вычислительной мощности, отданной под майнинг, принадлежит пулам (AntPool, F2Pool, BTCC Pool, Bit Fury). Если эти пулы договорятся, они могут осуществить атаку, но они не рискуют делать нечто подобное, потому что в результате пиратства упадет цена валюты, большие запасы которой принадлежат им.

Тем не менее, некоторые криптологи справедливо отмечают, что группа лиц в состоянии взломать несколько пулов и провести атаку.

Такую атаку может провести государство или представитель крупного бизнеса (банк или враждебный хедж-фонд). Действительно, затраты на необходимые вычислительные мощности и энергию для подобной атаки должны быть огромными: в феврале 2016 года общая мощность системы биткойн составила 1,2 миллиона терахешей[33]! Учитывая, что терахеш стоит около 4000 долларов, для получения подобной мощности потребуется не менее 4,8 миллиарда долларов США. И наконец, если безопасность сети была нарушена, существует процедура обработки чрезвычайной ситуации.

Блокчейн и анонимность[34]

Ложные проблемы анонимности

Блокчейн часто критикуют за анонимность. Возможность иметь цифровые децентрализованные деньги или золото привлекает многих субъектов экономики, но опасение открыть дорогу для различных видов незаконной деятельности, на которые распространяется анонимность, справедливо это или нет, тормозит принятие этой технологии.

Рассматривая вопрос под более техническим углом, понимаешь, однако, что опасения могут быть в значительной степени сняты: биткойн не настолько анонимен, как кажется… С одной стороны, если мы не должны обеспечивать подпись информации для создания портфолио или отправки транзакции, то с другой стороны, все, что происходит в цепочке блоков биткойна, прозрачно, что позволяет публично отслеживать все сделки. Таким образом, каждый может создать проводник, отслеживающий данные блокчейна, как это делает, например, сайт blockchain.info (см. раздел «Участники» в конце книги).

Биткойн-адреса сами по себе не связаны с физическим или юридическим лицом. Именно поэтому говорят, что биткойн является анонимным, или, вернее, безымянным. Действительно, в сети биткойн личность пользователя скрыта за криптографическим псевдонимом, который может быть изменен по желанию владельца. Транзакции подписываются псевдонимом и распространяются в общедоступную сеть для проверки их подлинности и назначения биткойнов новому владельцу.

Тем не менее, личность человека может быть связана с биткойн-адресом с помощью других средств. Когда это происходит, можно реконструировать действия этого лица в прошлом, восстанавливая историю блокчейна. Точечное нарушение анонимности индивидуального участника может дойти до выявления всех биткойн-транзакций этого человека.

Если ваш партнер по сделке – частное лицо, которое знает вас, он может попытаться вывести из открытых данных баланс вашего портфеля. Если ваш партнер по сделке – организация (банк, государство, социальная сеть), которой вы обязаны предоставить данные о себе, это еще хуже: она уже все знает о вас, и ее компьютерные средства позволяют сопоставить имеющуюся у нее информацию с вашими «отпечатками пальцев» в блокчейне.

Этой информацией, например, уже владеет сеть, к которой относится ваша банковская карта, но вы не хотите в обязательном порядке делиться ею с теми, кто продал вам последнюю пару кроссовок.

Таким образом, в то время как коллективное сознание упирается в чересчур раздутую проблему анонимности биткойна, специалисты ищут способы сделать блокчейн действительно анонимным.

Это правда, что биткойн не поддерживает процесс Know-Your-Customer (KYC) (который заключается в том, что компания проверяет личность своих клиентов) и что можно открыть столько кошельков, сколько захочется, не оставляя при этом своих личных данных. Но это не значит, что биткойн будет на 100 % анонимным (или, скорее, скрывающим псевдонимы) в повседневной жизни благодаря своей основной функции: отслеживанию данных.

Прослеживаемость и прозрачность

Почти все существующие криптовалюты используют прозрачный блокчейн, и только малая часть проектов старается сделать его непрозрачным. Например, Dash[35], в отличие от биткойна, использует архитектуру клиент-сервер, которая работает, используя принцип *proof of work* (подтверждение выполнения работы) так же, как и биткойн, и делает заключения в режиме *proof of stake* (с защитой по методу «подтверждение доли»), создавая подсети, состоящие из специальных серверов (mastemodes), которые обеспечивают дополнительные функциональные возможности вроде моментальных проводок, в том числе поддерживают частные сделки (darksend). Основная идея заключается в том, что операции становятся непрозрачными путем перемешивания денег, которые направляются на masternodes. Dash – это просто более анонимный

биткойн, но и он не в состоянии обеспечить полную непрозрачность.

Zerocoin[36], а затем ZeroCash Project[37] – это еще один проект подобного рода. Его идея заключается в том, чтобы отправлять биткойны в сеть Zerocoin, а затем получать их обратно, анонимизируя с помощью протокола. Эта идея впоследствии развилась в Zcash[38] – валюту, которая позволяет осуществлять сделки на прозрачной основе с возможностью сделать их анонимными перед платежом за счет перехода через внутреннюю собирательную схему, разновидность blackbox (черного ящика), которая обеспечит непрозрачность. Zcash основана на криптографической схеме, носящей название *zero-knowledge proof.*

Проект Monero

В области полной анонимизации наиболее успешным проектом на сегодняшний день является Monero[39].

У Monero (что означает «валюта» на эсперанто) есть два основных свойства:

• он позволяет отправлять и получать денежные средства без того, чтобы транзакции были видны всем;

• он создает неопределенность, что делает практически невозможным отслеживание потраченных средств.

Протокол Monero использует метод одноразовой кольцевой подписи (*one-time ring signatures),* очень мощную технологию достижения анонимности, позволяющую полностью скрыть транзакцию.

При формировании транзакции случайным образом выбирается цепочка других блоков, которые подписываются по кольцу, чтобы создать цифровой отпечаток пальцев для публикации. Этот отпечаток, характеризующий транзакцию, называется key-image (ключевое изображение). Эта хитрость прячет от наблюдателей подлинную подпись, гарантируя, что сделка, несомненно, законна и что она не является мошенничеством.

С помощью ключей view-keys также невозможно идентифицировать

получателя платежа. Транзакция отправляется не с помощью открытого ключа, но на адрес, который будет использован лишь один раз. Только получатель, имеющий в своем распоряжении правильный view-key (ключ для просмотра), имеет право на чтение транзакции, которая ему предназначена.

В блокчейне медленно, но верно деньги приводят к переменам.

Остается узнать, как будет реагировать регулирующий орган, учитывая, что биткойн работает с 2009 года без полноценного учета законов той страны, где он используется. Что произойдет, если валютная система вроде Monero распространится по всему миру? Сейчас ее капитализация превышает 100 миллионов долларов – капля в море в рамках мировой экономики. Но стоит знать, что весной 2016 года Microsoft интегрировала эту систему в свой сервис BaaS (Blockchain-as-a-service).

Само собой разумеется, что Monero, как и биткойн, может гарантировать анонимность пользователю только до тех пор, пока он остается внутри системы. Если бы в мире не было никакой другой валюты, кроме Monero, все платежи были бы анонимными. И напротив, с каждым использованием Monero для обмена с другими прозрачными валютными системами (fiat или crypto) все возвращается на уровень конфиденциальности, принятый в этой валютной системе. Если кто-то хочет оставаться анонимным, ему не стоит выходить из системы Monero.

На основе этой информации вы можете понять, что дилер, который хотел бы поместить незаконно полученные деньги в криптовалютную систему, несколько раз подумает, прежде чем сделать это. И после принятия окончательного решения есть вероятность, что он не сможет спать спокойно: в самом деле, как он собирается вывести свои деньги из системы, если ему достаточно перевести небольшую сумму на банковский счет, и он тут же оставит след на сервере в той или иной части земного шара?

Развитие, масштабируемость

Масштабируемость – это способность системы адаптироваться к изменению масштаба, в частности способность поддерживать свои функции и производительность в случае большого спроса… Проблемой для некоторых «классических» блокчейнов является экспоненциальный рост ресурсов – технических, экономических, энергетических, – необходимых для выполнения конкретных задач. Пример: beAchain с его специфическим протоколом на основе консенсуса/ проверки – на 100 % масштабируемый.

А что насчет масштабируемости блокчейна биткойн и его эволюции?

Читая о технических возможностях блокчейна биткойн, мы отлично понимаем, что имеем дело с отказоустойчивой технологией, которая сегодня доказала свою надежность и очень широко распространена в мире. Что нужно сделать, чтобы мы могли планировать все более разнообразные варианты ее использования, сохраняя присущую ей результативность? Как осуществить множество микроплатежей, не нарушая работы системы? Как улучшить время отклика, если мы предполагаем возможность проведения тысяч транзакций, по примеру того, что делают, например, операторы при оплате банковской картой[40]?

Исходя из этих вопросов и, следовательно, возникающих в связи с ними проблем, мы видим пять вариантов решений:

- альткойны;
- увеличение размера блоков транзакций;
- «боковые цепи» или коллатеральные цепи;
- Lightning Network;
- «клиентские базы данных» или базы данных блокчейна.

Альткойны[41] **или «альтернативные криптовалюты»**

На сегодняшний день существует более 700 криптовалют[42], которые опираются на собственный блокчейн, биткойн или эфириум, и каждая из них специализируется на особом сервисе или функции.

По состоянию на конец 2017 года общее число криптовалют (или виртуальных валют) превысило 1300[43].

Ниже приводится рейтинг первых десяти криптовалют на конец ноября 2017 года (источник CoinMarketCap).

	Наименование	Обозначение
1	Bitcoin	BTC
2	Ethereum	ETH
3	Bitcoin Cash	BCH
4	Ripple	XRP
5	Dash	DASH
6	Litecoin	LTC
7	IOTA	MIOTA
8	NEO	NEO
9	Monero	XMR
10	NEM	XEM

Сайт CoinMarketCap.com позволяет отслеживать рынок криптовалют и показывает, что капитал этих валютных систем остается в итоге меньшим, чем общий объем международной торговли в иностранной валюте fiat[44] (в валютных системах под эгидой государства).

Различные криптовалютные системы

Среди различных криптовалютных систем необходимо упомянуть следующие.

 Litecoin[45] – шестая криптовалютная система с точки зрения капитализации, капитал более 3,8 миллиардов долларов.

 Namecoin[46], предоставляющая возможность создания децентрализованных сетей с доменными именами, основанная на технологии блокчейн. Одной из целей Namecoin является создание системы адресов для компьютеров, подключенных к сети Интернет, которая может заменить нынешнюю систему DNS (Domain Name System), принадлежащую в основном американским организациям. В ней принят принцип «первый пришел, первый обслужился», где первая запись проходит успешно, а вторая нет, – задача отлично подходит для протокола консенсуса биткойна. Namecoin является реализацией старейшей и самой успешной системы записи имен, основанной на этой идее.

 OneCoin[47] – это первая и единственная криптовалютная система в мире, хранящая в своих блоках документы Know-Your-Customer (KYC) в целях обеспечения полной прозрачности операций. За два года (2014–2016) OneCoin стала одной из самых значимых виртуальных валютных систем на рынке и стремится стать первой криптовалютной системой в мире. В дополнение к созданию стабильной валюты в соответствии со всеми нормами OneCoin создала экосистему вокруг своей валюты с целью повышения частоты и удобства ее использования.

 Криптовалютные системы сообществ, такие как Potcoin[48] и Mazacoin[49].

 Весьмаперспективные проекты вроде BitShares[50], Dash[51] (бывший Darkcoin), Blackcoin[52], Viacoin[53], совсем недавно появившийся Zcash[54] и т. д.

CONSCOIN, КРИПТОВАЛЮТНАЯ ЭТИКА С ДОБАВЛЕНИЕМ СОЗНАТЕЛЬНОСТИ

У этой криптовалюты сильные козыри. По сути, Сопбсою – это независимая криптовалюта с этикой и руководством и ничего более.

В конце 2015 года группа исследователей из Университета Джорджтауна в Вашингтоне выпустила документ[55] с предложением ввести новую криптовалюту, которая использует искусственный интеллект (ИИ, или AI) для разработки валютной системы, имеющей предопределенную группу этических принципов для управления своими расходами.

Они указывают, что криптовалюты, такие как биткойн, предлагают новые пути расширения экономических прав и возможностей людей во всем мире[56]. Да, конечно, эти валюты также обеспечивают мощный инструмент, способствующий развитию преступной деятельности, и приносят много вреда людям и сообществам. Но, заявили защитники криптовалют, этические ценности криптовалют не являются чем-то качественно новым, поскольку деньги всегда воспринимались как пассивный инструмент, не связанный с этическими ценностями, и могли использоваться как в хороших, так и в дурных целях.

Группа исследователей оспаривает предположение о том, что деньги должны иметь нейтральную ценность. Действительно, с появлением искусственного интеллекта, криптографии и машин с заложенной этикой криптовалюты с искусственным разумом, которые не являются этически нейтральными, а самостоятельно регулируют правила их использования, уже не кажутся абсурдом.

Для достижения такого результата эти исследователи предлагают установить технологические основы подобных криптовалют, а затем проанализировать правовые последствия, этические и экономические, их использования.

Эти автономные и управляемые криптовалюты (Autonomous Ethically Guided Cryptocurrency, AEGC) представляют собой приложение, которое включает в себя две отличительные черты:

• наличие определенной формы искусственного интеллекта, который позволяет контролировать окружающую среду, собирать и анализировать информацию и принимать самостоятельные решения, ориентируясь на заложенные этические принципы;

• функционирование в качестве криптовалютной системы, которая может быть охарактеризована как средство обмена и жетон (token) для хранения ценности.

Объединяя технологию блокчейна с особой формой искусственного интеллекта, можно разработать криптовалютную систему, которая может оценивать обстоятельства, связанные с определенной финансовой операцией, в которой человек – владелец криптовалюты – будет участвовать и формулировать решение, определяющее, разрешить или нет использование его криптовалюты в сделке.

Во время процесса определения, является ли сделка разрешенной, программное обеспечение искусственного интеллекта криптовалютной системы не интересуется финансовыми аспектами сделки. Вместо этого оно анализирует и определяет этический контекст транзакции с целью дать свое заключение о сделке.

Это нововведение может увести нас далеко от «умных данных» (smart data) в область «разумных данных» (sapient data). Таким образом, возникает криптовалютная система, полностью «приклеенная» к своему обладателю и его ценностям. Есть о чем задуматься.

Colored Coins (вариант биткойнов) («Окрашенные монеты»)

Принцип Colored Coins[57] – «раскрасить» некоторые биткойны, находящиеся в обращении, и назначить им определенные свойства, значение которых может отличаться от базовых свойств биткойна. Colored Coins – это протокол биткойн 2.0 с открытым исходным кодом и система, разделенная на два уровня:

• уже известная нам система биткойн;

• автономная, но зависимая от протокола биткойн сеть.

Это разделение позволяет выпускать инструменты обмена, отдельные от сети биткойн. Это «протокол в протоколе», который может быть использован в инфраструктуре и сети Bitcoin как альтернативная валюта, производный продукт, акции или облигации или даже интеллектуальная собственность.

Можно представить себе создание на базе этих Colored Coins независимых и децентрализованных фондов социального обеспечения, управляемых принявшим их сообществом.

Counterparty[58] (вариант bitcoin)

Counterparty – это платформа и портфолио, построенные поверх блокчейна биткойн, которые позволяют создавать активы посредством токенизации[59].

Counterparty имеет собственную валюту под названием XCP. Эта валюта используется для обмена товарами, а также для создания умных контрактов, которые обращаются на платформе за плату в XCP. Это делимые и программируемые активы, в процессе выполнения умных контрактов они могут быть переправлены с одного адреса на другой. В целом Counterparty – это эквивалент платформы эфириум, но с использованием блокчейна биткойн.

Увеличение размеров блоков транзакций

В настоящее время сеть биткойн обрабатывает около 160 тысяч транзакций в день, и блоки заполнены в среднем на 50 %, или 0,5 Мб. В таком случае довольно быстро достигаются пики активности, и все сделки, даже дешевые, в конечном счете будут валидированы. Однако если биткойн будет продолжать расти текущими темпами, вполне возможно, что в следующем году будет достигнуто ограничение в 1 Мб. С этого момента пользователи будут конкурировать за расходы, которые они выплачивают майнерам, и сделки, не имеющие цены или недорогие, больше не будут валидироваться.

Проблема в том, что, согласно этому сценарию, сеть биткойн, в конечном счете, будет обрабатывать только очень крупные сделки с высокой ценностью (в абсолютном выражении, но слабые относительно суммы) и, например, в сети могут начать развиваться компенсации между компаниями.

Так как же ограничить риск большой централизации и, следовательно, ослабления сети?

Между желанием увеличить размер блоков и переходом к его осуществлению есть разрыв, который трудно преодолеть. Действительно, «мудрецы» цепочки блокчейна биткойн не всегда приходят к консенсусу, когда речь идет о пересмотре кода протокола, что оставляет эту проблему пока нерешенной.

Боковые цепочки и коллатеральные цепи

Не создают ли альткойны проблемы уязвимости или неустойчивости? Обсуждение остается открытым, но основные вопросы те же, что возникают при обсуждении блокчейна биткойн.

В действительности основная техническая проблема – это взаимодействие с существующими системами и, потенциально, между различными сетями блокчейнов. Как эти *регистры* могут взаимодействовать, если они построены отдельно для различных типов активов и работают согласно технологии инфраструктуры существующего рынка?

Именно это говорил о блокчейне биткойн Адам Бэк[61], изобретатель HashCash[62]*(proof of work[63]),* один из основателей Blockstream[64].

По сути, он считает, что эволюция блокчейна биткойн может происходить лишь очень медленно в силу принятых для его развития решений. Эти решения зависят от процесса, требующего согласия, которого трудно добиться от тех, кто трудится для его обслуживания и не организован в иерархическую структуру. Это, кстати, проблема, постоянно возникающая с полностью децентрализованными приложениями, которые вследствие своей природы не контролируются людьми.

Учтя это замечание и собрав команду исследователей, Адам Бэк разработал метод привязки блокчейнов друг к другу – систему «боковых цепочек» (*sidechoin*), для которой в 2014 году была опубликована «белая книга»[65].

В действительности, система боковых цепей позволит переносить объекты цепи А в цепь В. Они исчезнут из цепи А, чтобы появиться в цепи В, и могли бы в принципе вернуться в цепь А.

Lightning Network[68]

Блокчейн биткойн очень перспективен с точки зрения распределенных бухгалтерских книг, но как платформа для оплаты сегодня он не может выполнять операции мировой торговли.

Поэтому его качества также являются и тормозом для его расширения. Действительно, все изменения в рамках гроссбуха распространяются по набору узлов (участников) – это означает, что каждый узел сети биткойн будет знать обо всех операциях, которые происходят на глобальном уровне, что автоматически становится огромным тормозом, влияющим на время отклика сети.

Отсюда возникает идея создания параллельной системы, охватывающей все сделки таким образом, чтобы не приходилось жертвовать децентрализацией и безопасностью, которые дает сеть биткойн.

Эта новая система микроплатежей на биткойне была создана по инициативе компании Blockstream, которая сотрудничает с лидерами отрасли – Lightning Network. Она возьмет на себя большие объемы микроплатежей (внедрение этого решения изменит ограничение на количество транзакций в секунду с 7 до более 7000) посредством использования почти нулевых расходов на транзакции и работая со скоростью «молнии». Первый «драфт» появился в феврале 2015 года, а «белая книга» была опубликована в январе 2016 года[69].

На сегодняшний день существует четыре реализации Lightning (источник Bitcoin.fr):

 Lightning Corp (авторы) и Bitfury[70] (нет собственных реализованных проектов, но сотрудничают с LN Corp.);

 Blockstream;

 Blockchain.info;

 Lightning ACINQ[71].

«Белая книга» Bitfury[72]

Эта «белая книга» под названием «Flare: An Approach to Routing in Lightning Network» посвящена Flare, алгоритму гибридной маршрутизации платежей на Lightning Network.

Bitfury предлагает двухэтапный алгоритм:

• упреждающее обновление карты маршрутизации узла, который хранит информацию о топологии сети;

• оперативный сбор информации в зависимости от потребностей по запросу от Lightning Network.

Этот документ является первой попыткой описать и проверить предварительно алгоритмическое решение для будущей реализации Lightning Network на блокчейне биткойн, который позволит осуществить приспособляемость процесса обработки транзакций.

«Боковые базы данных» или блокчейн баз данных

Так же как существующие боковые цепи были созданы для того, чтобы улучшить время отклика ранее созданных блокчейнов, теперь есть базы данных, которые позволяют повысить скорость передачи и обработки данных: назовем их, используя тот же неологизм, «боковыми базами данных».

В действительности, если оценивать производительность блокчейна биткойн с точки зрения традиционных критериев баз данных, результат получается просто катастрофический:

• пропускная способность (дебет) составляет всего несколько сделок в секунду (tps);

• временной промежуток перед тем, как осуществится операция записи, составляет десять минут;

• емкость порядка нескольких десятков гигабайт (GB);

• отсутствие линейной масштабируемости при добавлении узлов: с удвоением числа узлов

сетевой трафик возрастает в четыре раза без заметного уменьшения производительности, задержки или пропускной способности сети;

• добавление узлов выполняется правильно примерно до 10 тысяч единиц, потом производительность падает;

• нет возможности выполнить запрос *(query)* данных с использованием SQL или без.

Похоже, что BigchainDB[73] нашла решение, способное улучшить эти

показатели.

BigchainDB – это база данных, масштабируемая и совместимая с биткойном, эфириумом, Chain, Eris и т. д. Она заняла свою нишу, позиционируя себя как мост между блокчейном и системой хранения данных.

Но, даже оставляя в стороне внешний вид блокчейна, BigchainDB предлагает множество функций, отсутствующих в NoSQL и распределенных базах данных. Только одно это – уже веская причина использовать BigchainDB в большинстве случаев. Более того, система настроек позволяет создавать конфигурации, которые подходят как для частных, так и для общедоступных блокчейнов.

Тем не менее на этом мы закончим обзор новых решений, возникающих для того, чтобы компенсировать некоторые недостатки старого блокчейна или ускорить его работу.

Блокчейн эфириум

Невозможно говорить о блокчейне и не упомянуть эфириум (Ethereum), который часто выступает по отношению к биткойну, как Bitcoin 2.0 к предшествующему ему биткойну, или «биткойн – к Steroids».

Немного истории

Создателем эфириума является Виталик Бутерин[76]. Впервые он открыл для себя технологию блокчейн и реализацию криптовалютных систем посредством биткойна в 2011 году и сразу же оценил эту технологию и ее потенциал. В сентябре 2011 года он стал соучредителем Bitcoin Magazine и после двух с половиной лет размышлений о технологии и существующих приложениях в ноябре 2013 года опубликовал свою идею в виде «Белой книги»[77].

Виталик Бутерин считает, что блокчейн – технология, лежащая в основе биткойн, – способен на большее, чем просто перемещать деньги из точки А в точку В. По его мнению, Сатоси Накамото предназначил блокчейну биткойн только функцию проведения денежных операций и даже при внесении определенных исправлений этот блокчейн не способен ни на что большее.

Бутерин пишет, что блокчейн биткойн сравним с протоколом SMTP (Simple Mail Transfer Protocol) и отлично подходит для конкретной задачи передачи денег, но он не был задуман в качестве фундаментальной оболочки, на которой можно выстроить любой тип протокола.

В начале 2014 года он выпускает в предварительную продажу первые ethers[78] для того, чтобы приобрести необходимые средства для развития проекта (он получает около 18 миллионов долларов). 30 июля 2015 года была опубликована Frontier – первая версия Ethereum. Создан исходный блокчейн[79].

Сейчас Бутерин работает в составе научно-исследовательской группы Ethereum, которая прорабатывает будущие версии протокола Ethereum.

Хронология версий

2013 год

 Ноябрь: публикация «Белой книги».

2014 год

 1 февраля: подтверждение концепции (PoC) 1;

 20 февраля: PoC2;

 1 марта: PoC3;

 9 апреля: PoC5;

 с 22 июля по 2 сентября: продажа эфиров;

 5 октября: PoCб.

2015 год

 13 января: PoC7;

 24 февраля: PoC8;

 9 мая: Olympic;

 30 июля: Frontier.

2016 год

 13 февраля: 1000 000 блоков;

 4 марта: Homestead – стабильная версия;

 Проект: Metropolis;

 Проект: Serenity;

 Проект: Ethereum 2.0;

 Проект: Ethereum 3.0.

Определение

Как и блокчейн биткойн, Ethereum – это публичный блокчейн, особенностью которого является возможность создания пользователями умных контрактов благодаря языку, полному по Тьюрингу. Создаваемые контракты основаны на протоколе, относящемся к информационным технологиям и позволяющем осуществлять проверку или обеспечивать выполнение двустороннего договора. Эти контракты разворачиваемы и доступны для публичного обсуждения внутри блокчейна.

Майнинг

Как и протокол биткойн, Ethereum обращается к майнингу с *proof of work.* Вместе с тем протокол Ethereum планирует в ближайшее время переключиться с современного майнинга с *proof of work* (Frontier) на майнинг с *proof of stoke*[81].

Валюта

Ethereum использует в качестве оплаты контрактов расчетную единицу, которая называется эфир (ether). Его аббревиатура, используемая в системе обмена валют, – ETH. Эфир – это вторая по значимости криптографическая децентрализованная валюта после биткойна, с капиталом более 1,6 миллиарда долларов[82].

Покупка эфира

Существует два способа покупки эфира:

• купить эфир, предъявив удостоверение личности, на какой-либо платформе (см. список в конце книги);

• обменять биткойны или другую криптовалюту на эфир.

Первый вариант быстрее, но дороже. Нужно войти в платформу

(например, Coinhouse[83]), с помощью которой вы сможете купить эфир. Как правило, для создания учетной записи, проверки личности и выполнения транзакций будет достаточно нескольких часов. С другой стороны, при этом отчисляется комиссия от б до 10 %.

Второй вариант является более длительным, но менее затратным. Надо войти в платформу, где осуществляется обмен (например, Kraken), а затем выполнить перевод со своего банковского счета на эту платформу для того, чтобы купить биткойны, а затем обменять биткойны на эфир.

Функционирование

Можно рассматривать Ethereum как всемирный компьютер (состоящий из тысяч компьютеров), раскинувшийся по всей земле, к которому каждый может получить доступ. Его вычислительная мощность поступает от майнеров, услуги которых оплачиваются «газом».

В обмен на вознаграждение майнеры совместно выполняют необходимые операции (проверка, добавление данных, выполнение *умных контрактов*) для функционирования блокчейна Ethereum. «Газ» можно обменять на эфир, который затем может быть обменен на валюту без наценки на торговых платформах.

Таким образом, в блокчейне Ethereum можно хранить все, что вам будет нужно, даже код. Этот блокчейн находится в распоряжении частных лиц, профессионалов, которые могут свободно его использовать.

Ethereum отличается от других блокчейнов наличием умных контрактов (*smart contracts*) и DAO *(decentralized autonomous organizations*, децентрализованных автономных организаций).

Эта система позволяет сократить число судебных разбирательств, а также делает управление бизнесом более удобным. В этой системе не нужно доверять ни партнеру, ни центральной власти. Эта компьютерная система полностью автоматизирована, что гарантирует честность сделки.

Умные контракты DAO

Умные контракты

Ник Сабо, специалист в области криптографии, создатель сети, предшествовавшей биткойну, – она называлась BitGold, – а кроме того, подозревавшийся в том, что именно он изобрел биткойн, придумал название и разработал концепцию умных контрактов[84] в 1994 году. По сути, он хотел организовать автоматическую связь умных контрактов со сделками в области электронной торговли между людьми, неуверенно владеющими Интернетом[85].

Умные контракты – это компьютерные программы, которые регистрируют и/или выполняют условия договора, характеристики которого были предварительно четко определены, когда срок его действия подходит к концу (финансовые кредиты, выпуск акций, голосование, брачный договор, контракт…)[86].

Цель умного контракта заключается в выполнении условий договора, таких как оплата и поставки, а также в соблюдении конфиденциальности и выполнении взаимных обязательств. Теоретически цифровой и автоматизированный характер договора позволяет двум партнерам наладить деловые отношения без необходимости доверять друг другу с самого начала, причем без участия централизованных третьих лиц или властей. Сама система, а не ее сотрудники, гарантирует честность сделки. Таков смысл проекта Ethereum, который позволяет создавать крупномасштабные умные контракты[87], используя нематериальный метод проверки партнера. При этом проверка может быть проведена непосредственно участниками, имеющими равные права, и без использования дополнительных правовых инструментов.

В блокчейне эту функцию выполняют программы, которые доступны для всех уполномоченных сторон, их выполнение в любой момент может быть проконтролировано. Эти программы автоматически выполняют

условия договора, как только определенные элементы объединяются.

Эти умные контракты делают блокчейн надежнее: в рамках договора страхования, если условия уплаты соблюдены, контракт выполняется и сделка совершается. Благодаря умным контрактам блокчейн не ограничивается только хранением информации!

Умные контракты позволяют записывать информацию в условиях полной защищенности, соединяя между собой все части договора. Таким образом, благодаря блокчейну, договор имеет датированное, неопровержимое и защищенное от подделок подтверждение.

Важно отметить, что умные контракты – это палка о двух концах. Действительно, неизменность желательна, но в случае ошибки в написании кода контракта будет невозможно вернуться назад.

В Ethereum каждый умный контракт входит в блокчейн с помощью специального языка Solidity[88]. Solidity – это язык высокого уровня, синтаксис которого напоминает JavaScript. Он был разработан для того, чтобы компилировать код для виртуальных машин Ethereum[89]. Будучи полным по Тьюрингу языком, Solidity позволяет писать как простые, так и довольно сложные программы.

В отношении умного контракта, условия выполнения которого связаны с временными индикаторами или записями в цепочке блоков, проверка осуществляется автоматически. И напротив, в случае, если нужно проверить некие внешние условия (например, получение груза), следует обратиться к доверенной третьей стороне, Oracle на жаргоне Ethereum. Oracle может быть третьим лицом для обеих сторон, доверительным учреждением / ассоциацией или консенсусом нескольких сторонних объектов (проект Oraclize[90]).

Исполнение договора потребует «газ» (стоимостью порядка евроцента для простого договора до нескольких евро для сложного контракта).

В этой обширной области умных контрактов основная задача заключается в том, как привязать декретный договор (имеющий отношение к юридической стороне вопроса) и зашифрованный договор в

блокчейне.

DAO (decentralized autonomous organization)

Принцип

DAO – это сокращение от слов «decentralized autonomous organization», или «децентрализованная автономная организация»[92]. Как указывает название, это автономная организация (без центрального органа управления), функционирующая благодаря одному или нескольким умным контрактам, которые приносят в сообщество прозрачные правила управления и безопасного обмена. Это то, что иногда называют системой управления 2.0 (например, Bitnation[93]) или системой долевого управления.

Отметим, что, хотя в настоящее время DAO плавают в правовом вакууме, законы о них, как ожидается, появятся в ближайшем будущем. Действительно, при текущем состоянии вещей в определенных ситуациях DAO весьма уязвимы. Например, если DAO доверяет свои средства исполнителю – поставщику, который не выполняет условия договора (в умном контракте пока не хватает механизма контроля за связью DAO и поставщика услуги), – DAO не может выдвинуть против него юридические обвинения. DAO не имеет никакого юридического статуса, и в этом качестве договор между DAO и поставщиком не имеет никакого значения.

Это только один пример ограничений DAO. Эта новая форма организации возникла совсем недавно, и она будет развиваться, чтобы обеспечить оптимальное использование этого механизма.

Анализ Тибо Вербьеста[95]

Атака на The DAO, или Слабые места системы

Напомним факты: проект The DAO, запущенный сообществом, организованным в основном вокруг стартапа Slock.it 16 мая 2016 года,

начал широкую кампанию по сбору средств. В течение четырех недель им удалось собрать более 120 миллионов долларов.

17 июня 2016 года The DAO оказалась жертвой крупномасштабной атаки, которая привела к прекращению ее разработки.

Редактируемый блокчейн – утопия или реальность?

Хакерская атака на The DAO показала необходимость возможности изменений в частных (или эксклюзивных) системах блокчейнов. Что же касается технологии «обычного» блокчейна, если кто-то пытается внести изменения в блок, он «ломает математику» или цепочку алгоритмов, поддерживающую всю совокупность блоков. За исключением ситуации, когда участники принимают изменения, система выполняет отказ, оставляя блокчейн в прежнем виде и создавая отслеживаемое подтверждение манипуляции. Если достаточное число участников соглашается с необходимостью внесения изменений, то можно добавить *fork* (как это произошло в Ethereum в июле 2016 года), при этом ветвь заканчивается там, где находится неисправный блок, а другая ветвь продолжается после исправленного блока. После того как блок был исправлен, необходимо восстановить все последующие блоки. Это может быть разрушительным и очень дорогим способом, а в некоторых случаях практически невыполнимым.

Вот почему в сентябре 2016 года был создан Accenture – прототип новой функции, которая позволяет технологии блокчейн работать в чрезвычайных обстоятельствах и устранять человеческие ошибки с учетом правовых и нормативных требований, сохраняя при этом обеспечение криптографии. Этот прототип, по данным Accenture, представляет собой значительный шаг вперед в использовании технологии блокчейн, в том числе в банковском секторе, в области страхования и капиталов. Таким образом, речь идет о модифицируемом блокчейне[98] – то есть о том, что идет вразрез с основными принципами самого блокчейна.

Протокол консенсуса в распределенных сетях

Определение

Как уже говорилось раньше, термин *distributed ledger*– распределенный регистр (или распределенная главная бухгалтерская книга) – начал распространяться во многих сообществах блокчейнов и в специализированных изданиях для того, чтобы отличать публичные, или исторические, блокчейны (биткойн, эфириум) от новых блокчейнов (частных или гибридных), а следовательно и более современных по своей конструкции и более гибких в использовании.

Но сам термин «блокчейн» – подходит ли он для публичного блокчейна?

Продвинемся немного дальше в своих рассуждениях и, если хотите, рассмотрим здесь один момент, который мне кажется ключевым для понимания пространства блокчейнов и формирующих его технологий.

Когда мы говорим о блоках и цепочках блоков, не подразумеваем ли мы одно и то же?

Мы знаем, что блокчейн – это структура данных в виде «цепочки блоков», но это связывание в цепь на самом деле лишь часть распределенного протокола реестра. Следовательно, в более широком смысле будет более логично назвать эти технологические платформы, эти блокчейны, «распределенными протоколами реестра» (с открытым или закрытым реестром).

Ключевой аспект открытого распределенного реестра – это характер распределения данных и эффективность алгоритма консенсуса,

устанавливающего истинность транзакций, зарегистрированных в различных узлах сети. Именно на основании этого алгоритма была выведена большая часть свойств распределенного реестра.

Вот почему в широком смысле мы считаем, что было бы желательно назвать блокчейны «распространенными протоколами консенсуса».

Вот компоненты распределенного протокола консенсуса:

• жетоны *(token)* (например, криптографическая валюта, такая как биткойн);

• механизм консенсуса (например, *proof of work,* или подтверждение выполнения работы);

• структура (например, блокчейн);

• сеть участников (узлов);

• набор правил (например, протокол Ripple).

Теперь, когда мы познакомились с биткойном, эфириумом и публичными блокчейнами, давайте рассмотрим различные типы блокчейнов.

Типы блокчейнов

Вопрос, является ли блокчейн публичным или частным, не нов. Но он снова стал актуальным после того, как финансовые учреждения и банки, в том числе и центральные, заинтересовались технологией блокчейна с тем, чтобы поэкспериментировать с полностью частными приложениями.

Блокчейн публичный или блокчейн частный[99]

Публичный блокчейн, или Исторический блокчейн

Это реестр *(ledger),* открытый для всех. Этот блокчейн характеризуется полной открытостью: каждый может получить к нему доступ и выполнять разнообразные операции, и каждый может участвовать в процессе достижения консенсуса.

Вследствие этого в данном типе блокчейна нет никакого центрального реестра или доверенного третьего лица. Это самый известный тип блокчейна, который лежит в основе данной технологии и соответствует современной экономике. Некоторые считают, что при упоминании этой технологии следует употреблять только единственное число – мы, таким образом, говорим о блокчейне. Его действие основано на «криптоэкономике»[100], то есть на сочетании экономических стимулов и механизмов верификации с использованием криптографии в качестве доказательства выполнения работы (РоЛ) или доказательства участия (РоБ). Публичный блокчейн по своей природе полностью децентрализован.

Блокчейн консорциума, или Гибридный блокчейн

Здесь процесс консенсуса контролируется совокупностью предварительно выбранных узлов (участников).

Можно представить себе, например, консорциум из 15 финансовых учреждений, каждое из которых управляет узлом, и из них по крайней

мере 10 должны подписать каждый блок для того, чтобы этот блок считался легитимным. Доступ к этому блокчейну может быть публичным, а возможно, число участников будет ограниченным. Эти блокчейны могут рассматриваться как «частично децентрализованные».

В качестве примера можно взять гибридный блокчейн консорциума R3 CEV, членами которого являются около 50 банков.

Частный блокчейн

И, наконец, существуют полностью частные блокчейны, доступ к записи в которые выдается центральной организацией (это может быть, например, центральный банк), но разрешение на чтение может быть открытым или ограниченным (частным).

Характеристики и консенсус

Каждый из блокчейнов определяется его сообществом, типом допускаемых в нем транзакций, используемым в нем методом проверки честности консенсуса, а также его характером (частный он или общественный).

 Публичный блокчейн (или *unpermissioned blockchain,* а также *blockchain mining*):

• характеристики: общественная сеть без посредников и без цензуры;

• консенсус *(proof of work):* дорогой, «медленный», с присущей ему компенсацией сети (майнеры).

ПУБЛИЧНЫЕ БЛОКЧЕЙНЫ И УБЫТКИ ОТ СДЕЛОК

Все протоколы распределенного консенсуса (блокчейны, за исключением биткойна, эфириума и их разновидностей) являются альтернативными решениями проблемы защиты данных в децентрализованном публичном реестре. Все они не только более быстрые и более эффективные, чем решение биткойна, но также разработаны с помощью формальных методов, которые обеспечивают

правильность посредством математической точности.

Теперь, когда мы представили публичные блокчейны и консенсусы, мы считаем уместным напомнить, что биткойн не предлагает формального математического подтверждения правильности своего функционирования. Наоборот, доказано, что в его протоколе имеются определенные недостатки, с теоретической точки зрения. Действительно, в некоторых случаях он оказывается не в состоянии решить проблему византийских генералов.

Было отмечено, что на практике (и это общеизвестно, по крайней мере, среди специалистов) в случае fork (ветвления) его блоков биткойн может потерять данные. Когда fork – ветка – восстановится, развиваться будет только самая длинная ветка, и лишь она будет признана легитимной, что приводит к возможности того, что транзакции в меньшей ветке будут полностью потеряны.

 Частный блокчейн (или *permissioned blockchain,* или консенсус блокчейна):

• особенности: частный или получастный (различные права доступа к платформе), участники известны или идентифицируемы, сектор регулируемый;

• консенсус: между известными участниками функционирование внешнее по отношению к платформе (ответственность берут на себя один или несколько уполномоченных представителей частного блокчейна).

 Блокчейн биткойн:

• с валютой биткойн: биткойн (BTC);

• с другой валютой: Factom (Factoids), Mastercoin (MSC), Counterparty (XCP), Namecoin (NMC).

 Блокчейн, не являющийся блокчейном биткойн:

• с валютой биткойн: Blockstream, Truthcoin;

• с другой валютой: эфириум (ETH), BitShares (BTS), Truthcoin (Cashcoin), Litecoin (LTC), PayCoin (XPY).

 Блокчейн не-блокчейн:

• с консенсусом без майнинга: Ripple (XRP), Stellar (STR), NXT[101] (NXT), Hyperledger, Tendermint, Pebble, Open Transactions, beAchain.

 Нейтральный блокчейн:

• интеллектуальные услуги: Monax (бывший Eris Industries), PeerNova, Codius, SmartContract, SAE, Tezoz, Tillit.

Вот небольшой обзор, который позволяет нам классифицировать некоторые существующие решения, но этот список не является исчерпывающим, классификация крайне субъективная, и рейтинг блокчейнов постоянно меняется.

Консенсус

Определение

Как мы уже говорили ранее, «информационный консенсус в области распределенных систем – это способ, при помощи которого узлы (участники) могут договориться о легитимности сделки и обновлять бухгалтерские книги, представляющие собой стройную систему согласованных фактов»[102].

Таким образом, с точки зрения своей базы и истории (алгоритмы консенсуса появились около 1970 года), консенсус остается основополагающим элементом в области распределенных вычислений, то есть там, где мы имеем ряд узлов (участников), которые должны согласовать решение. Принцип заключается в том, чтобы добиться определенной надежности системы при решении распределенных задач в условиях наличия неисправности.

Таким образом, в теоретической информатике проблема консенсуса требует наличия протокола, который отвечает следующим критериям:[103]

• окончание: любой процесс должен получить некую величину;

• целостность: все процессы принимают значение, которое было предложено одним из процессов;

• согласие: все процессы принимают одно и то же значение.

Протокол, который может гарантировать эти свойства в присутствии не менее t отключений, называется t-robust.

Мы не намерены здесь объяснять функцию консенсуса (математический алгоритм), а всего лишь хотим показать, что в блокчейнах (так называемых публичных) и в распределенных протоколах консенсуса (так называемых частных блокчейнах) существуют различные консенсусы.

Когда мы знакомили вас с функционированием блокчейнабиткойн, мы вводили понятие *proof of work,* или доказательство выполнения работы (майнинг). Но теперь мы знаем, что существуют распределенные алгоритмы консенсуса, более эффективные (в зависимости от варианта применения) и менее энергоемкие, чем *proof of work.*

ПОДТВЕРЖДЕНИЕ ЗАИНТЕРЕСОВАННОСТИ ИЛИ УЧАСТИЯ

Мы знаем, что майнинг – это энергоемкий процесс и некоторые участники, в частности в эфириуме, предпочитают отбросить *proof of work* и перейти к *proof of stake* в связи со слишком большими энергозатратами на огромные вычислительные мощности.

При такой замене для проверки блоков не нужно использовать огромные вычислительные мощности и, следовательно, «сжигать» энергию, можно просто иметь определенное количество криптовалюты.

Обзор консенсуса

Чтобы обеспечивать защиту, упорядоченный и целостный вид реестра, существует ряд алгоритмов консенсуса (по дате появления).

 **1998 год | Подтверждение выполнения работы** – *proof of work* (PoW)[104]: пользователи должны несколько раз выполнить алгоритм хеширования или просчитать математическую головоломку согласно определенному алгоритму для подтверждения электронных транзакций:

• биткойн (специфика: все узлы являются анонимными и потенциально вредоносными, поэтому необходим *proof of work,* «бесполезный» на первый взгляд, но необходимый для безопасности сети);

• эфириум (специфика: та же, что и для биткойна);

• Peercoin и Decred[105] используют гибридный метод PoW/PoS, чтобы воспользоваться преимуществами обеих систем и создать более устойчивый консенсус.

 **1998 год | Paxos**

 **2013 год | Доказательство заинтересованности или участия –** *proof of stake* (PoS)[106]: пользователь должен обладать некоторым количеством криптовалюты, если он хочет претендовать на подтверждение дополнительных блоковблокчейнейне, и получать за это вознаграждение, если таковое предусмотрено:

• проект Ethereum 2017 (Sharding[107]);

• Peercoin[108], подтверждение использования PoS;

• (i) подтверждение обладания – *proof of hold* (PoH): чем больше у вас денег, тем больше у вас прав на проведение проверки;

• (ii) подтверждение использования – *proof of use* (PoU): чем больше вы обмениваете валюту, тем больше у вас прав на проведение проверки;

• (iii) подтверждение ставки/время – *proof of stake/time* (PoST): математическая функция, которая учитывает время владения объектом, чтобы определить вероятность быть выбранным для проверки следующего блока в блокчейне (примеры: Peercoin, Vericoin);

• (iv) подтверждение минимальной ставки/время – *proof of minimum aged stake* (PoMAS): метод, объединенный со взвешиванием (s);

• (v) подтверждение значимости – *proof of importance* (PoI): пользователи, которые имеют наибольшее подтверждение ставки в криптовалюте, будут вознаграждены (пример: NEM).

PROOF OF WORK И PROOF OF STAKE

Proof of work (подтверждение работы) и proof of stake (подтверждение ставки или владения) – два наиболее известных способа проверки блоков. Они состоят из двух совершенно разных механизмов консенсуса.

Процесс, который заключается в решении вычислительных задач,

подразумеваемый *proof of work,* называется майнингом: мы говорим о майнерах.

Процесс решения вычислительных задач, подразумеваемый *proof of stake,* называется минтинг: мы говорим о минтерах.

 **2013 год | Делегирование права на владение –** *delegated proof of stake* (DPoS): здесь консенсус использует систему репутации, набираемой путем голосования, для подбора ограниченной группы людей, которым все доверяют. Только такие люди имеют право записывать блоки и делают это в случайном порядке. Все обладатели жетонов могут голосовать, голоса взвешиваются по количеству фишек, которыми владеет голосующий.

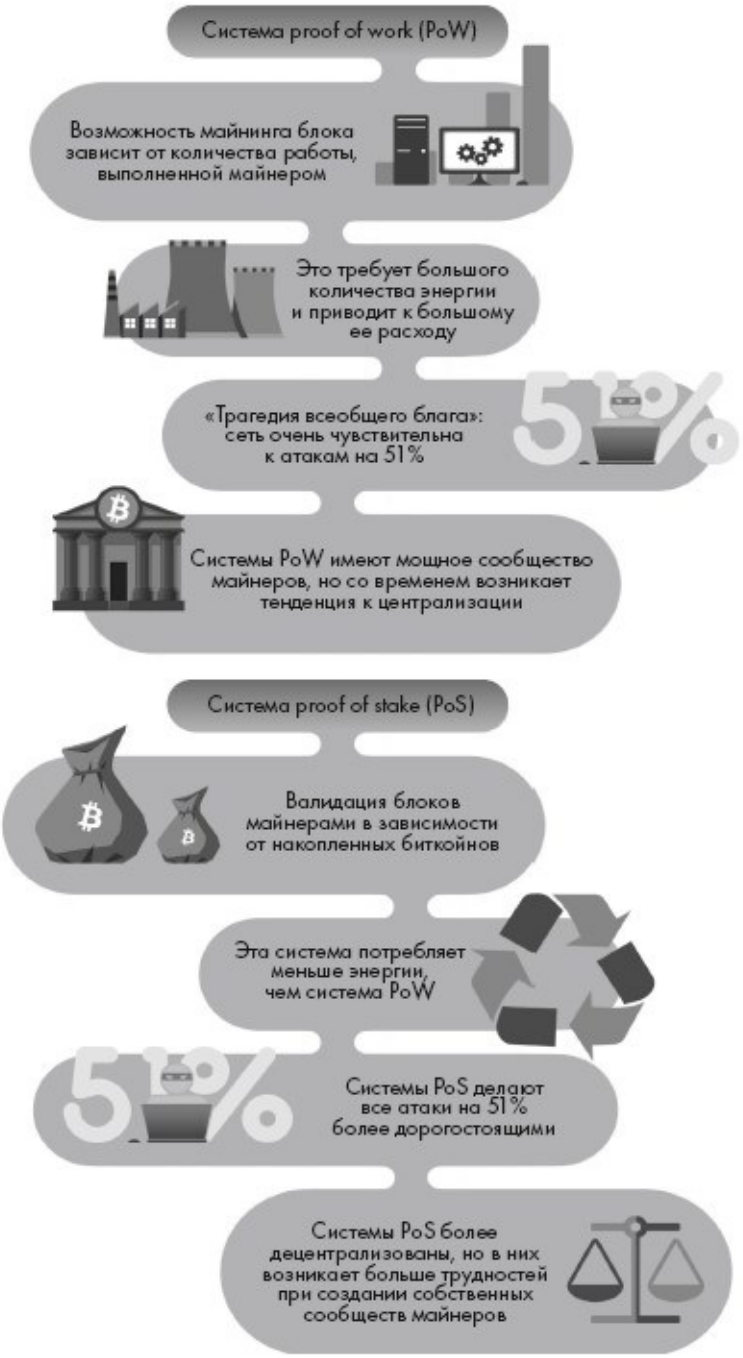
- Bitshares[109];
- Graphene [110];
- Steem[111].

 **2013 год I Raft[112]**(производный от Paxos):

- подтверждение права: один или несколько узлов могут добавлять блоки;
- подтверждение активности (в соответствии с профилями узлов);
- подтверждение возможности (в зависимости от профилей узлов);
- подтверждение личности (например, beAchain);
- толерантность к ошибкам типа задачи византийских генералов (например, Hyperledger и beAchain).

 **2016 год | Juno[113]**(производный от Raft) – творение JP Morgan.

2016 год | **Tangaroa[114]**(производный от Raft).



КОНСЕНСУС МЕЖДУ МАШИНАМИ, МЕЖДУ ОБЪЕКТАМИ, УСТАНАВЛИВАЕМЫЙ BEACHAIN

В то время как одна или несколько машин, участвующих в цепочке, заявляют транзакцию (заявка на установление подлинности/авторизацию, обмен ценностями, часть определенного договора и т. д.), некоторое количество взаимосвязанных в данный момент машин должны прийти к согласию относительно того, принимать ли данную транзакцию или нет. Количество компьютеров (см. теорию ацикличных графов) вариабельно: чем оно выше, тем больше время достижения консенсуса, но результат будет гарантирован.

Экосистемы

Вот краткий обзор последних нововведений (список не исчерпывающий) в этой области блокчейнов, которые некоторые называют blockchains 2.0, – даже если нам намного ближе протоколы реестров, которые распространяются как блокчейны.

Lisk – Dapps[115]

Lisk – это молодая компания, основанная Максом Кордеком. В начале 2016 года она собрала на новый проект 14 тысяч биткойнов. Проект Lisk во многом похож на Ethereum, в частности в том, что облегчает развитие и размещение Dapps (см. врезку ниже).

Lisk – это платформа нового поколения, которая обеспечивает развитие и распространение децентрализованных приложений, написанных на JavaScript. В Lisk разработчики могут создавать, публиковать, распространять и монетизировать свои приложения для работы с внутренней криптовалютой. Система построена таким образом, что она использует блокчейн, определенный пользователем, умные контракты, облачные хранилища данных и вычислительные узлы – все в одном решении.

Lisk – первое средство, децентрализованное приложением, написанным полностью в Node.js. Эта система работает в асинхронном режиме и позволяет обрабатывать без явных задержек такие задачи, как транзакции в сети. Для выполнения сложных запросов база данных использует SQLite. Работа фронтенда Lisk базируется на HTML5 и CSS3.

Использование стандартных и хорошо известных языков приводит к тому, что экосистема Lisk доступна тысячам разработчиков без дополнительных навыков. Любой веб-разработчик, который уже знает JavaScript и Node.js, может сразу взять Lisk и с первого дня начать создавать децентрализованные приложения.

Основная цель Lisk – создание системы *plug-and-play,* которая позволит разработчикам создавать и выполнять все: дизайн, проектирование, разработку, публикацию, монетизацию – все это внутри одной платформы. Используя экосистему Lisk, разработчики могут быстро развернуть Dapps JavaScript к Lisk Hosting & Storage Nodes, видимый в Lisk App Store, и иметь непосредственный доступ к узлам Lisk для выполнения кода. Все это поддерживается функциями целостности и безопасности, которые возникают из функционала консенсуса боковых цепочек Lisk.

Все задачи экосистемы выполняются пользователями и делегатами Lisk, которые оплачиваются посредством автоматической внутренней платежной системы (или в самой сети – в случае делегатов). Вознаграждение узлов выполняется LSK – собственной криптовалютой Lisk или биткойнами.

Stellar Consensus Protocol (SCP)[116]

Stellar.org предложил свой протокол консенсуса (SCP) – конструкцию для **«византийского** соглашения» (метод организации обмена сообщениями по двунаправленным линиям связи в мультипроцессорных системах – Federated Byzantine Agreement – FBA).

SCP был вдохновлен биткойном, и в него добавили возможность допускать участников, нецелесообразных в условиях низкой вычислительной мощности.

SCP является первой надежной конструкцией для FBA, и, в отличие от большинства существующих подходов для достижения консенсуса, у него имеются четыре ключевых свойства:

• децентрализованное управление: SCP в качестве протокола FBA гарантирует безопасность в условиях нерационального поведения, ему нужны достаточно скромные вычислительные ресурсы, за счет чего снижается планка входного барьера;

• гибкий предел достоверности: это означает, что пользователи обладают свободой доверять в любой комбинации сторон, которую они считают правильной;

• небольшое время задержки;

• асимптотическая безопасность: безопасность основывается на цифровых подписях и серии хешей, в которых параметры могут быть разумно отрегулированы таким образом, чтобы обеспечить защиту системы от противников с большой вычислительной мощностью. Чтобы зрительно представить себе это, вообразите пароль, длина которого может расти по мере увеличения вычислительной мощности злоумышленника.

Ripple[117]

Запущенная в 2012 году сеть Ripple позволяет осуществлять «финансовые операции, глобальные, безопасные, мгновенные и почти бесплатные, любого размера и без отзыва проводок». Она поддерживает любые бумажные деньги, любую криптовалюту, биржевые товары или любые другие ценные объекты, такие как бонусные мили, минуты мобильных устройств…

Ripple – это протокол[118] для обмена валютами, который можно определить как «http для денег». Как и в случае с http, его использование бесплатно и не требует лицензии; как и в случае с биткойном, он позволяет заключать сделки на деньги.

В 2016 году Ripple был третьей по величине криптовалютной системой по капитализации после биткойна и эфириума.

Протокол Ripple все больше и больше берут на вооружение банки и системы оплаты. Из пятидесяти крупнейших в мире банков десять уже работают с ней. Ripple – это частный блокчейн (*permissioned*).

IOTA[119]

Поскольку Интернет вещей *(Internet-of-Things,* IoT) продолжает распространять идею необходимости взаимодействия и совместного использования ресурсов, IOTA позволяет компаниям изучить новые модели B2B, делая из каждого технологического ресурса потенциальный обменный сервис на открытом рынке в режиме реального времени и без затрат.

IOTA базируется на новой распределенной бухгалтерской книге, Tangle, в которой устранены все неэффективные элементы конструкции нынешних блокчейнов и введен новый способ достижения консенсуса в одноранговой децентрализованной системе. Впервые благодаря IOTA люди могут перевести деньги без затрат. Это означает, что при помощи IOTA могут осуществляться даже самые небольшие платежи.

IOTA предназначен для работы совместно с другими блокчейнами вроде биткойна или эфириума. Некоторые его особенности таковы.

 Структура данных не принимает форму блокчейна, то есть цепочки блоков, содержащей транзакции. Вместо этого там находится DAG[120] *(Directed Acyclic Graph)* с именем Tangle. IOTA – это криптовалюта на базе Tangle.

 Транзакции, запущенные узлами P2P, будут образовывать Tangle – это означает, что транзакции образуют гроссбух в форме DAG.

 Когда возникает новая транзакция, система должна утвердить две предыдущие сделки. Эти утверждения, представленные в виде ребер графа, вносят свой вклад в защиту сети.

 Если нет направленного ребра между транзакцией A и транзакцией B, но есть путь длиной ≥ 2 от A до B, то говорят, что A косвенно одобряет B.

Hyperledger[121]

«Сделать блокчейн реальным для бизнеса».

Hyperledger – это проект с открытым исходным кодом, который родился в декабре 2015 года благодаря активности нескольких крупных игроков (Accenture, Airbus, Fujitsu, Digital Asset, IBM, Intel, JP Morgan, R3CEV…). Этот проект осуществляет фонд Linux Foundation, который

намерен объединить усилия, направленные на создание технологии блокчейна, или, говоря более точно, технологии распределенных реестров, отвечающей специфическим потребностям фирм. Проект объединяет более 100 участников и развивается быстрее всех остальных проектов Linux Foundation[122]. Участниками являются как технологические консорциумы (IBM, Intel, Fujitsu, Digital Asset, R3, Red Hat…), так и различные производственные предприятия (Airbus, JP Morgan, BNP paribas, ABN Amro).

Основной проект, разрабатываемый под эгидой Hyperledger, называется Fabric. Значительная часть кода поступает из лаборатории IBM, которая поместила его в открытом доступе.

Он предусматривает создание *permissioned ledger* для промышленности. В *permissioned ledger,* в установлении консенсуса могут принять участие только участники сети, становясь узлами системы. Действительно, в условиях производственного регламента идентификация и авторизация участников просто необходимы.

Hyperledger может повысить безопасность данных для блокчейнов в сфере бизнеса за счет многочисленности сообщества, разрабатывающего его элементы, и модульной платформы. У проекта нет цели создать работающий разделенный регистр. Вместо этого предполагается, что в распоряжении предприятий окажется набор основных элементов, позволяющих построить *business-ready* блокчейн (готовый к работе в компании).

В дополнение к характеристикам классических блокчейнов (распределенный реестр, децентрализованный, неизменный, имеющий возможность включения умных контрактов) технология Hyperledger содержит дополнительные функции, очень полезные для бизнес-приложений:

• защита анонимности (невозможность связать данные о личности автора сделки или сделок между собой): можно не раскрывать личность автора записи, опубликованной в едином реестре, если это необходимо в определенных нормативных рамках для обеспечения конкурентоспособности или защиты ноу-хау;

• настраиваемый алгоритм консенсуса: режим консенсуса может быть изменен в зависимости от вариантов использования. Это позволяет достичь уровня производительности, близкого к уровню нераспределенных систем (в плане объема, пропускной способности и времени отклика);

• конфиденциальность: содержание операции может быть зашифровано для обеспечения конфиденциальности сделки. Благодаря этому свойству можно определить, к какой информации имеет доступ каждый участник сети;

• контролируемость: система обеспечивает контролируемость сделок;

• масштабируемость: Hyperledger предназначен для обработки больших объемов транзакций и сохранения устойчивости системы с течением времени.

ПРИМЕРЫ ПРИЛОЖЕНИЙ

Код Hyperledger уже использовался в различных проектах. Например, HSBC и Bank of America использовали его для обработки финансовых аккредитивов. Проект повторяет систему обмена бумажными аккредитивами между экспортной фирмой, предприятием-импортером и их банками через автоматически исполняемые контракты.

Во Франции Crédit Mutuel Arkéa планирует применять для обеспечения обмена информацией со своими клиентами принцип КУС *(Know Your Customer,* знай своего клиента). Голландский банк ABN AMRO, в свою очередь, намерен использовать Hyperledger для того, чтобы стандартизировать информацию для реструктуризации и финансового оздоровления системы. Walmart планирует применять Hyperledger для отслеживания продаж свинины в Китае, Japan Exchange Group – для упорядочения оформления сделок, финская компания Kouvola собирается соединить Hyperledger с подключенными в систему объектами, чтобы улучшить логистические цепочки. UBS после двухлетнего испытания технологии блокчейна планирует использовать эту технологию для того, чтобы создать систему импортно-экспортных сделок, охватывающую весь мир.

Interledger[123]

Этот протокол, разработанный компанией Ripple Labs для подключения блокчейнов к системе распределенных регистров, позволяет проводить платежи через различные сети и использует условные депозиты для обработки движения средств между двумя отдельными гроссбухами. Протокол Interledger формально создан с использованием TLA+[124], он также используется Amazon для исправления критичных ситуаций в системе.

В отличие от подхода биткойна, этот протокол не требует никакой глобальной системы координации блоков.

Tendermint[125]

Tendermint – это протокол[126], который безопасно и последовательно реплицирует приложение на большом числе машин. Tendermint способен работать, даже если до трети машин подверглись случайным сбоям (консенсус BFT).

Tendermint состоит из двух основных технических элементов: консенсусный движок блокчейна и универсальный интерфейс приложения. Движущий консенсус называется Tendermint Core. Он гарантирует, что одинаковые копии сделки сохраняются на каждой машине в том же порядке. Интерфейс приложения называется Tendermint Socket Protocol (TMSP). Он позволяет обрабатывать транзакции на любом языке программирования. В отличие от других вариантов блокчейна и консенсуса, разработчики могут использовать Tendermint для репликации машины состояний BFT независимо от языка программирования и среды разработки.

Monax[127] (ранее – Eris industries)

Monax – это концепция, которая позволяет создавать и использовать распределенные веб-приложения без сервера. Каждое приложение использует для достижения общего консенсуса распределенный блокчейн, выступающий в роли сервера и созданный в сети Ethereum. Пользовательский интерфейс построен с использованием HTML, CSS и

JavaScript. На платформе Eris может быть воспроизведен любой вид существующих веб-приложений, например форум, веб-платформа для коллективного финансирования, рынок и др.

Corda[128] от R3CEV

В начале декабря R3CEV выпустила исходный код своего распределенного регистра для банков и финансовых компаний – Corda. Тестовая версия содержит пять видов умных контрактов. Разработчики подчеркивают, что новая система не базируется на классическом блокчейне.

По данным «белой книги», «Corda – это платформа для ведения распределенного бухгалтерского учета и обработки финансовых соглашений. […] В отличие от биткойна и эфириума, Corda не упорядочивает транзакции при помощи цепочки блоков и, как следствие, не использует майнеров или доказательства выполнения работы (консенсус). Вместо этого каждое состояние указывает на “oracle" или “нотариуса", которые являются сервисами, гарантирующими, что сделка будет подписана только в том случае, если все точки входа будут приведены в соответствие.

Пользователи сети не получат доступ ко всему реестру операций, они будут видеть только подмножество данных, управляемых системой. Данные подтверждаются, если по крайней мере двое участников системы достигнут консенсуса по этому вопросу, в то время как любой комбинации участников разрешается участвовать в процессе достижения консенсуса относительно записи, внесенной в реестр.

Чтобы получить доступ к данным клиентов Corda, могут быть использованы составные ключи. Платформа позволяет им передавать дополнительные ключи и их комбинации третьей стороне, участвующей в операции».

Главной особенностью Corda в качестве системы является возможность выполнения умных контрактов. Текущая версия этой системы предлагает пользователям пять видов умных контрактов: работа с наличными, работа с товарами, работа с коммерческими бумагами, процентный своп и работа

с обязательствами. По словам разработчиков, все контракты могут быть связаны во времени: «Контракты с ограниченным сроком действия с нотариусами (или *oracles)* должны быть синхронизированы с атомными часами военно-морской обсерватории США».

Пользователи могут объединять и редактировать шаблоны, чтобы создать уникальные контракты, адаптированные к их потребностям. Команда Corda опубликовала целый учебник, посвященный тому, как в текущей версии кодировать простой договор с доступными элементами.

В настоящее время платформа Corda находится на стадии тестирования. Для того чтобы продолжить исследования и разработки, R3CEV получил поддержку ведущих мировых банков, включая Bank of America, JPMorgan, Credit Suisse, Barclays, Deutsche Bank, HSBC, Citi, Commerzbank и Société Generale (Santander и Goldman Sachs покинули консорциум в конце ноября).

beAchain[129] – объектно-ориентированный блокчейн (ООБ)

beAchain – это блокчейн (находящийся на стадии разработки), который позволяет своим пользователям разрабатывать собственные безопасные одноранговые приложения, причем даже тем, кто не является специалистом в области компьютерных технологий.

Объектная ориентированность блокчейна означает, что он позволяет подключенным объектам – компьютерам, планшетам, смартфонам, а также всем устройствам, связанным с IoT (Интернетом вещей), – датчикам, транспортным средствам, домам, одежде, бытовой технике, беспилотным летательным аппаратам и пр. – взаимодействовать между собой, сравнивать свои данные, опрашивать друг друга и, в конечном счете, принимать решения в соответствии с индивидуальными алгоритмами о том, принимается транзакция или нет. В перспективе это позволяет реализовать несколько десятков тысяч операций в секунду. Для этого beAchain опирается на конкретные протоколы с ультракомпактными режимами шифрования и ультрабыстрыми процессами.

Перегруппировывая объекты в группы связанных объектов (GOA), beAchain позволяет создавать временные виртуальные организации (Quick

Virtual Organization, QVO), альтернативные модели экономического развития промышленного предприятия. Без адреса, без помещения, без хранения, без обмена валюты, без затрат и заработной платы, QVO – организация с децентрализованным автономным производством, в котором связанные между собой машины могут вести собственный бизнес, управляемый контрактами, созданными пользователями. Обеспеченные инструментами искусственного интеллекта, эти интерфейсы позволяют создавать свои умные контракты на естественном языке (русский, французский, английский…), которые алгоритмы beAchain переводят в коды для запуска на компьютере. Любой такой контракт может быть проверен и переписан каждой из заинтересованных сторон, прежде чем он будет публично запущен на выполнение.

Любой объект beAchain одновременно способен владеть криптовалютой, привлекать коммерческие контракты с другими объектами *(smart contracts),* быть вызванным для выполнения конкретной задачи или участвовать в консенсусе транзакций. Так, например, можно ссылаться на приложения с любыми автомобилями и только с автомобилями. Или адресоваться только туда, где есть упоминание о датчиках температуры. Или исключить из конкретного протокола все смартфоны. Учетные данные компьютеров договаривающихся сторон защищены устойчивыми к поломкам подтверждениями личности *(quantum-resistant),* зависящими от набора частных/открытых ключей, что гарантирует оптимальную защиту.

Блокчейны beAchain, одновременно частные, общедоступные и гибридные, в зависимости от используемых протоколов, могут применяться, например, для производства (автомобили, энергетика, управление запасами, отслеживание продуктов), организации онлайн-сервисов (страхование, переводы, отслеживание учетных данных), организации мероприятий, в средствах массовой информации (*pay-per-view*), на транспорте (VTC, упаковочные материалы, услуги по продаже билетов), для контрактации между объектами (раздел имущества / установление принадлежности и проверка подлинности файлов STL, управление 3D-принтерами) или в качестве платформы для обмена.

QVO, ВРЕМЕННЫЕ ВИРТУАЛЬНЫЕ ОРГАНИЗАЦИИ

Построенная по той же модели и той же технологии, что и QVE, QVO –

это модель развития beAchain, гораздо менее ориентированная на бизнес. Она адаптирована под специфику создания культурных, политических, социальных, спортивных мероприятий.

С концептуальной точки зрения QVE и QVO приближаются к DAO эфириума с той лишь разницей, что они ориентируются не на срок, а на цель. Например, «QVO Paris – New York»[130], где целью является полностью открытая и децентрализованная организация трансатлантического перелета.

Подведем итоги

Итак, мы добрались до конца главы 2, посвященной реестрам, протоколам и консенсусам, которые являются технологическим продолжением блокчейна биткойн, поддерживающим одноранговые сделки по торговле криптовалютой – биткойнами.

Изобретенный в 2008 году Сатоси Накамото, биткойн представляет собой децентрализованную платформу, позволяющую при помощи ряда протоколов и технологий обеспечить доверие и безопасность обмена валютой, полностью убрав облеченную властью третью сторону (в данном случае банки).

Транзакции передаются в зашифрованном виде, анонимные, защищенные, а их история – это зашифрованная цепочка блоков, распределенная между всеми компьютерами таким образом, что не требуется ни одного сервера, на котором эта информация будет собираться, храниться, сосредотачиваться и перераспределяться. Эта технология идеально горизонтальна, транзакции в ней узакониваются не некоей внешней организацией, но прямым консенсусом между участниками системы.

Пользователи этой системы очень быстро пришли к очевидному выводу: потенциал блокчейна[131] огромен, а варианты его применения практически безграничны при условии возможности расширить поле деятельности, ограниченное, например в биткойне, исключительно финансовыми потоками.

В 2014 году молодой разработчик Виталик Бутерин создал эфириум – платформу блокчейна по образу биткойна, но разработанную таким образом, что она могла предоставить множество других вариантов ее использования. В результате появилось понятие «глобальный компьютер»: все компьютеры, подключенные к эфириуму, могут обмениваться данными, делиться ими, работать друг с другом и разделять задачи, чтобы

произвести данные, которые будут распределены по горизонтали, организованные в блоки в зашифрованном виде.

Одновременно начали появляться и другие блокчейны: Lisk, Ripple, IOTA, Hyperledger, Interledger, Tendermlnt, Monax, Corda, beAchaln… новые горизонты открылись и для экспериментов.

Посредством протокола платформы блокчейн обещает, что в ближайшем будущем будет создан не просто автономный электронный носитель, способный вести диалог с вашим смартфоном по вопросам платежей, но универсальная платформа, позволяющая всем пользователям самостоятельно создавать необходимые им приложения – не важно, для личных или коллективных нужд, реализуемые посредством умных контрактов, защищенных от изменения и фальсификации.

Блокчейн проникает и в такие области, где Интернет вещей (IoT), искусственный интеллект (ИИ) и одноранговые технологии (блоков) сходятся воедино, создавая децентрализованные формы обмена валюты без собственника, открытые, основанные на системах взаимного доверия и осуществляющие платежи по горизонтали в режиме реального времени, что гарантируется самим протоколом.

Перейдем к практике…

Глава 3

Блокчейн на практике

Систематические инновации требуют быть готовым относиться к изменениям как к удобному случаю

Питер Друкер

Примеры использования, приложения

На данном этапе развития технологии блокчейна задачи дезинтеграции и преобразования бизнеса являются приоритетными, в связи с чем трудно охватить взглядом картину целиком.

Тем не менее, следует уточнить, что в сфере финансов возможность дезинтеграции должна быть предоставлена в первую очередь участникам, находящимся на концах цепочки добавленной стоимости (эмитенты, инвесторы), при этом посредников (доверенных лиц) следует заменить на функции с добавленной стоимостью.

Принципы технологии блокчейна

Блокчейн – новая, децентрализованная, надежная и прозрачная технология, которая позволяет хранить, обменивать, проверять и верифицировать информацию, причем эти действия стоят недорого и поддерживаются самим пользователем (что позволяет обойтись без третьего доверенного лица). Какие же области применения этой технологии могут быть?

Централизация или децентрализация

Децентрализация является важной концепцией, которая связана не только с блокчейном биткойн. Вопрос «централизация или децентрализация» возникает в самых разнообразных цифровых технологиях. Например, в Интернете, являющемся децентрализованной системой, существует электронная почта, ядром которой является

децентрализованная система на основе протокола SMTP (Simple Mail Transfer Protocol), открытый стандарт. Что касается социальных сетей, несмотря на множество усилий энтузиастов, разработчиков и предпринимателей по созданию альтернативной модели, они остаются централизованными системами – в частности, Facebook и LinkedIn, которые доминируют на этом рынке. В действительности, этот конфликт зародился задолго до цифровой эпохи, и аналогичную борьбу между этими двумя моделями можно было наблюдать в истории телефонии, радио, телевидения и кинематографа.

На практике ни одна система не является чисто децентрализованной или чисто централизованной.

Например, электронная почта – в основном децентрализованная система, и любой может использовать сервер электронной почты по собственной инициативе. Тем не менее, возникла ситуация, когда небольшое число централизованных поставщиков электронной почты стали доминировать на этом рынке. Несмотря на то что протокол биткойн является децентрализованным, такие услуги, как обмен валютой биткойна, позволяющий конвертировать биткойны в другие виды валют, программное обеспечение бумажника *(wollet)* и программное обеспечение, позволяющее людям управлять их биткойнами, могут быть в разной степени централизованы или децентрализованы.

Распределенный консенсус

Основной технической проблемой, которую приходится решать при построении распределенной системы, независимо от вариантов ее использования, является достижение распределенного консенсуса. Эта же концепция консенсуса характеризует блокчейны и порождает заметные различия между различными технологиями блокчейна. Так, блокчейны биткойна или эфириума обращаются к консенсусу *proof of work* (доказательство выполнения работы или майнинг), в то время как другие блокчейны, такие как Casper, обращаются к консенсусу *proof of stoke* (доказательство с защитой по методу «подтверждение доли»).

Сфера применения технологии блокчейна очень широка, но это не означает, что ее можно использовать для чего угодно. Так, например, не

всегда нужно применять модель «доказательства выполнения работы», требующую наличия большого сообщества и более чем значительных затрат энергии (см. понятие майнинга в главе 2).

Отказ от посредников

Принцип отказа от посредников, или удаления третьего доверенного лица, является самой сутью технологии блокчейна. Действительно, она работает без посредников.

В качестве примера рассмотрим сделку между двумя лицами без блокчейна. Банк проверяет, что плательщик имеет заявленные им средства, после чего верифицирует сделку или отвергает ее. Банк играет роль посредника и доверенного лица.

С другой стороны, если два человека выполняют эту транзакцию с помощью системы на основе блокчейна, то сама система проверяет условия сделки. Таким образом, эта технология служит для проверки истинности информации, товарообмена, сделок независимо от их природы, без необходимости обращаться к доверенной третьей стороне. При этом невозможны никакие обманные манипуляции, так как для этого потребуется вносить изменения во все точки хранения блоков в блокчейне.

Принятие принципа распределенных гроссбухов с «избавлением» от финансового посредничества приводит к тому, что сделки, принятые или отклоненные, становятся результатом распределенного консенсуса, а не волеизъявления централизованного учреждения. Некоторые наблюдатели предсказывают, что блокчейн с его отказом от доверенной третьей стороны должен «сделать горизонтальной» всю нашу коммерческую деятельность.

Активизация блокчейнов в наши дни говорит о том, что доверие, которое традиционно оказывалось учреждениям, переносится сегодня на сообщества пользователей, из чего можно сделать вывод о стремлении общества к горизонтали.

Безопасность

Безопасность является следствием децентрализованное™ и распределенности системы: информация не хранится в одном месте, но распространена по сети.

Эта технология используется в рамках сетевых устройств (компьютеров, смартфонов, смарт-объектов ит.д.), которые связаны между собой независимо от того, расположены они близко или далеко друг от друга.

Таким образом, в рамках блокчейна биткойн каждый участник (узел) в этой сети идентифицируется с помощью адреса, определяемого в момент его вступления в систему. Именно этот адрес будет использоваться в сделке. Что касается дыр в системе безопасности блокчейна – об этом шла речь в разделе «Атака на 51 %» в главе 2.

Прозрачность и неизменность

Свободный и бесплатный блокчейн прозрачен:[136] он позволяет получить доступ к исходному коду платформы, ознакомиться с информацией и историей всех транзакций или событий, произошедших с момента создания блокчейна.

В «блокчейнизированной» системе все записи необратимы и недоступны для фальсифицирования. Другими словами, когда что-то регистрируется в этой системе, оно хранится постоянно и доступно для ознакомления всем участникам (узлам).

Прослеживаемость

Напомним лишь, что блокчейн – это активный реестр, заполняемый в хронологическом порядке, распределенный, проверяемый и защищенный от подделки с помощью распределенной системы доверия, благодаря которой все, что там зарегистрировано, доступно для отслеживания и не может быть удалено.

Таким образом, мы сможем применить этот принцип прослеживаемости в самых разных областях. Таких, например, как продукты, лекарства, произведения искусства, драгоценные металлы. Также возможно создать способ достоверного отслеживания, не прибегая

к неоднократной передаче документов – источнику возникновения ошибок и благодатной почве для мошенничества.

Что касается произведений искусства, в мае 2015 года компания Deloitte Luxembourg разработала технологическую альтернативу традиционным письменным свидетельствам, которые подтверждают происхождение произведения искусства и его перемещение. Этой альтернативой является приложение ArtTracktive. В нем содержится распределенный реестр, куда заносятся происхождение и локализация произведений искусства. В нем использовано доказательство концепции на основе блокчейна, которое осуществляет управление взаимодействием между различными участвующими в сделке сторонами, художниками или владельцами картины, включая экспедиторов, таможню, художественные галереи и музеи, вплоть до потенциальных покупателей.

Таким образом, применительно к рынку искусства технология блокчейна позволяет записывать надежные и полностью прослеживаемые истории произведений искусства, начиная с их создания и заканчивая выставками и покупкой.

Проверка подлинности, нотариальное заверение

Купленный или проданный предмет, зарегистрированный патент, заявленный товарный знак и т. д. – все эти перемещения объектов, активов, документов, имущества и договоров проходят проверку подлинности, поскольку они зарегистрированы в блокчейне. Можно еще добавить нотаризацию блокчейна владельца и/ или заявителя, а также час, день и год.

Учтя все эти вопросы, французский стартап Block-ness[139] работает над созданием решений, позволяющих проследить происхождение и свойства объектов до любого перемещения (дарения, уступки), а также над обеспечением аутентификации процессов (качество, ISO и т. д.).

РАЗЛИЧНЫЕ ПРИЛОЖЕНИЯ

Мы решили привести здесь далеко не полный список различных приложений технологии блокчейн [141].

Список приложений (классифицированный по областям применения) [142]

(Мы указали в скобках наименования и имена некоторых участников, которые разрабатывают эти приложения).

 Активы – цифровое управление (Colu).

 Приложения – доказательство права собственности на модули, используемые для разработки приложений (Assembly, MyPowers).

 Искусство – установление подлинности произведений искусства (Verisart).

 Страхование – микроконтракты (Czam).

 Авизо, экспертное заключение – установка подлинности авизо и экспертных заключений посредством Интеренета (The World Table, Asimov).

 Кадастр – управление (Factom).

 Предоплаченные карты (BuyAnyCoin).

 Продовольственные запасы (Skuchain, Thing-Chain, Caravaggio, Cognizant, Consentio, Fluent, Kouvola Innovation, Modum, Open Trade Docs, Synechron, Zerado).

 Сотрудничество в области компьютерных проектов (BlockchainValley).

 Контент – распределение (Alexandria).

 Контракты – оцифровывание контрактов (Colu).

 Контракты – управление контрактами и командами (UbiMS).

 Контрафакт – борьба с контрафактом (TheReal-McCoy, Chainlink, BlockVerify).

 Контрафакт (Blockness, Blockverify).

 Сбор средств на проекты в области блокчейна (Koinify, BlockchainValley).

 Бриллианты – управление (Everledger).

 Дипломы – определение подлинности дипломов (KeeeX, dipl.me).

 Документы – определение подлинности документов, доказательство их существования, доказательство собственности на цифровой контент (Ascribe, Artplus, blockai.com, blockness.io, bitproof. io, ChainyLing, crypto Public Notary, factom.org, KeeeX, proofofexistence.com, remembr.io, Stampery).

 Данные – публичные базы данных (Mayor Chains).

 Данные – анализ данных (Belem.io).

 Данные – блокчейн данных (КееeX).

 Электронная коммерция – децентрализованные платформы (OpenBazaar).

 Энергия – умный электрический компьютер (E-Energy Center).

 Энергия – возобновляемая энергия и распределенная экономика (TransActive Grid, powerledger. com, SolarCoin).

 Лояльность – карты постоянного клиента (Ribbit.me).

 Лояльность – подсчет баллов (Gyftblock).

 Доверительное управление условными депозитами (PlayCoin, NewSystemTechnologies, Fundes).

 Финансы – финансовые операции (SETL, FactoryBanking).

 Реквизиты – проверка подлинности реквизитов (ShoCard).

 Реквизиты – управление (Ascribe, Verisart, One-name).

 Реквизиты цифровые (Onename, Trustatom, Fol-lowMyVote).

 Недвижимость – управление недвижимостью (Blockness.io,

Bitproof, Blocknotary).

- Информация – аудит, прослеживаемость информации (Factom).
- Альтернативные виды Интернета (ZeroNet).
- Интернет вещей – IoT (IOTA, beAchain, Adept, Filament, Hyperledger).
- Игры (Spells of Genesis, Voxelnauts).
- Marketplace – платформы для создания marketplace (NXT).
- Media streaming (Streamium).
- Медицина – управление медицинскими досье, медицинская информация (BitHealth).
- Почта (Getgems, Sendchat).
- Майнинг (21 inc., Bitfury).
- Музыка (Ujo, Peertracks, BitTunes Music on the Blockchain).
- Доменные имена – управление (Namecoin).

 Объекты – управление (Blockness.io, Slock.it).

 Платежи – простые и защищеннные линейные платежи (Alipay).

 Акции – монетизация акций в стартапах (Founderbeam).

 Прогнозы – управление рыночными прогнозами (Augur).

 Уступки между участниками (MoneyCircles).

 Собственность – цифровая защита передачи собственности (Symbiont, Mirror, Secure Asset, Bitshares, Coin-e, equity-Bits, DXMarkets, MUNA).

 Интеллектуальная собственность (Blockness.io, Monegraph, Bitprof).

 Деловые сети (Debune).

 Социальные сети P2P (DATT, Synereo). Электронная подпись (BlockSign).

 *Smart grid, smart cities,* умные города, умные суда(1_03 Energy, Enerchain, ElectriCChain).

 Хранение золота (Bitgold).

 Хранение децентрализованное, виртуальное облако (Storj, BigchainDB, Sia. tech).

 Прослеживаемость (Blockness.io, Blockpharma, Provenance).

 Личный транспорт (aeCar, la'Zooz).

 Убер, уберизация (Arcade City).

 Частная жизнь – управление частной жизнью при помощи цифровых объектов (ShoCard, Uniquid).

 Голосование (Voatz, Belem, Neutral Voting Bloc, civicdApp.com, cryptovoter.com, v-initiative.org, followmyvote.com, unchain.voting).

Обзор далеко не полного перечня возможных приложений, вплоть до уже используемых

Проектов слишком много, чтобы перечислить их все. Важно помнить об их разнообразии и о том, что они применяются в наиболее распространенных областях жизни. У всех приложений есть нечто общее: почти абсолютная защита передачи и архивирования информации, что априори является их положительным качеством. Но то, что мы не видим (пока), – это глубокое изменение образа жизни и мышления, которое несет с собой эта технология; устраняя риски (мошенничества, потери, ошибки…), она устраняет сомнения в том, что человек является существом, одаренным разумом и совестью, а не просто машиной.

Тем не менее, потенциал применения блокчейна находится еще на стадии развития. Всего несколько месяцев назад кто мог бы представить себе большинство из этих приложений? И какие еще приложения появятся в течение трех, шести или девяти месяцев? Ближайшие два-три года

должны быть посвящены экспериментам, но я не сомневаюсь, что мы увидим еще много важных «блокчейновских» приложений.

Безусловно, обозревая все эти проекты, можно понять, что технология блокчейна не исчезнет. Она пришла, чтобы остаться и глубоко преобразовать нашу экономику и наше общество. Опишем несколько наиболее значительных приложений.

Энергия

Электроэнергетика вовсе не является главной причиной шумихи вокруг блокчейна, но это, конечно, отрасль, количество приложений в которой будет неуклонно расти.

Увеличение числа автопроизводителей влечет за собой огромные проблемы в области энергетики, связанные с традиционными сетями распределения ресурсов, исторически сконструированными определенным образом. Решение – это увеличение числа локальных сетей – умные сети[143].

В феврале 2016 года немецкий конгломерат RWE[144] объявил о своем эксперименте[145], проводимом совместно со стартапом Slock.it над новым поколением терминалов для оплаты подзарядки электромобилей. Во Франции Engie проводит аналогичные эксперименты, в частности в области отслеживания потоков (вода, газ, электричество).

В апреле 2016 года в Бруклине, при поддержке руководства штата Нью-Йорк, родилась инициатива, сочетающая в себе собственно энергию и децентрализованную экономическую систему. Эта микросеть[146] была разработана совместным предприятием TransActive Grid. Оно состоит из двух предприятий: L03 Energy[147], которая разрабатывает сети солнечной энергии, и ConsenSys[148], специализирующейся на блокчейне биткойн. В данном случае цель – дать возможность гражданам вернуть себе производство электроэнергии путем создания энергетических мини-сообществ; для этого датчики записывают историю создания энергии в конкретной точке и передают данные в блокчейн эфириум. Умные контракты затем могут регулировать правила использования этой энергии и цены производителей.

В июле 2016 года Ponton, стартап из Германии, разработал платформу Enerchain – первый европейский рынок энергетики на базе блокчейна. Enerchain позволяет отправлять заказы анонимно. Партнеры нажимают на кнопку на экране для завершения сделки, все осуществляется напрямую и, следовательно, без каких-либо посредников.

В октябре 2016 года, в ходе мероприятия Hackenergy [150] 2016, которое проходило в Гронингене, Нидерланды, была представлена

одноранговая торговая система энергосбережения (P2P), которая называется EcoCoin. Это торговая система на основе блокчейна *open source* Hyperledger (см. главу 2).

3 и 4 ноября 2016 года, в ходе мероприятия EMART Energy 2016, которое состоялось в Амстердаме, произошла первая сделка относительно европейской электроэнергии посредством бельгийского блокчейна Yuso и голландского Priogen.

Следует также упомянуть проект ElectriCChain открытого исследовательского консорциума Chain of Things. ElectriCChain имеет своей целью создание общедоступного и безопасного инструмента для отслеживания производства и использования солнечной энергии в реальном времени и в глобальных масштабах. На практике ассигнования на солнечную энергию передаются в местные регистраторы (подключенные к панели солнечных батарей), которые подключены к узлу блокчейна. Информация оказывается в глобальной сети общего доступа.

Традиционно энергетика всегда медленно принимала новые технологии. Но сегодня этот сектор стремительно меняется, внедряя цифровые технологии, и многие компании готовы использовать новые технологические разработки для решения задач. Коммунальные службы пытаются понять, каким образом они могли бы принять участие в этом новом мире распределенной энергии.

Прослеживаемость продуктов питания

В этой области задействовано несколько проектов, самым важным из которых является проект, запущенный в октябре 2016 года компаниями Walmart, IBM и университетом Цинхуа, подписавшими в Пекине соглашение; согласно ему они должны были изучить прослеживаемость и достоверность цепи поставок пищевых продуктов с использованием технологии блокчейн. Здесь мы имеем дело с тремя мощными участниками рынка в экономике, где прослеживаемость пищевых продуктов очень важна и постоянно совершенствуется.

Борьба с пиратами в области создания фильмов, видео и музыки

Загрузка произведений из Интернета стала обычным делом, хотя ее и пытаются регулировать. Появление платформ дистанционной загрузки и потоковой трансляции Spotify, Apple Music или Deezer нанесло серьезный удар по всей системе авторских прав в музыкальной индустрии. Во многих странах широко распространено незаконное скачивание музыки или фильмов, мимо сайтов, которые платят отчисления артистам и продюсерам. Например, последний сезон сериала «Игра престолов» был незаконно загружен более 14 миллионов раз.

Бизнес-модели этой отрасли в настоящее время пытаются изменить ситуацию с потерей доходов вследствие нарушения авторских прав. Технология блокчейна позволяет бороться с этим.

В этом же состоит и цель австралийского стартапа Veredictum[151], создавшего приложение для киноиндустрии, или стартапа Revelator[152] – для музыкальной индустрии[153]. Речь идет о том, чтобы предложить производителям хранить фильмы, сценарии и другие работы в блокчейне с помощью системы токенизации[154] (в ходе тестирования). Таким образом, любое незаконное использование этой информации будет автоматически распознано, так как оно не будет подтверждено цепочкой блоков. Аналогичное решение было создано для видео на платформах типа YouTube.

Проверка подлинности товаров, включая лекарства

Рынок подделок процветает, и Интернет способствует незаконной торговле этого вида товаров. Все или почти все товары копируются, при условии, конечно, что у них есть хоть какая-то рыночная стоимость. Особый случай – это лекарства, поскольку это товар, связанный со здоровьем. Примерно от 10 до 30 % лекарств, поставляемых в развивающиеся страны, являются поддельными.

Всемирная организация здравоохранения насчитывает до 700 тысяч смертей в год, вызванных поддельными лекарствами. Как способ борьбы с этим явлением можно было бы создать универсальную систему с возможностью отслеживания лекарственных средств. Французский стартап Blockpharma[155] предлагает свое решение для мгновенной проверки подлинности купленной упаковки лекарств с использованием смартфона.

Архивирование медицинских данных и совместное использование медицинской информации

Медицинские данные о каждом из нас в целом являются очень личной, даже интимной информацией, требующей полной конфиденциальности. Но знание некоторых данных третьими лицами бывает необходимо

в случае чрезвычайной ситуации, аварии, серьезной болезни и другой подобной ситуации. Как убедиться, что скорая помощь владеет всей медицинской информацией, необходимой медику, но при этом такая информация не станет известна первому встречному?

Стартап из Калифорнии Blockchain Health[1] начал архивировать медицинские данные ряда людей, работающих с центрами медицинских исследований. Блокчейн позволяет более эффективно управлять доступом к медицинской документации (DMP) и защищать его благодаря системе умных контрактов. С аналогичной инициативой выступил проект MedRec[156][157].

Можно пойти дальше и обеспечить доступ к медицинской информации посредством системы мультиподписи, позволяющей открывать папки при помощи подписей пациента и врача. И предусмотреть, чтобы для этого доступа требовалось определенное количество подписей (ключей). Отчасти это внедряет развивающийся в Массачусетском технологическом институте проект Enigma[158], который направлен в целом на защиту личных данных.

Кадастр

Известно, что кадастр позволяет картировать границы объектов, позволяя государству взимать налоги в случае наследования или продажи. При отсутствии земельного кадастра не только государство теряет доходы, но и владельцы земельных участков не могут подтвердить, что эти участки принадлежат именно им.

Например, в Африке или в Латинской Америке многие страны либо не имеют кадастра вообще, либо их кадастр ненадежен. Чтобы решить эту проблему, ONG Bitland[159] объявил о запуске проекта цифрового

земельного кадастра в Гане, который позволит владельцам обследовать свои земли с помощью GPS и записать акты, подтверждающие владение землей, посредством блокчейна. Аналогичный проект возник в Гондурасе – он заявил о своем желании воспользоваться этой технологией совместно с компанией Epigraph[160].

Администрация

Все государства, большие и малые, должны обрабатывать ряд документов своих граждан – не только административные документы, связанные с налогами, конечно, но также и различные официальные документы, такие как водительские права, удостоверения личности, визы и многое другое.

В Дубае наследный принц объявил в октябре 2016 года о создании архива подобных данных на основе блокчейна, в частности для того чтобы проверять визы. Это позволит стране сэкономить до 25,1 миллиона рабочих часов административных служащих в год.

Паспортные данные

Цифровые паспортные данные позволяют организовать связь между числовым объектом и личностью физического лица (людьми, предприятиями и объектами). Цель этого – проверка данных конкретного физического лица, например в банках, на транспорте, а также преобразование в нематериальную форму свидетельств о рождении и смерти, создание системы виртуальной репутации.

Проектами организации систем хранения цифровых удостоверений личности с помощью блокчейнов уже занимаются несколько компаний-старт-апов. Например, ShoCard[161] осуществляет регистрацию данных из документов, удостоверяющих личность, для нужд контроля в аэропортах (или на других платформах перевозки).

Есть и другой род систем. Американский стартап Onename[162] осуществляет создание «виртуальной личности» в Интернете с помощью блокчейна: это похоже на учетные записи Facebook, которые позволяют открывать счета без запрашивания адреса, e-mail, логина и/или пароля.

Личные данные не хранятся централизованно на серверах компании, а записаны в цепочке блоков. Только владелец данных может получить к ним доступ с помощью секретного ключа. В Facebook (и др.) становится невозможным «перепродать» наши личные данные третьим лицам в коммерческих целях.

Платежи

На ближайшие годы одним из самых важных вопросов в области банковского дела будет противодействие мошенничеству при совершении электронных платежей. Однако, несмотря на меры безопасности, разработанные банками, такие как технологии 3D-Secure, мошенники продолжают действовать. Таким образом, это область, которую хотели бы усовершенствовать все участники банковских операций. На сегодняшний день наиболее успешной инициативой, помимо биткойна, является Ripple[163]. Ripple позволяет проводить безопасные транзакции мгновенно, почти без комиссий, любого размера и безотказно. Он поддерживает любую валюту, криптовалюту, товар или любые другие ценные объекты вроде бонусных миль, минут мобильных операторов, расстояний GPS…

Поставка и платеж

Блокчейн можно применять в самых разных сферах, в том числе на финансовых рынках и в расчетных системах поставок и платежей.

Приходится констатировать, что даже спустя более чем тридцать лет после дематериализации ценных бумаг Франция несколько отстает в освоении технологий послеторгового оформления сделок. Чтобы наверстать упущенное, блокчейн сегодня может быть не только реестром для выдачи и движения документов, но также и средством регистрации ценных бумаг (или валюты). Таким образом, блокчейн будет выполнять все функции реестра, рынка и «счета для ценных бумаг».

Именно это создает лондонский стартап SETL[164], который может заменить центральные депозитарии ценных бумаг, расчетные и клиринговые палаты, а также системы расчета и доставки.

Долевое финансирование

«Мы будем извлекать пользу из постановления по вопросам финансового регулирования, стряхнем пыль с кассовых бонов и создадим минибоны, чтобы поэкспериментировать с блокчейном», – заявил 29 марта 2016 года Эммануэль Макрон во время заседания, посвященного долевому финансированию. Это заявление уже в следующем месяце дало плоды, и в результате блокчейн начали применять в соответствии с французскими законами как «распределенное устройство записи информации, позволяющее проверить подлинность операций».

Зарезервированные для финансового посредничества на платформах, утвержденных «консультантом по долевым инвестициям (ClP)» или «поставщиком инвестиционных услуг» (PSI), минибоны имеют правовой статус, унаследованный от кассовых бонов, с усиленной системой безопасности. Срок погашения минибонов более пяти лет. Минибоны являются именными ценными бумагами, зарезервированными для акционерных обществ (OAO) с упрощенными

акциями (SAS) или с ограниченной ответственностью (OOO), имеющих не менее трех отчетных периодов и полностью свободный капитал. Они могут приобретаться частными вкладчиками, такими как организации и предприятия. Для осуществления эмиссий платформы могут получить доступ к банковскому файлу FIBEN эмитента для оценки финансового состояния предприятия и получения возможности в полной мере выполнять свою миссию консультанта по инвестициям.

Подлинная инновация минибонов заключается в способе их распространения, поскольку постановление правительства позволяет платформам использовать устройство, основанное на технологии блокчейна, – это первый подобный случай во французском законодательстве. Во многом сектор долевого финансирования – это полигон во французском правовом поле, идеально подходящий для блокчейна.

Это происходит прежде всего потому, что объем обрабатываемых посредством ClP транзакций относительно низок, по крайней мере по сравнению с регулируемыми и организованными рынками, что делает

беспредметными некоторые упреки, часто обращенные в адрес блокчейна, такие как сравнительная медлительность подтверждения сделок, сомнения относительно возможности этой технологии обрабатывать значительные объемы транзакций (scalability) или энергоемкий характер процедуры[165].

С другой стороны, поскольку операции, осуществленные через ClP с помощью блокчейна, не представляют особой сложности в рамках права на забвение или с позиций закона об интеллектуальной собственности, этот свод правил сложно совместить с принципами нерушимости и децентрализации публичного блокчейна. В частности, минибоны идеально подходят для подобного эксперимента.

Участники долевого финансирования заинтересованы в блокчейне для ведения реестра. Компании, выпускающие такие долговые ценные бумаги, как минибоны, а также облигации и акции, обязаны хранить реестр подписчиков. Если этот реестр можно будет делегировать третьим лицам на определенных условиях, блокчейн сможет значительно улучшить ситуацию. Действительно, если некоторое количество участников планирует поддерживать реестр в виде стандартной базы данных, блокчейн может оказаться очень интересным вариантом резервного копирования, потому что он имеет форму, радикально отличающуюся от обычных баз данных. Таким образом, кажется немыслимым, чтобы две системы разрушились одновременно, в то время как синхронизация этих двух систем выполняется просто и практически мгновенно. Более того, блокчейн обеспечивает большую прозрачность ведения реестра. Преемник отвечает за реестр, но эмитенту не нужен преемник для того, чтобы получить доступ и оформить все юридические документы.

Несколько французских участников долевого финансирования уже рассматривали этот вариант использования блокчейна. Однако осенью 2016 года только Enerfip, платформа долевого инвестирования, реализовала*proof of concept* в виде, применимом для ее бизнеса. Enerfip предлагает использовать блокчейн биткойн, взяв из этой технологии систему доступа, тогда как платформа будет играть роль стороннего доверенного лица.

BNP Paribas Securities Services объявила об изучении случая

использования минибонов в партнерстве трех платформ, а также о ведении реестра некотирующихся ценных бумаг. Здесь речь идет скорее об использовании частного блокчейна.

Со своей стороны, профессиональная ассоциация Financement participatif France организовала партнерство с Кассой вкладов и депозитов для того, чтобы проверить использование умных контрактов, опирающихся наэфириум, в отношении минибонов.

Распределенное цифровое голосование

Самой большой проблемой, связанной с голосованием в Интернете, остается, несомненно, безопасность. Благодаря технологии блокчейн избиратель может удостовериться в том, что его голос был успешно передан, оставаясь анонимным для остального мира.

Многие государства используют машины для голосования, которым уже более десяти лет. Эти не слишком удачные конструкции давно устарели, к тому же они становятся все более и более дорогими в обслуживании. Из-за этого растет количество отказов, мошенничества на выборах, что подрывает саму ткань демократии.

Наши правительства должны использовать технологию блокчейн, чтобы добиться большей прозрачности в процессе выборов и, особенно, большего доверия избирателей[166].

В 2014 году либеральный Альянс, политическая партия в Дании, стал первой организацией, использовавшей блокчейн для голосования.

Начиная с октября 2016 года европейский парламент изучает возможность использования блокчейна для голосования. Документ, представленный Филиппом Буше, аналитиком европейского парламента, называется What if Blockchain Technology Revolutionised Voting?[167] и представляет собой взгляд на блокчейн с позиции электронного голосования.

Филипп Буше задается вопросом: является ли блокчейн революционным преобразованием в области электронного голосования в

плане безопасности и прозрачности, и если да, то каковы последствия этого процесса для будущего демократии? В действительности, несмотря на оцифровывание нескольких важных аспектов современной жизни, выборы по-прежнему в значительной степени реализуются на бумаге. С начала века электронное голосование рассматривается как перспективное и (возможно) неизбежное направление развития, которое следовало бы ускорить и упростить, чтобы уменьшить расходы на выборы. Возможно, это даже приведет к более высокой явке избирателей и укреплению демократии.

Интеллектуальная собственность

Поскольку мы уже упомянули о Belem, продолжим говорить о ней и посмотрим, как эта компания открывает путь к новому рынку нотариальных услуг. Belem разработала модуль проверки подлинности информации, который обеспечивает простой, экономичный и надежный способ зафиксировать и защитить личные и деловые данные.

Блокчейн позволяет сохранить датированную информацию, неопровержимую и не подлежащую изменению, факт существования данных или документа, дату и время его создания, с помощью цифровой подписи, функционирующей в качестве доказательства его существования на конкретную дату.

Таким образом, содержание зарегистрированных данных может быть распределенным, будучи одновременно конфиденциальным, но любой может видеть копию этих данных. Безопасность данных относительно обеспечена. Неприкосновенность блокчейна решает проблему уязвимости существующих нотариальных структур.

Модуль проверки подлинности Belem позволяет определить происхождение промышленного патента или идеи, хранить свидетельства о рождении или смерти, доказательства права на жилье и данные финансовых рынков, а также подтвердить платежеспособность и кредитоспособность. Можно оцифровать дипломы, свидетельства о праве собственности на землю или физические объекты (ключи, автомобили, произведения искусства, акции, облигации и т. д.).

Вот еще один пример конкретного использования цифровых приложений, реализуемых с помощью технологии блокчейна.

Анализ данных

Продолжаем говорить о компании Belem, которая разрабатывает очень интересные приложения: «После проверки надежности блокчейна на поле демократии и интеллектуальной собственности мы приступили к разработке инновационной платформы, которая позволяет анализировать конфиденциальные данные без ущерба для конфиденциальности, поддерживая при этом максимальный уровень безопасности».

Таким образом, возможности для применения платформы огромны: финансы, страхование, здравоохранение, электронная коммерция, Интернет вещей и т. д. В общем, в этот круг входят любые сферы, в которых необходимо проанализировать данные, не раскрывая их.

Цепочка поставок / логистика

Этот обзор будет неполным, если мы не опишем наиболее перспективные проекты в области цепочек поставок. Это область, в которой технология блокчейна должна активно развиваться, потому что это сектор, где имеется множество заинтересованных сторон, масса документов, нуждающихся в удостоверении их подлинности, проверок выполнения платежей и подтверждений процесса реализации.

Большинство приобретаемых нами продуктов сделаны не одним лицом или компанией, но прошли через целую цепочку поставщиков, продающих компоненты (например, пластиковую упаковку) компании, которая собирает и продает конечный продукт. Если одного из этих компонентов не хватает или один из участников не соблюдает должную процедуру, производственная цепочка будет нарушена.

Что произойдет, если компания будет обладать защищенными и проверяемыми цифровыми записями, которые показали бы заинтересованным лицам состояние продукта и его местоположение на каждом этапе пути от производителя к потребителю? Это одна из многих идей применения технологии блокчейна в цепочке поставок.

Революционность блокчейна с данными

Технология блокчейна обещает сохранить информацию о сделке, атакже доказательство существования данных или программ и связанной с ними информации в неизменном виде. Две самые важные платформы – биткойн и эфириум – в разной степени обеспечивают эти функции. На сегодняшний день очевидно, что эту неизменность информации гарантируют только доказательство выполнения работы и оплата труда майнеров. Что еще более интересно, это позволяет сохранять данные неизменными за фиксированную стоимость первоначального обслуживания. Что бы ни случилось в будущем, независимо от того, продолжит ли сеть майнеров свою работу или прекратит ее, этот параметр не изменится.

Доказательство существования данных обеспечивается путем расчета криптографических сумм на базе файлов. Эта операция проста. Но, чтобы сделать убедительной сложную систему взаимодействий, включающую множество документов, подписей, сертификатов, временных меток, необходимо связать между собой данные, их контрольные суммы, подписи и сертификаты, атакже временные отметки.

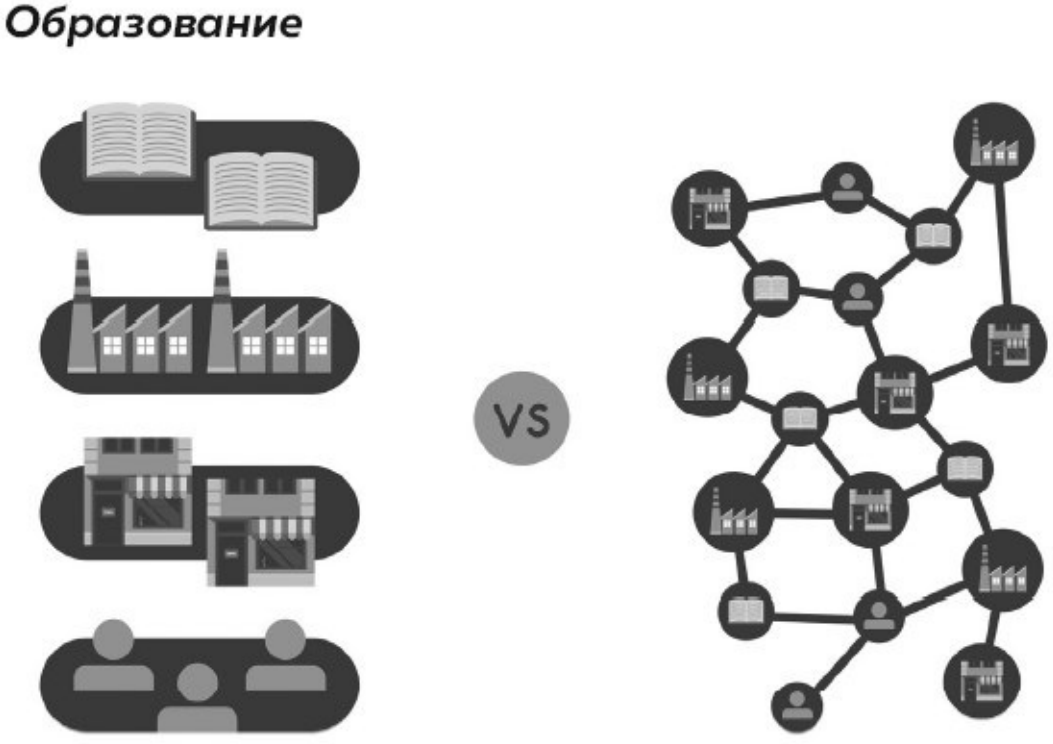
Это решение, защищенное международными патентами французского происхождения, создано французским стартапом, компанией КеееХ[171]. Доказательства целостности файлов преобразуются в личные данные, идентификатор, представляющий собой уникальное имя, доступное для поисковых систем, которое можно использовать в любом документе или другом файле для их идентификации.

Одним из результатов использования КеееХ является тот факт, что данные, организованные согласно их технологии, считаются целостными и подписанными вместе со всем, что с ними связано, без возможности повреждения. Неизвестно ни об одном случае нападения на криптографические хеши, поскольку невозможно создать два файла с одним и тем же «идентификатором личности», а тем более сформировать файл, имеющий тот же идентификатор, что и уже известный. Таким образом, можно развертывать данные и создавать бизнес-процессы, не важно, автоматизированно или при участии людей, главное, что это может происходить без создания инфраструктуры, дополняющей уже

существующую.

Конечно, идентификатор файла естественным образом находит свое место в сделке, записанной в блокчейне. Таким образом, мы создаем непрерывность и доказательность блоков вплоть до данных и файлов. Сочетание биткойна и КееeX также впервые в истории придает большую доказательную ценность цифровому документу, чем оригиналу, написанному на бумаге.

Эта революция в мире документов происходит во всех секторах обработки информации и промышленности: договоры и процессы, осуществляемые по контрактам со многочисленными подписями и датами, надежные и датированные фотографии, заверенные счета, платежные ведомости, расходные документы, дипломы и табели, посланные заказным отправлением с уведомлением о вручении, цифровые удостоверения – вот лишь некоторые возможные варианты.



В сфере образования также разрабатывается множество проектов, потому что наконец при дистанционном обучении появилась возможность

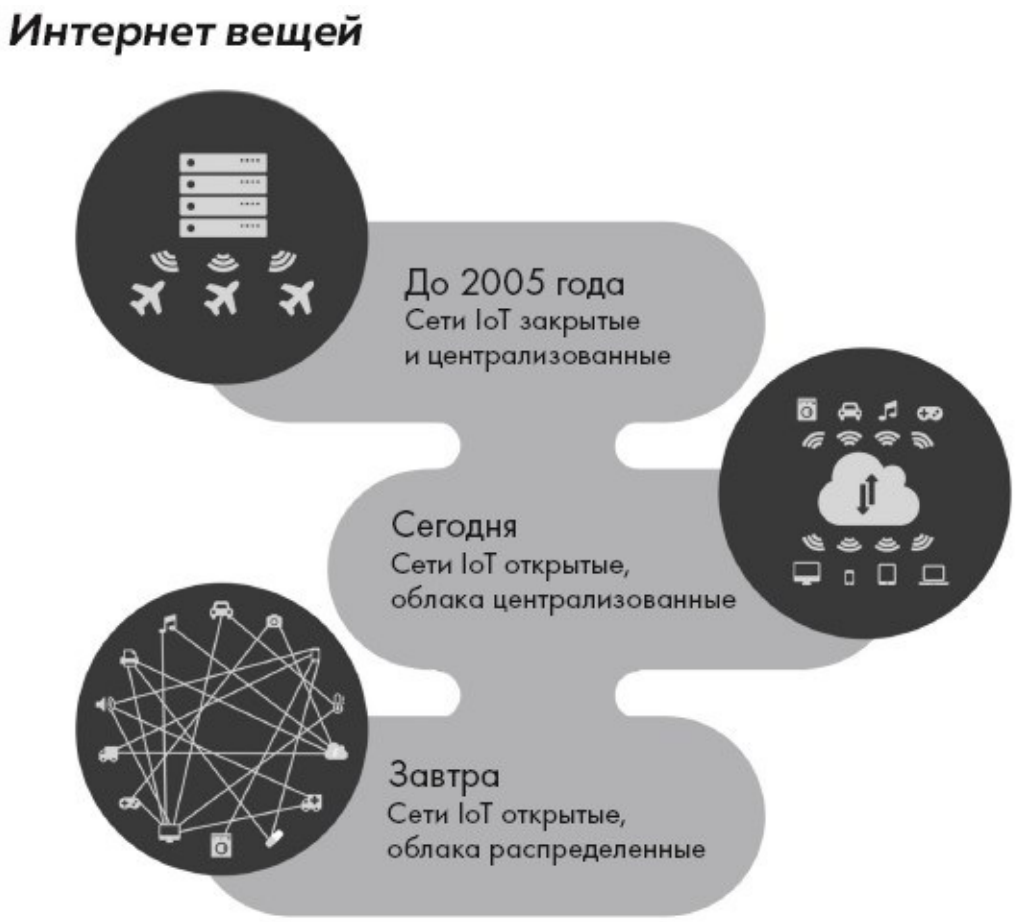
обмениваться информацией, проверять уроки или домашние задания, а также многое другое.

Так, в ходе недавнего исследования Knowledge-Works[172] изучался потенциал использования технологии блокчейна на уровне школы, учителей, родителей и учащихся.

Некоммерческая организация BEN[173] (или Block-chain Education Network) – огромная международная сеть – была основана в 2014 году с целью создания клубов биткойна и блокчейна в университетских городках. Учащиеся совместно со сверстниками изучают этот социально-экономический опыт и создают новые варианты применения блокчейна. В целом совместными усилиями всех этих клубов создается сеть соединенных между собой блокчейнов по всему миру для совместного использования ресурсов и исследования новых вариантов применения этой технологии.

Другой пример – школа Holburton в Сан-Франциско. Это школа разработки программного обеспечения, использующая технологию блокчейна для того, чтобы выдавать свои дипломы и хранить данные о них. В этой системе используются шифрование и двухфакторная аутентификация, чтобы создать диплом, подписать его и поместить в базу данных блокчейна. Школа всегда выдает ученикам бумажные копии, но в системе генерируется децентрализованный компенсационный номер (DCN), который позволяет будущим работодателям осуществлять проверку.

Блокчейн – это технология с отказом от посредничества, которая имеет массу применений в мире обучения на индивидуальном, институциональном, групповом, национальном и международном уровнях и в самом разном контексте: в школе, колледже, университете, интернет-образовании, бизнесе, на предприятиях и при создании баз знаний.



UIT[174] (Международный союз электросвязи) определяет Интернет вещей (IoT) как «глобальную инфраструктуру информационного общества, которая позволяет обеспечить передовые услуги путем передачи объектов, физических или виртуальных, с использованием технологий информации и коммуникации, совместимых с существующими или развивающимися».

Мы можем добавить, что объекты, составляющие этот мир IoT, способны не только просто сообщаться между собой, но также взаимодействовать и, прежде всего, проводить надежные контракты и микротранзакции. Инфраструктура алгоритмического доверия блокчейна идеально подходит для обслуживания потребностей IoT. Благодаря этому, создаваемые сегодня технологии, такие как IoT или beAchain (французский вариант), позволяют разрабатывать огромное количество полезных приложений.

Блокчейн и предприятия, возможность применения

Если мы начнем с постулата о том, что технология блокчейна значительно меняет структуру компании и систему ее работы, то она может быть воспринята как угроза. Если же, наоборот, допустить, что блокчейн может облегчить работу, устранить заторы в сетях, улучшить отношения с клиентами и поставщиками, ускорить финансовые потоки и уменьшить расходы, тогда блокчейн воспринимается как источник дополнительных возможностей.

Блокчейн, разрушительная технология, выгодная для бизнеса

Так же как Fintech[176], которые раскачивают и даже разрушают банковскую и финансовую системы, блокчейн, а также Blocktech[177] могут, в свою очередь, подрывать всю совокупность организаций в глобальном масштабе.

Предприятия ведут битвы на рынках, создавая продукты в постоянно меняющихся условиях. От протокола TCP-IP в веб-сообществе до смартфонов, электронной коммерции и социальных сетей, технологические революции последних десятилетий перемешали все карты и создали цифровую пропасть между различными предприятиями одной отрасли.

Тем, кто не сумел адаптироваться, пришлось заплатить высокую цену (Microsoft и отказ от мобильных телефонов) или просто исчезнуть (Kodak и появление цифровой фотографии). В этой нестабильной среде главной задачей является необходимость уловить технологические изменения на наиболее ранних стадиях.

Учитывая опыт прошлого, можно посоветовать представителям любой сферы внимательно отслеживать все, что в ней происходит, и делать наброски решений в виде блокчейна, чтобы избежать разрушения вашей текущей экономической модели от рук конкурентов, оказавшихся более проворными и гибкими в отношении цифровой трансформации.

Таким образом, после определения принципов технологии блокчейна и ее возможного воздействия на ваш бизнес задайте себе несколько вопросов:

 Какие процессы вашего бизнеса будут изменены или

потенциально затронуты технологией блокчейна?

 Какие риски и возможности возникают в связи с принятой у вас бизнес-моделью?

 Каковы приоритетные направления в области рисков и возможностей?

 Кто будет узлами (участниками) этого блокчейна?

 Какой консенсус будет предусмотрен и какие типы авторизации вы предполагаете настроить в вашем варианте блокчейна?

 Каковы затраты, сроки и ограничения для этой реализации блокчейна?

 Каковы риски, связанные с этим вариантом реализации блокчейна? Каковы возможные последствия?

 Как вы собираетесь организовать испытания блокчейна (PoC)?[178] И на каких процессах?

 Есть ли в вашей компании технические навыки или вам придется передавать вовне всю или часть реализации этого блокчейна?

 Есть ли у вас внутренние ресурсы для проведения этих исследований?

 Работает ли ваша профессиональная организация или коллеги над этой темой?

 Можете ли вы объединить все или некоторые из этих работ с целью повышения результативности и уменьшения затрат?

 Существует ли организация или профсоюз, профессионально посвященные блокчейну, которые могут помочь вам до, во время и после выполнения этого проекта?

Конечно, этот список не является исчерпывающим, и вопросы будут варьироваться в зависимости от типа компании, ее бизнес-модели, уровня цифрового преобразования и т. д.

Они могут также улучшить и рационализировать свою внутреннюю деятельность, процессы, происходящие у них с клиентами и поставщиками. В итоге они могут самостоятельно преобразовать свою деятельность полностью или частично в «цепочку блоков».

ЧТО ТАКОЕ ПРАВИЛЬНЫЙ СЛУЧАЙ ИСПОЛЬЗОВАНИЯ «БЛОКЧЕЙНА КОНСОРЦИУМА»?

Сегодня во всех областях инновационного управления крупными счетами происходит брожение умов, даже FOMO[179], относительно блокчейна и его последствий: технологических, организационных, финансовых и др.

Учитывая масштабы приближающейся смены парадигмы, каждый должен определить возможные последствия влияния блокчейна на свою область бизнеса.

Мы попытаемся поделиться с вами некоторыми мыслями относительно вариантов использования блокчейна в качестве объекта для первых экспериментов.

Все, что может развиться с помощью децентрализованного блокчейна, также может быть реализовано и посредством централизованного подхода. Поэтому нужно понять и изучить, как использовать эту технологию с максимальной эффективностью. Это то, о чем мы уже говорили выше (см. «Примеры использования, приложения»).

Преамбула

В этом примере мы поговорим о «протоколах распределенных реестров» или «протоколах распределенного консенсуса», которые для краткости бы будем называть блокчейном.

Затем речь пойдет о создании «блокчейна консорциума», часто называемого «приватным», даже если мы предпочитаем термин «permissioned» (эксклюзивный), а не о создании сценариев реализации открытых блокчейнов (система оплаты биткойн, сертификация данных и т. д.).

Какой вопрос следует задать?

Первым порывом для любого человека будет спросить: «Какую проблему мы должны решать с помощью технологии блокчейна?»

Но это не совсем правильный вопрос, потому что, говоря о блокчейне, мы говорим о разрушении привычного уклада. Поэтому же, внедряя блокчейн в производство, наиболее логично действовать в соответствии с идеологией Lean Startup[180]. Она позволяет сократить циклы выпуска продукции, регулярно измерять ход прогресса и получать обратную связь от пользователей. Она также позволяет разрабатывать продукты и услуги, удовлетворяющие запросам потребителей, с минимальными первоначальными инвестициями. Именно этот метод мы и предлагаем принять для разработки своего блокчейна.

Характеристики правильного использования блокчейна

Как только этот вопрос будет задан, нужно будет решить, каким образом можно применить распределенные регистры, открытые или закрытые, на вашем предприятии.

Мы сформулировали восемь основных аспектов бизнеса, при наличии которых использование блокчейна будет давать наилучшие результаты:

• если вам *необходимо хранить донные.* Этот аспект является совершенно очевидным, потому что мы говорим о распределенном реестре;

• с *несколькими участниками записи.* Если в нашем случае использования блокчейна имеется только один участник, который записывает данные, блокчейн не имеет смысла. Блокчейн – это система, которая включает нескольких участников записи данных. На сегодняшний день еще не получается отказаться от традиционных баз данных, поскольку они позволяют также осуществлять запись данных несколькими пользователями;

• с *участниками, интересы которых расходятся или между ними отсутствует доверие.* Следует отметить, что расхождение интересов или отсутствие доверия не означают, что это должны быть разные юридические лица. Например, два подразделения одной и той же компании могут работать по различным правилам и с разным видением действительности, вследствие чего данные одного подразделения недействительны в рамках правил и деятельности другого подразделения (например, логистика и бухгалтерский учет не обязательно действуют по одинаковым правилам и используют одни и те же учетные ведомости);

• *при желании или необходимости работать без участия третьих доверенных лиц.* Для реализации блокчейна важно, чтобы его участники имели общее желание запустить распределенный реестр, участником которого будет каждый из них. Среди причин, оправдывающих нежелание использовать доверенного посредника, можно упомянуть следующие: снижение затрат на транзакции, ускорение транзакций, согласование автоматизированного бухгалтерского учета… или просто неспособность участников найти подходящее доверительное лицо;

• *потребность в правилах, контролирующих операции.* Важно определить правила, которые позволят проверять сделки и будут реализованы на уровне алгоритма консенсуса блокчейна. Без возможности определить эти правила технология блокчейна работать не будет;

способность определять, кто будет валидировать сделки. В блокчейне есть валидирующие узлы (часто называемые майнерами), которые участвуют в распределенном консенсусе. Эти узлы играют решающую роль и уполномочены проводить проверку транзакций, которые могут посчитаться вредоносными или привести к конфликтам, связанным со сделками. Поэтому необходимо продумать выбор участников на эту роль для установления баланса полномочий между различными субъектами;

• *взаимодействие транзакций.* Взаимодействие между участниками будет иметь вид транзакций, например, когда речь идет об активе, который меняет владельца или управляющего (пример: сеть поставок);

• наличие *гаранта активов, используемых в модели.* Блокчейн будет моделировать взаимодействие и транзакции между участниками, поэтому необходимо, чтобы компании обеспечили гарантии в отношении активов, которые будут входить в модель (товары, активы, др.), в противном случае реальность блокчейна войдет в противоречие с существующей ситуацией.

Итог

Грамотный вопрос следует сформулировать следующим образом: какую полезную возможность обеспечит нам создание блокчейна? Необходимо, чтобы участники блокчейна имели достаточно веские причины внедрить эту технологию вместо использования третьего доверенного лица.

Конечно, наша цель не в том, чтобы на одной-двух страницах объяснить, в чем заключается метод Lean Startup, мы просто хотим кратко показать, что вы сможете извлечь большую пользу из подхода *proof of concept,* как в отношении экономии и организации времени, так и с позиций финансовой выгоды.

Этот метод появился не в результате попыток выявить проблему и решить ее, он не был продиктован желанием использовать новую технологию – в его основе лежит реальная потребность, высказанная в ходе сеансов «мозгового штурма». В заключение можно сказать, что блокчейн – это рычаг, позволяющий проложить дорогу для инноваций, и способ создания новых услуг или продуктов. Кроме того, это прекрасная

возможность открыть для бизнеса новые горизонты.

Какую технологию использовать?

Что следует использовать для вашего проекта – блокчейн или базу данных совместного пользования?

Мы не будем возвращаться к детальному обсуждению выбора между публичным и частным блокчейнами. Мы уже объяснили, что публичный блокчейн (биткойн, эфириум и т. д.) является открытым для любого участника, который может проверять транзакции и принимать участие в достижении консенсуса. Частный же блокчейн изначально включает в себя контроль над доступом – это означает, что каждый участник, или узел, сети осуществляет контроль над входящими в эту сеть, а также над участниками, обеспечивающими консенсус.

Таким образом, частный блокчейн позволяет финансовым учреждениям поддерживать базу данных совместного пользования и согласованные сделки. Это позволяет каждой организации-участнику читать данные распределенного гроссбуха с гарантией, что все записи в ней легитимны и согласованы с данными, имеющимися у других участников.

Безопасность публичного блокчейна, например, такого, как биткойн, основана на достижении консенсуса или доказательства выполнения работы *(proof of work)* – майнинга, что делает математически невозможным совершение неправомерных сделок или записей и, прежде всего, делает невозможным их изменение или удаление. Кроме того, использование внутри публичного блокчейна криптографии и структуризации, к примеру дерева Меркла, позволяет проверять данные и препятствовать внесению незаконных сделок в цепочку блоков.

В публичном блокчейне доверие возникает скорее вследствие самого процесса, чем из-за статуса участников. В этой распределенной и

безопасной базе общего пользования каждый участник хранит собственную копию данных… платежи валидируются всем коллективом участников и почти сразу появляются в сети. Криптография гарантирует, что сделки могут совершаться только сертифицированными участниками и что существует только одна – истинная – версия транзакции.

Исходя из этих общих положений, касающихся частного и публичного вариантов блокчейна, можно задаться вопросом: не являются ли частные блокчейны просто новым типом баз данных?

Вопрос кажется вполне резонным в связи с тем, что такая база данных может быть распределенной и при этом не обязательно присутствие центрального администратора или третьего доверенного лица. Это создает ощутимый контраст с базами данных типа Б<31_, которые находятся под контролем одного лица, даже если мы можем наблюдать признаки распределенной архитектуры.

С другой стороны, блокчейн, несомненно, обеспечивает большее доверие, надежность и, следовательно, более высокую безопасность информации. Поэтому, если в вашем проекте доверие и надежность не приоритетны, то вы вполне можете обойтись базой данных общего пользования. С другой стороны, если вы ищете возможность полностью избавиться от посредников (отказаться от централизованной власти), то нужно выбирать технологию блокчейна.

ВОПРОСЫ, КОТОРЫЕ СЛЕДУЕТ СЕБЕ ЗАДАТЬ

Если мы продвинемся в своих рассуждениях чуть дальше и будем расценивать умный контракт как «кусок компьютерного кода», который может быть внедрен в базу данных общего пользования, мы, говоря проще, сведем все к вопросу использования алгоритмов и языков. А как насчет умного контракта в блокчейне – когда он должен взаимодействовать с внешним миром?

Следует учитывать производительность. Действительно, сегодня публичный блокчейн будет более медленным, чем база данных общего пользования. Эта медлительность обусловлена задачами, которые призван решать блокчейн, такими как механизм консенсуса или генерация и

проверка цифровых подписей транзакций. (Но и здесь мы могли бы обратить внимание на определенные нюансы, отметив, что некоторые частные блокчейны благодаря своей архитектуре и типу консенсуса или некоторые публичные блокчейны, использующие новые алгоритмы, обеспечивают отличное время отклика.)

Таким образом, если у вас есть проект современного блокчейна, просто помните, что нужно взвесить все достоинства и недостатки выбранного вами типа (публичный или частный блокчейн), базы данных общего пользования и гибридной платформы или архитектуры.

Что касается проекта блокчейна, универсального варианта не существует, так как каждая организация и, как следствие, каждый проект уникальны.

Управление и права

Блокчейн уже много месяцев подряд вызывает огромный интерес. Статьи, симпозиумы, презентации, посвященные этой технологии, имеют большой успех. Банки очень внимательно изучают эту технологию, сознавая всю ее значимость для их работы, а также связанные с ней риски, способные повлиять на их доходы.

Центральные банки не хотят оказаться в числе последних, кто заинтересовался этим новшеством, и даже правительства внимательно изучают, как эта технология может повлиять на государственные финансы.

Если экономический эффект этой технологии становится все более очевидным, то его правовые последствия пока еще плохо определены. Или, точнее, пока не ясно, как закон трактует блокчейн.

В связи с этим возникают два основных вопроса: первый связан с управлением блокчейном, а второй касается юридической силы операции, выполненной с помощью этой технологии. В обоих случаях анализ зависит от типа организации «цепочки», от того, находится ли она в открытом или в закрытом блокчейне. Но в любом случае следует иметь в виду, что блокчейн – это прежде всего технология.

Что такое свободное программное обеспечение?

В мире программного обеспечения следует отделить ПО со свободным доступом от того, которое защищено законом об интеллектуальной собственности.

Программное обеспечение является свободным, только если его лицензия гарантирует четыре основных вида свободы:

- свобода использования программного обеспечения;
- свобода копирования программного обеспечения;
- свобода изучения программного обеспечения;
- свобода изменения программного обеспечения и распространения измененных версий.

Последние два вида свободы могут применяться только в том случае, если имеется доступ к исходному коду, который является в каком-то смысле «рецептом» создания этого программного обеспечения.

Кто является владельцем блокчейна?

Опять же ответ зависит от типа используемого блокчейна.

 В частном блокчейне технология, разработанная органом, уполномоченным управлять им, защищена правом собственности, даже если при создании блокчейна она в значительной степени опирается на исходный код, полученный свободно.

 И наоборот, в публичном блокчейне никто не является «собственником» исходных кодов в соответствии с коммунитарными принципами теории общественных благ.

В финансовой сфере вопрос собственности или контроля над исходными кодами стоит более остро: это вопрос защиты секретных алгоритмов, используемых в некоторых финансовых операциях и разработанных экспертами. Большинство из них не могут быть защищены с помощью патентов или авторских прав.

Юридическая сила сделок блокчейна

Блокчейн – это технология. Конечно, совершенно новая, но это всего лишь технология. Следовательно, операции либо отражают транзакции блокчейна (например, операции обмена валюты или продажи объектов недвижимости и земельного участка), либо сами состоят из транзакций (например, биткойн). Задача развития блокчейна заключается в том, чтобы связать «крипто»-контракты и «реальные» контракты – этот термин объединяет все, что касается традиционной правовой среды.

Почему умный контракт не является полноценным контрактом

«Code is Law» – это одна из фраз, наиболее часто повторяемых для объяснения того, что транзакция, после того как она была выполнена в блокчейне, не может быть изменена или удалена кем-либо без контроля центрального органа. Таким образом, мы готовы сказать, что программы, написанные для блокчейна, играют роль закона, так как они применяются автоматически и действия, которые ими описываются, соблюдаются системой.

Эта особенность, характерная для умных контрактов, на самом деле характерна и для любой компьютерной программы: компьютер выполняет написанный код, точно соблюдая полученные на входе инструкции. Дополнительное свойство блокчейнов состоит в том, что база данных составляется только для чтения, она не может быть изменена, и, в частности, нельзя изменить «сальдо» счетов виртуальной валюты без согласия владельцев адресов. Именно это последнее свойство, которое, по сути, и реализует утверждение «Code is Law», – является ложным, с точки зрения закона, и умный контракт на самом деле не является договором в юридическом смысле.

По сути, умный контракт написан разработчиком и выполняется с помощью машин (узлов, блоков). Если исполнение договора и является непогрешимым, так как оно осуществляется в полном соответствии с его условиями (кодом), то его составление таковым не является. Авантюра с The DAO (см. главу 2) – отличный тому пример. Контракт между инвесторами в The DAO и будущими проектами включал в себя по крайней мере одно предложение, строгое соблюдение которого привело к трансферу около 40 миллионов.

Таким образом, есть ли у нас реальная способность выполнять обязательства, сформулированные в умном контракте? Ответ – очевидно,

нет. Любой мог заметить недостаток, заложенный в умный контракт The DAO, и увидеть, что положение договора не соответствует объекту обязательств, но лишь один человек это понял и воспользовался этим к своей выгоде.

Вторая проблема касается обратимости и возможности нарушить обязательство. После того так трансфер, предусмотренный умным контрактом, но не предусмотренный контрагентами, будет осуществлен, невозможно просто вернуться к предыдущей ситуации, не нарушая основных принципов блокчейна. В случае классического контракта, когда оказалось, что одна из сторон не была правомочна заключать договор, соглашение отменяется судом и его последствия аннулируются. Суд заставляет сторону, которая получила выгоду вследствие сложившейся ситуации, возместить убытки потерпевшей стороне, вплоть до конфискации при необходимости. В случае блокчейна это невозможно, если это не было предусмотрено при создании контракта. Это вторая причина, по которой умный контракт не является полноценным юридическим контрактом.

Так что же делать?

На языке разработчиков, мы говорим о шаблонах компьютерных программ, созданных с учетом определенных заранее принципов или рамок, в которых эти программы перерабатывают существующий код и выполняются в среде, подготовленной в соответствии с заданными принципами работы. Сегодня необходимо, чтобы разработчики и юристы трудились рука об руку для создания шаблонов умных контрактов и соответствующих рамок, структура и характеристики которых соответствуют юридическим законам той страны, где они применяются.

Глава 4

Завтрашний день блокчейна

Будущее создается для того, чтобы его изменять.

Пауло Коэльо

Революция на марше

Экономика и общество знали немало великих потрясений, которые некоторые называют разрушительными или даже революционными. Во всяком случае, в такой ситуации глубокие изменения будут затрагивать очень многие сферы жизни.

Для того чтобы определить и выявить этот революционный потенциал, следует сделать краткий обзор предыдущих революций, оказавших огромное влияние на наши экономики и общества, начиная с XVIII века.

Времена промышленной революции

В период с 1771 года и до наших дней мы можем выделить пять последовательных периодов, в том числе три промышленные революции.

1771 год – 1-я промышленная революция: эпоха механизации промышленности и использования гидравлической энергии

Место возникновения: Великобритания.

Первый пример: мельница Аркрайта начинает работу в Кромфорде.

Новые отрасли промышленности или преобразованные старые: авиация и механизированная обработка хлопка, проковка железа, машиностроение.

Новые инфраструктуры или преобразованные старые: каналы и водные пути, использование гидравлической энергии.

1829 год – эпоха пара и железных дорог

Место возникновения: Великобритания.

Первый пример: испытание паровоза Rocket для линии Ливерпуль – Манчестер.

Новые отрасли промышленности или преобразованные старые: двигатели, паровые машины, шахты по добыче железа и угля, строительство железных дорог, производство подвижного состава, энергия пара используется во многих отраслях промышленности (включая текстиль).

Новые инфраструктуры или преобразованные старые: железные

дороги, почтовая служба, телеграф (на национальном уровне), большие порты, крупные флотские склады и парусники, газ.

1875 год – 2-я промышленная революция: эпоха стали, электричества и тяжелой техники

Место возникновения: Великобритания, США и Германия.

Первый пример: в Питтсбурге, штат Пенсильвания, открывается стальной завод Carnegie Bessemer.

Новые отрасли промышленности или преобразованные старые: дешевая сталь, химия, тяжелая и строительная техника, авиация и электрооборудование, медь и кабели, консервы и бутылки, бумага и упаковочные материалы.

Новые инфраструктуры или преобразованные старые: экспедиции по всему миру на паровых судах, Суэцкий канал, трансконтинентальные железные дороги, большие мосты и тоннели, всемирный телеграф, телефон (в основном на национальном уровне), электрические сети (для освещения и промышленного использования).

1908 год – век нефти, автомобилей и массового производства

Место возникновения: Соединенные Штаты и Германия.

Первый пример: первая «модель Т» завода Форда в Детройте, Мичиган.

Новые отрасли промышленности или преобразованные старые: массовое производство автомобилей, топливо из нефти и дешевая нефть, нефтехимическая промышленность (синтетические материалы), двигатель внутреннего сгорания для легковых автомобилей, транспорт, тракторы, самолеты, танки и электричество, бытовые приборы, охлажденные и замороженные продукты.

Новые инфраструктуры или преобразованные старые: сети дорог, автомагистралей, портов и аэропортов, сети нефтепроводов, электросети (универсальные для промышленности и жилых домов), аналоговые

телекоммуникации (телефон, телекс и каблограммы).

1971 год – 3-я промышленная революция: век информации и телекоммуникаций

Место возникновения: Соединенные Штаты Америки.

Первый пример: о микропроцессоре Intel было объявлено в Санта-Кларе, Калифорния.

Новые отрасли промышленности или преобразованные старые: дешевая микроэлектроника, компьютеры, программное обеспечение, телекоммуникации, контрольно-измерительные приборы, биотехнологии, компьютеры и новые «революционные» материалы (смолы, силикон, керамика).

Новые инфраструктуры или преобразованные старые: телекоммуникации международные цифровые (кабели, оптоволокно, радио и спутниковое телевидение), Интернет, электронная почта и другие электронные услуги, мультимодальная высокоскоростная связь (земля, воздух, море). Интернет порывает с привычной парадигмой работы за счет повышения интенсивности обмена данными в масштабах планеты.

Джереми Рифкин[185] называет эту новую эпоху информации и телекоммуникации, начавшуюся в 1971 году, «третьей промышленной революцией» (или информационной революцией), которая отделила классические отрасли промышленности от производственных и характеризовалась развитием новых информационных технологий и средств коммуникации.

От информационной революции до Web 2.0

Мы могли бы разбить период «технологической революции» на следующие этапы:

• компьютер в 1944 году;

• мэйнфрейм в 1954 году;

• мини-компьютер в 1964 году;

• персональный компьютер в 1974 году;

• Macinstosh в 1984 году;

• Интернет в 1994 году;

• социальные сети в 2004 году;

• блокчейн в 2014 году.

Почему это развитие можно считать революцией?

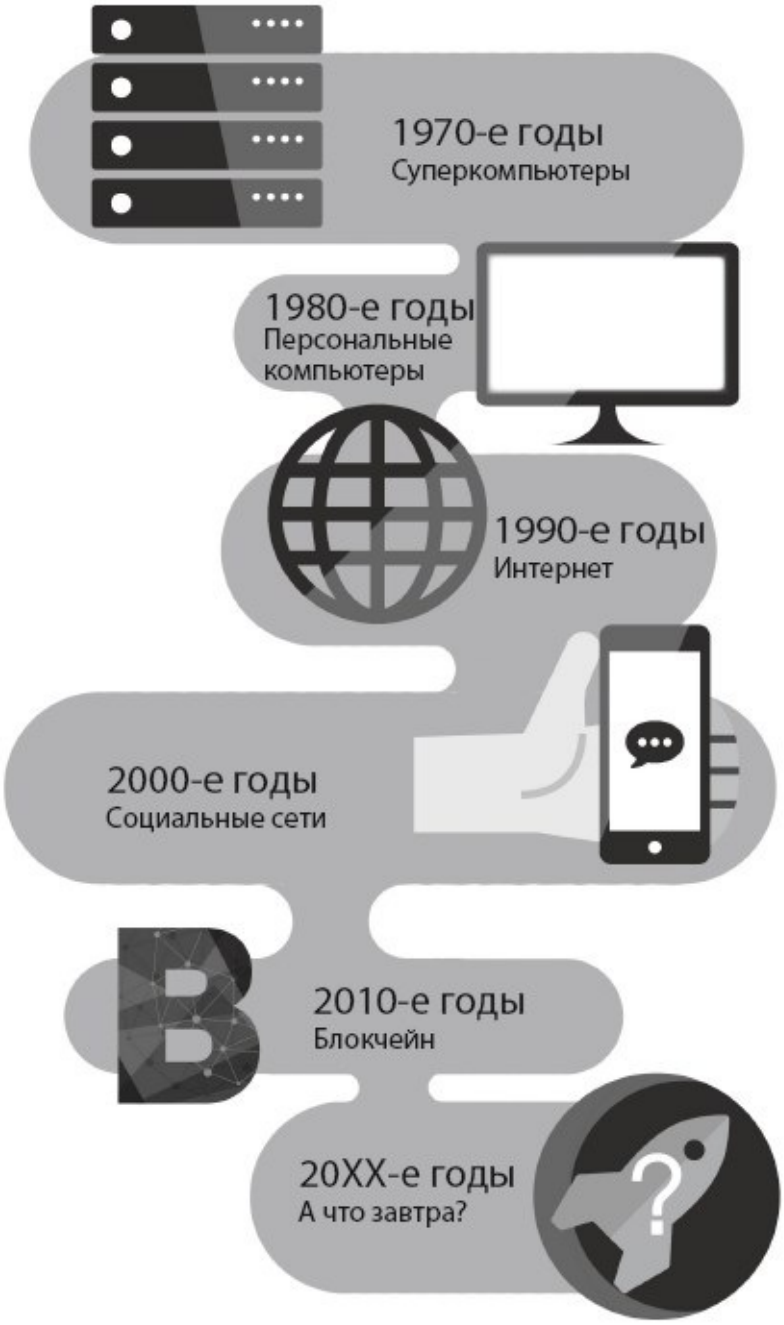
Согласно мнению Карлоты Перес, технологическую революцию отличают и оправдывают ее концепцию, как революции, две основные характеристики:

• сильные взаимосвязи и взаимозависимости участвующих систем, как в области технологии, так и в области рынков;

• способность к глубокой трансформации остальной части экономики (и общества).

Первая характеристика более заметна и определяет то, что в народе

понимается как «революция». Но в действительности именно вторая характеристика – возможность преобразования экономики и общества – оправдывает использование этого термина.



Революция в области технологий – это способность преобразовывать различные отрасли промышленности и создавать новые, двигающие развитие на протяжении длительного периода, вызывая повсеместное

увеличение производительности труда, сопровождающееся реорганизацией экономической и социальной жизни общества.

Попробуем воспользоваться очень простыми рассуждениями: а если энергией этой новой революции был просто компьютер, Интернет? Не находятся ли экономика и общество в центре радикальных преобразований благодаря (или вследствие) этой технологической революции? Разве технология блокчейна, или, более широко, система распределенных регистров, не создается, передается и расширяется с помощью Интернета? В этом случае, если мы признаем правоту этого рассуждения, революция налицо.

Дон Тапскотт, автор книги «Технология блокчейн – то, что движет финансовой революцией сегодня»[188], заявил недавно: «Интернет вступает во второй период. У нас был информационный Интернет. С появлением блокчейна мы наблюдаем за возникновением Интернета ценностей. Существуют огромные возможности для улучшения экономики и управления государством».

Продолжая эту параллель со Всемирной сетью, многие эксперты утверждают, что появление блокчейна выглядит столь же революционным, как и изобретение Интернета. В 1990-х и 2000-х годах Интернет произвел революцию в обществе, потому что он изменил систему поиска данных и общий принцип использования информации в интернет-сообществах. «Блокчейн идет еще дальше, – говорит Даниэль Дьемер, партнер PwC Strategy& Suisse, – блокчейн позволяет обеспечить распределение и управление практически всеми типами данных, в том числе сертификатами собственности, реальными и цифровыми ценностями и даже данными, связанными с идентификацией личности. Короче говоря, эта технология дает возможность распространять, обновлять и координировать любые электронные списки практически в реальном времени».

Возникла ситуация полноценного творческого разрушения, синонима создания рабочих мест и рынков за счет уничтожения других рабочих мест и рынков. Так, в 1942 году в книге «Капитализм, социализм и демократия» Шумпетер объясняет, что «новое не выходит из старого, а появляется рядом со старым, конкурируя с ним до полного его разорения».

Мы считаем, что эпоха Web 2.0 с Интернетом и коллективной экономикой достигает своей наивысшей точки в технологии блокчейна, так как именно она позволит, опираясь на Сеть, Интернет вещей и искусственный интеллект, сделать умнее энергетику, города, здания, автомобили, промышленность, торговлю и т. д. Все для того, чтобы внести в нашу экономику и общество больше прозрачности и доверия.

Поэтому представляется, что введение технологии блокчейна станет следующей революцией.

Мысли и представления

Кризис, связанный с отсутствием доверия в обществе, на рубеже 2007–2008 годов привел к рождению биткойна, а затем к развитию технологии блокчейна в той форме, которую мы видим сегодня. Именно с этого момента в мире финансов веет либертарианским духом[190].

Банки и другие учреждения первыми отреагировали на появление биткойна и попытались завладеть технологией, угрожающей разрушить их налаженную систему, поскольку эта децентрализованная и распределенная технология гарантирует уверенность и прозрачность.

В этом суть обещаний блокчейна.

Было бы заблуждением полагать, что экономика и общество будут меняться и преобразуются всего за несколько месяцев благодаря технологии блокчейна. С другой стороны, мы знаем, что движение началось, и теперь мало что способно его остановить. По всему миру появляются инициативы, связанные с криптовалютами и публичными блокчейнами. Общественные или частные организации начинают масштабные международные блокчейн-проекты. Но какие мысли возникают в связи с этим? Вступаем ли мы в новый мир? Окажет ли эта технология на наш образ жизни какое-то влияние?

Вот три идеи, которые должны лечь в основу наших размышлений.

Американский экономист, который хотел заменить деньги биткойнами

Кеннет Рогофф[191] – экономист с большим стажем, глава международного валютного фонда и профессор Гарвардского университета, объясняет цели системы бумажных наличных денег и ее негативное воздействие на экономику.

В своей недавно вышедшей книге «Проклятие денег»[192], а также во время пресс-завтрака в начале сентября 2016 года Кеннет Рогофф назвал два основных фактора, лежащих в основе его предложения положить конец наличным деньгам: их большой оборот в теневой экономике и неспособность правительства США контролировать потоки наличных.

О наличных деньгах, циркулирующих на подпольных рынках

Денежные средства, носящие название «анонимных», такие как биткойн (защищенные с учетом наличия прослеживаемого публичного государственного реестра сделок), должны стать основной валютой для работы на подпольных рынках.

Сегодня значительная часть незаконной и преступной деятельности осуществляется при помощи наличных денег, из-за чего правительственным учреждениям становится практически невозможно отслеживать поток денежных средств, используемых в незаконных сделках.

Вот почему Кеннет Рогофф предполагает, что правительства, в частности федеральное правительство США, прекратят обращение наличных денег, чтобы уменьшить их поток и таким образом положить конец большинству теневых операций.

Отрицательные процентные ставки

Кеннет Рогофф также считает, что единовременная реализация отрицательных процентных ставок ведущих мировых центральных банков, в том числе Федеральной резервной системы, должна помочь стимулировать экономический рост, потому что теоретически все большее число вкладчиков будет вынимать свои вложенные деньги, чтобы пустить их в оборот.

Некоторые из крупнейших центральных и коммерческих банков уже начали применять отрицательные процентные ставки. В ответ вкладчики начали изымать свои деньги из банков и хранить в различных местах вроде шкафов или микроволновок или вкладывать их в покупку драгоценных металлов (золото, серебро, др.), и следовательно, снова копить.

Роль биткойна

Начиная с момента, когда правительства начнут обдумывать отмену наличных денег, будет построена цифровая система, или реестр, для упорядочивания валют и активов. В результате исследований и в соответствии с ними некоторые центральные банки, такие, например, как Банк Англии, рассматривают возможность использования технологии блокчейна для создания централизованной системы цифровых валют.

В случае если появятся эти сети частных блокчейнов, будет высокий спрос на доминирующие цифровые валюты, такие как биткойны, что увеличит их стоимость, а также их наличие и значимость в крупнейших экономиках мира.

Является ли блокчейн социальной и экономической революцией?

Ценности, созданные за счет Интернета, перешли во владение небольшого числа людей

В конце 1990-х годов однозначно произошла интернет-революция. В то время многие ощутили ветер свободы благодаря открытости ее международных аспектов, выходу из-под контроля и отсутствию жестких правил. Затем в течение нескольких лет вокруг крупных центров притяжения организовались экосистемы, почти новые государства, которые сегодня называют GAFA (Google, Amazon, Facebook, Apple), или, позднее, NATU (Netflix, Airbnb, Tesla, Uber). То, что, казалось, могло дать большую власть народу без контроля государства над реальным сектором экономики, в конечном счете, сосредоточило власть в руках нескольких людей, которые знали, как лучше использовать систему, присвоить ее плоды и извлечь материальную выгоду в ущерб другим. Модель, на конструирование и построение структуры которой потребовалось целых двадцать лет, освободила место для небольшого числа «избранных». В результате эти компании создаются и развиваются за счет свободы и легкости предпринимательства в сети и концентрируют ценности без контроля государства, сосредотачивая их в карманах тех, кто сумел лучше других воспользоваться характеристиками системы.

Блокчейн или возвращение доверия

В течение нескольких месяцев на всех социальных этажах общества – гражданском, экономическом, цифровом и политическом – говорят о новой – цифровой – революции, революции блокчейна. В основе этой технологии лежит криптовалюта биткойн. В журнале The Economist[193] эту технологию называют «машиной для создания доверия». Это реакция на

кризис доверия, сложившийся в политической и финансовой системе за долгие годы. Как это будет происходить? С помощью трех механизмов, составляющих систему блокчейна: асимметричное шифрование, распределенные системы и одноранговая модель функционирования, способная генерировать консенсус в распределенном режиме и без сторонних лиц[194].

Следовательно, блокчейн несет в себе вирус революции, такой же, возникновение которого представлялось возможным с появлением Интернета, но в конечном счете все закончилось усилением контроля, скрытости и гегемонии вместо увеличения личной свободы и перераспределения ценностей. Блокчейн может разрушить эту систему благодаря его способности создавать сеть из людей, которые не знают друг друга, не обязательно должны доверять друг другу, чтобы работать вместе, чтобы совместно создавать ценности и честно делить их прозрачным и безопасным способом. Биткойн – первая реализация блокчейна – является доказательством практической возможности этой модели. Он действительно позволяет людям со всех концов земного шара обменивать деньги без банка-посредника, полностью децентрализованно, прозрачно и надежно, с минимумом расходов, связанных с этой сделкой. Блокчейн отлично продемонстрировал свой экономический и социальный потенциал.

Демократическая технология

Блокчейн имеет демократический характер. Эта технология основана на модели open *source,* отлично зарекомендовавшей себя на протяжении многих лет в разработке программного обеспечения, которая и сегодня гарантирует полную открытость его работы – во всяком случае, для сторонних людей. Изначальное развитие блокчейна и его будущие изменения подчинены воле людей, разработчиков и пользователей, которые могут в любое время принять решение – соглашаться с тем, что им предлагает сообщество, или отклонить это. Также в основе развития системы блокчейна лежит консенсус, не связанный с проверками финансовых операций, циркулирующих в нем. И в этом, кстати, коренятся все блага и трудности, связанные с такой демократической моделью; в самом деле, управление, будучи полностью децентрализованным, без консенсуса не имеет возможности изменить правила. Система, таким

образом, является полностью политической, все поставлено на голосование, борьба за власть, естественно, присутствует, и, поскольку база для обсуждения сугубо технологическая, возможны лишь два варианта: а) сознательное голосование, потому что есть навыки, позволяющие понять, что к чему; б) голосование вслепую, основанное на доверии к разработчикам и самым влиятельным пользователям.

Опасность дрейфа к новой централизованной форме

Мы понимаем, что децентрализация может быстро перейти к новой форме централизации. Мы только что с этим сталкивались в виде концентрации власти, основанной на технических навыках. Но это также верно и для случая, касающегося создания ценностей на базе предоставляемой вычислительной мощности. Так, майнинг, который является основой процесса блокчейна, первоначально базировался на общем участии всех пользователей сети, несущих часть ответственности за проверку сделок и их регистрацию в блок, а затем и в цепочку блоков. Все возрастающая трудность майнинга в блокчейне биткойн – и это также верно в случае блокчейна эфириум – принуждала майнеров объединяться в пулы, позволяющие им увеличить свои шансы получить биткойны и, как следствие, создавать ценности.

Сегодня вычислительные мощности, в конечном счете сосредоточились в нескольких десятках пулов, которые могут в ближайшие годы объединить более 51 % мощности, что создаст благоприятные условия для мошенничества. Поэтому новая форма централизации должна быть продумана разработчиками и пользователями таким образом, чтобы избежать подобного дрейфа, но это невозможно сделать без консенсуса между всеми.

Технология на подъеме, но для нее надо подготовить почву

Благодаря ОАО, технология блокчейна принесла новые, чрезвычайно перспективные формы организации. Они будут способствовать образованию новых форм компаний без централизованной власти и на основе децентрализованного управления. Люди смогут объединяться друг с другом в одном или нескольких проектах без образования иерархических связей между ними. По сути это является наилучшим вариантом

распределения ценностей между участниками, поскольку все определяет код. Но кто будет принимать решение в случае разногласий или конфликта? В случае неплатежеспособности организации, хищения или злоупотребления против кого можно будет возбудить дело?

Таким образом, необходимо преодолеть еще немало проблем, чтобы блокчейн стал той цифровой революцией, какой его называют. Пока эта технология обратила на себя внимание специалистов мира цифровых технологий.

Это не значит, что блокчейн может уйти в небытие или же что проекты стартапа, которые будут запущены на базе этой технологии сегодня, обречены на неудачу. Прежде всего, нужно приспособить ее под себя, чтобы иметь возможность оценить социальные и экономические возможности, которые может дать блокчейн.

Блокчейн – это революция… но революция чего?

Блокчейн поднимает огромное число чрезвычайно важных вопросов. И это не учитывая широкое обсуждение его использования, реального или потенциального (отказ от использования третьих лиц, вопросы защиты сделок, торговли, залогов, технологии совместного использования ресурсов, экономия за счет масштаба, гарантия сделки, автоматическое исполнение контрактов, децентрализация процесса и др.). Возникает и ряд более сложных для решения вопросов.

История общества никогда не бывает гладкой или линейной. За периодами потрясений, жестокими и, как правило, очень быстрыми, следуют гораздо более длительные периоды, во время которых достижения, совершенные в периоды кратких потрясений, составляют основу общего блага. Если эти достижения постоянно перерабатывать, видоизменять, восстанавливать, улучшать, они становятся прочным фундаментом, на котором строится жизнь всего сообщества.

Революции и радикальные изменения

Современное западное общество в том виде, в котором мы его знаем сегодня, существует менее двух веков – со времени революции 1789 года и промышленного переворота, произошедшего в XIX веке. Самые значительные потрясения произошли главным образом в эпоху Возрождения в XIV веке и эпоху Просвещения в период между XVI и XVII веками. Каждая из них создала инструменты, необходимые для осуществления преобразований. Например, типографии изначально были изобретены в эпоху Средневековья, чтобы массово распространять учение христианской веры, но, в конечном счете, они оказались особенно полезны для Возрождения, позволив широко распространить тезисы гуманистов.

Этот пример отчетливо показывает, что технология, какой бы она ни

была, служит для улучшения, изменения и преобразования общества, но никогда не ставит под сомнение ни его основы, ни способы, которыми формируется реальность (например, переход от паровой машины к электрической, преобразовавший производство, не задевая экономические основы, связанные с тем «как производить»),

Блокчейн выделяет пять ценностей

Технологию, помимо того, для чего, по задумке создателей, она была создана, отличает то, что она приносит или не приносит. Вполне вероятно, наш мир, прошедший через ряд изменений, настолько глубоких, что они ставят под сомнение социальные модели, выстраивавшиеся в течение почти двух столетий, в конечном счете решит при помощи блокчейна ряд серьезных проблем.

Эта технология затрагивает по крайней мере пять ценностей: законность, деньги, работу, индивидуальность и демократию. Конечно, ее можно использовать и для того, чтобы ответить и на другие не менее важные вопросы (например, для решения проблемы сохранения окружающей среды, рационального использования энергии и т. д.), но мне не кажется, что блокчейн связан с этими проблемами по своей природе, в то время как пять перечисленных ценностей относятся к нему напрямую.

Ограничивая потенциал блокчейна известными и признанными областями экономики (децентрализованный обмен валюты, упрощенные транзакции, устранение дорогостоящих посредников), производством (моделирование бизнеса будущего 4.0, ОАО), чистыми приложениями (обеспечение безопасности обмена средствами и данными) или управлением (децентрализация, консенсус), мы сужаем свое видение его перспективы. Будучи ограниченными только этими функциями, мы оказываемся не в состоянии принять во внимание более широкую историческую перспективу.

Здесь мы последовательно рассматриваем вопросы законности (как блокчейн оценивается, на основании каких первоначальных допущений), денег (чему блокчейн служит, для чего годится, кто его генерирует), работы (что он производит), личности (как мы себя определяем), и наконец, его связи с политической организацией общества (зависимость от

принципа управления). Таким образом, мы показываем, что в блокчейне заложены теоретические модели, возможности которых выходят далеко за рамки того, для чего его первоначально планировали использовать.

Появление блокчейна

Сейчас возник ряд «практических применений» блокчейна, порой даже противоречащих тому, что утверждалось при его создании. Точно так же, как на вопрос «что такое Интернет и зачем он нужен?» давались совершенно разные ответы в 1996 году, в 2006 году или в 2016 году, вопрос «что такое блокчейн и для чего он служит?» не найдет единого ответа в разнообразии существующих формулировок. Ответ найдется со временем в его изучении и практике применения. То, как и для чего используется блокчейн и что пытаются с его помощью создать, скажет нам больше, чем все рассуждения и гадания, вместе взятые.

Именно в этом промежутке между «сказать» и «сделать» и появляется блокчейн. «Сказать» – значит мыслить только с экономических позиций, соединить логику, лексику и концептуальные инструменты и заявить, например, что «блокчейн обеспечит нам экономию». Это так, но это неверно. Это правда, поскольку таким будет непосредственный краткосрочный побочный эффект. Но это неверно с позиций реорганизации производства материальных благ в долгосрочной перспективе.

Блокчейн – это всего лишь инструмент, который использует мир, вступая в революционный период

Блокчейн – не революция сам по себе. Это всего лишь инструмент, который мир использует, вступая в революционный период. И поэтому, как ни парадоксально, нынешние попытки объяснить эту технологию чаще всего превращаются в рассуждения о том, что мир будущего, скорее всего, будет не лучше настоящего. Блокчейн не может быть описан ни с точки зрения его способности к разрушению, ни с позиций его технических возможностей без риска упустить то, что является самой его сутью: он всего лишь артефакт, осуществляющий перемены в цивилизации; изменения, которые он обещает, могут стать столь же радикальными и разрушительными, какими были в свое время перемены эпох Ренессанса и

Просвещения или промышленная революция для империй прошлого.

Заключение

Когда в 1990-х годах появился Интернет, эксперты предрекали революцию – серьезные встряски технического, экономического и социального характера, сопровождающиеся потерей рабочих мест и различными преобразованиями.

С тех пор прошло почти тридцать лет, и мы должны признать, что, хотя революция не приняла форму объявленного Большого Взрыва, последовательные технологические преобразования изменили большое количество бизнес-моделей, а также экономику и общество в целом, выйдя при этом за рамки, намеченные для них «отцами-основателями». При этом вебу так и не удалось окончательно добиться большего комфорта, большей свободы и большей власти для отдельного человека.

От простой инженерно-технической конструкции, которой веб был в самом начале, мы последовательно пришли к веб-контенту (блоги), веб-торговле (e-commerce), а затем поколения X и Y[196] изобрели социальные сети (Facebook, Instagram и т. д.) и новые способы применения сети, добавив большее разделение и прозрачность, что привело к трансформации общества и экономики. Этот социальный Интернет усилил взаимосвязь контента, породил мгновенную и совместную торговлю, дал людям возможность высказывать свое мнение и предоставил ресурсы для совместной работы.

Но Интернет не остановился в развитии. Он наметил и начал реализовывать новые цели, создавать перспективные модели, такие как BlaBlaCar, Airbnb и Uber. Кстати, именно в Интернете была изобретена уберизация, которая заключается в создании платформы без посредников.

На протяжении многих лет предприятия в значительной степени использовали все то, что предлагает Интернет. Сегодня они обнаруживают новую технологию, блокчейн, а вместе с ней и то, что она обещает и включает в себя. Стоит вспомнить не о способности блокчейна к

разрушению, но о том, что он может преобразовать и улучшить подавляющее большинство бизнес-моделей.

Завтра широкая общественность откроет для себя, благодаря технологии блокчейна и протоколам распределенного консенсуса, отказ от посредников, цифровые валюты, мгновенные транзакции, рыночные площадки и социальные сети без посредника, услуги коллективного страхования без центрального управления, прозрачную демократию, умные энергию и города и многое другое.

После финансового кризиса 2008 года мы потеряли доверие к нашим банкам и финансовым институтам, а затем и к политикам, органам власти, государству… Сегодня мы начинаем больше доверять сообществу, единому «мы», которое выглядит как мы, нашему альтер-эго, и мы ищем новые формы управления.

Начинает вырисовываться совершенно новый мир. После того как мы успешно вошли в мир прозрачности с децентрализованными, автономными и мгновенно действующими СМИ, а затем в мир коллективного пользования с социальными сетями и пространством для совместной работы (wiki), мы видим сегодня возникающее и крепнущее всеобщее доверие *(trust)* и новые варианты его применения благодаря технологии блокчейна.

То, что инициировал и разработал веб, технология блокчейна теперь будет укреплять и развивать. Она производит преобразования, удаляя посредников и вводя протоколы консенсуса. Это целый мир, который будет создан без доверенных третьих лиц – сам Uber станет работать вообще без посредников. Это и окажется высшей степенью уберизации, предсказанной Филиппом Эрленом[197].

Возможно, блокчейну удастся сделать то, чего не удалось добиться Интернету: большей гуманизации, свободы и доверия, идущих из самого сердца этой технологии, и постепенно ввести нас в мир викиномики (где действуют сообща) и трастономики [198] (доверия). Именно это нам и предстоит построить.

Вот и пришло к концу наше путешествие в мир блокчейна, и мы по-

прежнему с большим оптимизмом смотрим на его возможности и многочисленные приложения и их потенциал во многих областях деятельности, а также в экономике и обществе.

Но блокчейн – это не объявленная революция, «это всего лишь инструмент революционного мира».

Благодарности

Поскольку эта книга является результатом сотрудничества многих людей, а не написана одним человеком (не говоря уже о технологии совместной работы!), я хотел бы поблагодарить каждого из экспертов, которые вели меня по этому трудному пути и давали ценные советы. Их знания освещали мне дорогу и во многом способствовали тому, что эта книга увидела свет.

Агости, Паскаль

Паскаль Агости – адвокат и партнер «Каприоли и партнеры» (Адвокатура Ниццы), www.caprioli-avocats.com Он является специалистом по праву, связанному с новыми технологиями, информатикой и коммуникациями.

Доктор права. Преподаватель Университета Ниццы, магистр права в области информации и коммуникации, и Университета Ла-Рошели, магистр в области доверенных третьих лиц.

Бургиньон, Себастьян

Себастьян Бургиньон является менеджером OCTO Technology – консалтинговой компании в области IT-технологий. Он также является экспертом по блокчейну.

Он увлечен цифровыми приложениями, инновациями и стартапами. Он создал блог, в котором делится новостями, связанными с этими тематиками, а также разработал проект #PortraitDeStartuper. Кроме того, он регулярно публикует множество статей о различных платформах. http://sebastienbourguignon.com и http://www.octo.com

Бреги, Ален

Активист электронной демократии / электронной гражданственности и

свободных валютных систем, Ален Бреги является основателем Vol de nuit – компании, занимающейся использованием цифровых инноваций, к которым относятся искусственный интеллект, дополненная реальность, сетевые приложения, платформы коллективного пользования, блокчейн. Он также является соучредителем ассоциации France Blocktech, экосистемы французского блокчейна, и инициатором группы Blockchain Alsace. http://e-vdn.com/ и http://www.france-blocktech.org

Шрики, Видаль

Видаль Шрики является экспертом в области супермассивов данных и распределенных систем, вследствие чего он очень рано заинтересовался технологией биткойн и различными вариантами блокчейна. Он вдохнул жизнь в первую франкоязычную видеосерию *Blockchain Revolution,* посвященную биткойну и блокчейну. http://www.sii.fr

Компарини, Лука

Лука Компарини с сентября 2015 года несет ответственность заблокчейн в IBM France. Имея более десяти лет опыта работы в IT-инфраструктурах, он определяет себя как компьютерного фаната, ориентированного на бизнес, энтузиаста экосистемы с открытым исходным кодом и инновационных областей человеческой деятельности, таких как технологии блокчейна. https://www.linkedin.com/in/lucacompanni

Круазо, Фабрис

Фабрис Круазо окончил Centrale Lyon и HEC. Он является директором компании InTech – люксембургского сообщества из 100 человек, специализирующихся на консалтинге информационных систем и разработке приложений. InTech сопровождает своих клиентов, использующих новые технологии. Фабрис – энтузиаст цифровой культуры, ее развития и архитектуры. Он убежден, что использование принципов децентрализованного доверия, на которых основываются блокчейны, может революционизировать многие виды деятельности в самых разных областях, http://www.intech.lu

Де Воплан, Юбер

Юбер де Воплан – адвокат, партнер Крамера Левина (финансовое и банковское право, альтернативное финансирование, управление активами, цифровые платежи) и администратор France Blocktech, ассоциации экосистемы французского блокчейна. http://www. france-blocktech.org

Делаай, Жан-Поль

Жан-Поль Делаай – ученый и математик, профессор университета в Лилле. Он опубликовал множество статей в Интернете.

Энок, Лоран

Лоран Энок – выпускник Высшей политехнической школы, имеет степень доктора ИТ. Он является преподавателем и исследователем в области искусственного интеллекта, разработки программного обеспечения и интерфейсов «человек-машина». Работы по семантике Web привели его к тому, что он придумал, а затем и создал КеееХ. Эта компания использует несколько патентов, связанных с революционной технологией защиты файлов. http://www. КеееХ. те/

Могайар, Уильям (автор предисловия к книге)

Уильям Могайар живет в Торонто. Он инвестор, исследователь, блогер и автор книги «Блокчейн для бизнеса» (изд-во «Эксмо», 2017 г.). Он является активным участником рынка криптотехнологий, а также советником и членом совета директоров ряда крупнейших мировых компаний, занимающихся технологией блокчейн, в том числе Ethereum, OpenBazaar, Coin Center и Bloq. Он регулярно пишет статьи о настоящем и будущем блокчейнов в Startup Management. http://startupmanagement. org/blog/

Нуаза, Пьер

Пьер Нуаза – блогер[199] (e-ducat), генеральный секретарь ассоциации Bitcoin-France.org и один из основателей Paymiunn.com. Он является автором книги «Биткойн. Инструкция по применению», опубликованной в январе 2015 года, http://e-ducat.fr/

Пешу, Арно

Арно Пешу является менеджером проекта Practice Financial Service в Вейвстоуне. Он запускает крупные проекты преобразований в сфере банковского дела, страхования, промышленности и ритейла. Он также ведет лабораторию блокчейна в Вейвстоуне, цель которой – поддержка своих клиентов в деле открытия и работы потенциальных протоколов блокчейна. https://www.wavestone.com/

Руфаэль, Роман

Ромэн Руфаэль является генеральным директором стартапа Belem, http://www.belem.io

Шмитт, Жан-Люк

Жан-Люк Шмитт является одним из основателей и ведущим сайта Bitcoin.fr. https://bitcoin.fr

Теруцци, Давид

Давид Теруцци является редактором блога blogchaincafe.com. Он специализируется на освещении блокчейна и его вселенной. Является интернет-экспертом сайтов Finyear.com и BlockchainDailyNews. com, консультантом по блокчейну, техническим директором и соучредителем blockchain-conseil.fr, партнером-разработчиком проекта decred.org и программистом. Эксперт в области прикладной математики, http:// www.blockchain-conseil.fr

Вербьест, Тибо

Тибо Вербьест – адвокат и партнер фирмы De Gaulle Fleurance & Associés. Он обладает обширным опытом, в том числе в сфере интеллектуальной собственности и в сфере технологий, СМИ и электронных коммуникаций. Образование: внесен в список адвокатуры Брюсселя и Парижа с 1993 года. Степень магистра в Университете Сан-Диего, степень магистра общего права, экономики и публичного права (Свободный университет Брюсселя).

Вернь, Николя

Николя Вернь – студент ESSEC, вдохновленный миром блокчейна. Он написал небольшое эссе под названием «Горизонты блокчейна».

Я также благодарен Пьеру Лелу, моему сыну, дизайнеру Finyear и Blockchain Dally News, а также иллюстратору этой книги. http://www.leloup.graphics

И большое спасибо вам, мой читатель, что потратили немного своего времени на чтение этой небольшой книги, которая, надеюсь, по крайней мере частично ответила на ваши вопросы, дала пищу для размышлений и помогла в реализации вашего проекта на базе этих зарождающихся технологий.

Ресурсы

2008

Nassim Nicholas Taleb, Le *Cygne noir, la puissance de l'imprévisible,* Les Belles Lettres

2012

Pierre Noizat, *Bitcoin, monnaie libre,* электронная книга

Pierre Noizat, *Bitcoin Book,* электронная книга

Daniel Kahneman, *Système 1/Système 2, les deux vitesses de la pensée,* Flammarion

2013

Philippe Herlin, *La Révolution du bitcoin et des monnaies complémentaires,* Eyrolles

Serge Roukine, *Comprendre et utiliser le Bitcoin,* 19-е издание

Nassim Nicholas Taleb, *Antifragile, les bienfaits du désordre,* Les Belles Lettres

2015

Andreas Antonopoulos, *Mastering Bitcoin,* O'Reilly (перевод на франц. яз., PDF: http://e-ducat.fr/ download/mastering_bitcoin.pdf)

Pierre Noizat, *Bitcoin, mode d'emploi – L'invention d'une liberté,* электронная книга

Jeffrey Tucker, *Bit by Bit – How P2P Is Freeing the World,* Liberty.me

Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller et Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies,* Princeton University Press

Melanie Swan, *Blockchain,* O'Reilly

2016

Blockchain France, *La Blockchain décryptée – Les clefs d'une révolution,* Netexplo

Andreas Antonopoulos, *The Internet of Money,* электронная книга

Alex et Don Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World (2016),*

Портфолио

Paul Vigna et Michael J. Casey, *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic,* Picador

Roger Wattenhofer, *The Science of the Blockchain,* электронная книга

Didier Geiben, Olivier Jean-Marie, Thibault Verbiest et Jean-Francois Vilotte, *Bitcoin et Blockchain: Vers un nouveau paradigme de la confiance numérique?* La Revue Banque

William Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology,* Wiley Henning Diedrich, *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations,* Wildfire Publishing

Arvind Narayanan et Joseph Bonneau, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* Princetown University Press

Nathaniel Popper, *Digital Cold: The Untold Story of Bit-coin,* Harper

Eric Alton, *Blockchain: The Beginner's Guide to the Economy – Revolutionizing Technology,* электронная книга

Terry Parker, *Smart Contracts: The Ultimate Guide To Blockchain Smart Contracts – Learn How To Use Smart Contracts For Cryptocurrency Exchange,* электронная книга

Ghassan Karame et Elli Androulaki, *Bitcoin and Block-chain Security,* Artech House Publishers

Timothy Short, *Blockchain: The Comprehensive Guide to Mastering the Hidden Economy,* электронная книга

Участники

Платформы по обмену данными – Где купить биткойны и/или другие криптовалюты[200]: anxbtc.com/anycoindirect.eu/belgacoin.com/bitboatnet (Фр.)

bitcoin.de

bitcurex.com

bitit.gift (Фр.)

bitstamp.net

bity.com (CH)

btc-e.com

coinbase.com/coinhouse.io (RU)

flipco.in (RU)

kraken.com/lamaisondubitcoin.ru (RU)

localbitcoins.com/mineoncloud.com (RU)

paymium.com (RU)

safello.com

virwox.com

Упомянем особый случай: Uphold.com (ранее BitReserve), платформа, защищающая от уязвимости биткойна.

Исследователи блокчейнов и агрегаторы данных Bitcoin

bitcoinchain.com

bitcoinfees.21.com (расчет стоимости сделки)

biteasy.com

bitnodes.21.com (Фр.)

btc.blockr.io

chainflyer.bitflyer.jp

coinplorer.com

coinprism.info

goochain.net

kaiko.com (Фр.)

oxt. me (RU)

thehalvening.com (Фр)

Материалы по майнингу (Bitcoin/Altcoins)

mineoncloud.com (азиатские майнеры SHA-256, майнеры Asic Scrypt, контракты на майнинг)

la-boutique-du-mineur.com (материалы по майнингу:

Bitcoin и другие альткойны)

rigs.ch (материалы по майнингу)

antminerdistribution.com

Безопасность

badbitcoin.org (черный список мошенников, связанных с биткойном и децентрализованными валютами) bittrust.org (рейтинг магазинов и услуг, связанных с биткойном)

blockchainalliance.org (ассоциация по борьбе с киберпреступностью в блокчейне)

blockchaininspector.com (мониторинг блокчейна, выявление и локализация преступной деятельности)

chainalysis.com (мониторинг блокчейна, выявление и локализация преступной деятельности)

sabr.io (мониторинг блокчейна, выявление и локализация преступной деятельности)

scorechain.com (анализ и оценка адресов биткойна)

Компании Blockchain, Bitcoin, Ethereum и т. д.

Вместо того чтобы приводить список из более 300 наименований и ссылок, мы предлагаем вам посетить «Топ-лист компаний и стартапов», ежедневно обновляемый на Blockchain Daily News: http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html

КОГДА ВЫ ДАРИТЕ КНИГУ, ВЫ ДАРИТЕ ЦЕЛЫЙ МИР

ХОТИТЕ ЗНАТЬ БОЛЬШЕ?

Заходите на сайт:
https://eksmo.ru/b2b/

Звоните по телефону:
+7 495 411-68-59, доб. 2261

Примечания

1

Автор книги «Блокчейн для бизнеса», Эксмо, 2017. – *Прим. ред.*

2

Уберизация – неологизм по названию онлайн-службы для поиска такси Uber. Под «уберизацией» мы будем понимать влияние на секторы экономики сервисов, обеспечивающих координацию деятельности независимых агентов рынка и оптимизирующих взаимосвязи между ними. В данном случае «убер» – имя не собственное, но нарицательное, которое, подобно «ксероксу», будет обозначать целый класс явлений. См. https://pavlyuts. ru/posts/360, где подробнее описана связь Uber с экономикой. *Здесь и далее, если не указано иное, прим. авт.*

3

Сатоси Накамото – псевдоним человека, разработавшего протокол криптовалюты биткойн и его программное обеспечение. – *Прим. ред.*

4

К поколениям X и У относят людей, родившихся в период с 1961 по 1981 и с 1982 по 2004 годы, соответственно. – *Прим. ред.*

5

Квазиреальность – дословно: «как бы реальность», синоним вирутальной реальности. – *Прим. ред.*

6

Нотаризация – регистрация данных защищенной третьей стороной, что в дальнейшем позволяет обеспечить точность их характеристик. – *Прим. ред.*

7

Ориг. названия: Bitcoin и Ethereum. – *Прим. ред.*

8

Одноранговая, или децентрализованная, сеть – компьютерная сеть, основанная на равноправии участников. – *Прим. ред.*

9

Блокчейн – от англ. B1оскИа1п, дословно – «цепочка блоков». – *Прим. ред.*

10

Асимметричная криптография, или асимметричное шифрование, – система шифрования и/или электронной подписи. – *Прим. ред.*

11

ASCII (American Standard Code for Information Interchange) или американский стандарт кода для обмена информацией. Это стандарт кодирования символов в информатике достаточно стар и известен своим неизбежным влиянием на последующие варианты кодировки символов.

12

Филипп Эрлен – экономист и автор книги La Revolution du bitcoin et des monnaies complementaires.

13

http://santanderinnoventures.com/fintech-2-0-paper-highlightsthe-mu Iti-bill ion-dollar-opportunity-open-to-financial-technology-businesses-which-can-help-to-reboot-financial-services/.

14

R3CEV – консорциум, созданный с целью разработки и применения технологии блокчейна в финансовой сфере, в который входят 70 крупнейших финансовых компаний и банков мира. – *Прим. ред.*

15

Digital Asset Holdings: https://digitalasset.com.

16

Боны и минибоны: кредитные документы, дающие право обладателю получить по ним в определенный срок от определенного лица ценности. – *Прим. ред.*

17

В главе 3 читатель найдет подробное описание различных приложений блокчейна. В конце книги приведен список основных проектов, находящихся на стадии разработки или использующихся.

18

http://www.blockchain.vision

19

Ник Сабо – ученый, юрист и криптограф, известный своими исследованиями в области цифровых контрактов и цифровой валюты. Он дипломированный специалист из университета Вашингтона. – *Прим, О ВТ.*

20

RSA Security – компания, аббревиатура в названии которой образована из имен ее основателей: Рональда Райвеста, Ади Шамира и Леонарда Адлемана. Они совместно изобрели криптосистему с открытым ключом с тем же названием – шифрование RSA, которое является криптографическим алгоритмом асимметричного шифрования.

21

Ральф С. Меркле – американский криптограф и исследователь в области нанотехнологий. Он является одним из пионеров асимметричной криптографии наряду с Мартином Хеллманом и Уитфилдом Диффи. В 1974 году он создал головоломки Меркле, первые конструкции с открытым ключом.

22

CPU (Central Processing Unit) – центральное процессорное устройство, главная часть аппаратного обеспечения компьютера. – *Прим. ред.*

23

Хеш-алгоритмы SHA-256 и RIPEMD-160. Двойной хеш SHA-256 используется для получения хеш-блоков и, следовательно, *proof of work*, в то время как SHA-256 с последующим RIPEMD-160 используется для создания биткойн-адресов.

24

Bitcoin Core – это проект с открытым исходным кодом, который поддерживает и выпускает в свет программное обеспечение клиента биткойна, носящее название Bitcoin Core. Это прямой потомок оригинального клиентского программного обеспечения биткойн, созданного Сатоси Накамото после публикации знаменитой книги о биткойне.

25

Автор ссылается на статью «Пропаганда биткойна». Ее оригинал находится по адресу http://www.scilogs.fr/complexites/plaidoyer-pour-le-bitcoin/. В ней собраны ложные сведения, опубликованные средствами массовой информации и банками в 2013 году о Bitcoin. – *Прим. ред.*

26

Проблема византийских генералов // ACM Transactions on Programming Languages and Systems. 1982. Т. 4. N3. Июль.

27

Выдержка из статьи Юбера де Воплана, опубликованной в Finyear.

28

М. *Коррейя, Ж. С. Веронезе, Н.Ф. Невес и П. Вериссимо.* Византийский консенсус в асинхронной системе передачи сообщений: обзор // International Journal of Critical Computer-Based Systems. 2011. Т. 2.

29

Старое название DARPA (Defense Advanced Research Projects Agency), агентство департамента Министерства обороны США, занимающееся новыми военными технологиями и инициативами по ARPAnet.

30

Paxos (Паксос) – это алгоритм, который добивается консенсуса в распределенных системах, передавая сообщения в два этапа коммуникации.

31

Tendermint (https://tendermint.com) – еще один алгоритм консенсуса, устойчивый к проблеме византийских генералов. – *Прим. ред.*

32

Если злоумышленник пытается одновременно потратить свои биткойны у двух получателей, это двойная трата. Майнинг и блокчейн существуют для консенсуса в сети, чтобы определить, какая из двух сделок будет подтверждена и сочтена легитимной.

33

Вычислительная мощность майнеров выражается в хеш/сек (количество хешей, рассчитываемых в секунду) (Килохеш/Мегахеш/ Гигахэш/Терахеш).

34

Пункт подготовлен Дэвидом Теруцци (см. раздел «Благодарности»).

35

Dash (ранее известная под названием Darkcoin) – это криптовалюта, созданная в 2012 году Эваном Даффелдом и представленная широкой публике 18 января 2014 года. Ее первоначальное название, Darkcoin, было изменено 25 марта 2015 года на Dash – сокращение от digital cash, то есть цифровая наличность. См. https://www.dash.org.

36

http://zerocoin.org

37

http://zerocash-project.org

38

https://z.cash

39

https://getmonero.org

40

Об этом более подробно будет рассказываться в главе «Lightning Network».

41

http://altcoins.com

42

Виртуальная валюта, внутренняя для блокчейна, позволяет передавать ценности со счета на счет. Это форма цифровой валюты, основанная на математических методах, использующих методы шифрования для регулирования производства объектов валютной системы и осуществления перевода средств. Кроме того, криптовалюты работают независимо от центрального банка.

43

Источник СоюМагке^ар: http://coinmarketcap.com/all/views/all/.

44

Fiat Money, или Фиатные деньги – валюта, которую правительство объявило в качестве законного средства платежа, несмотря на то что она не имеет никакой внутренней стоимости и не обеспечена резервами.

45

https://litecoin.org/

46

https://namecoin.org

47

http://www.onecoin.eu

48

http://www.potcoin.com

49

http://mazacoin.org

50

https://bitshares.org

51

https://www.dash.org

52

http://blackcoin.co

53

https://viacoin.org

54

https://z.cash

55

Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values // http:// www.finyear.com/attachment/641777.

56

Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox? // https://papers.ssrn.com/sol3/papers. cfm?abstract_id=2393537/.

57

http://coloredcoins.org

58

https://counterparty.io

59

Токенизация – это технология, которая позволяет обезопасить электронные платежи с помощью системы шифрования данных. – *Прим. ред.*

60

Гэвин Андресен является научным руководителем Фонда биткойн. Он владеет криптографическим ключом, который позволяет ему публиковать предупреждение для всех клиентов биткой на. Его персональный сайт: http://gavinandresen.ninja/

61

Персональный сайт: http://www.cypherspace.org/adann/

62

В 1997 году: Адам Бэк изобрел HashCash – систему доказательства работы, – исходя из идеи, выдвинутой Синтией Дворк и Мони Наором в докладе, опубликованном в 1993 году: «Pricing via Processing or Combatting Junk Mail». Адам Бэк позднее стал первым партнером Сатоси Накамото, а недавно – соучредителем Blockstream.

63

http://www.hashcash.org

64

https://blockstream.com

65

См. также проект «Éléments» или «Elementsproject» (https:// elementsproject.org/sidechains), инициированный Blockstream и его сообществом. Вы можете присоединиться к этому проекту и создать собственный sidechain (https://elementsproject.org/ sidechains/creatingyour – own.html).

66

http://www.rsk.co/#l/

67

Полный по Тьюрингу: универсальная машина Тьюринга, которая потенциально имеет возможность вычислить все, что вычислимо. В теоретической информатике машина Тьюринга – это абстрактная модель функционирования механического вычислительного устройства, примером которого может послужить компьютер и его память. Этот шаблон был разработан Аланом Тьюрингом в 1936 году с целью дать точное определение понятию алгоритма или механической процедуры.

68

https://lightning.network/

69

https://lightning.network/lightning-network-paper.pdf

70

http://bitfury.com

71

http://acinq.co

72

«Flare: An Approach to Routing in Lightning Network» (плод сотрудничества соавтора Олаолува Осонтокун и остальной команды сети Lightning), http://bitfury.com/content/5-white-papers-research/whitepaper_flare_an_approach_to_routing_in_ lightning_network_7_7_2016.pdf.

73

https://www.bigchaindb.com

74

https://www.ascribe.io

75

https://www.rethinkdb

76

https://about.me/vitalik_buterin

77

Белая книга/White Paper Ethereum.

78

Ether: валюта блокчейна Ethereum.

79

Первоначальный блок – первый блок в блокчейне.

80

Фонд Ethereum: https://ethereum.org/foundation.

81

Proof of stake, дословно: Подтверждение доли – метод защиты в криптовалюте, при котором вероятность формирования нового блока в блокчейне его участником зависит от доли его владения этой крипто валютой. – *Прим. ред.*

82

См. CoinMarketCap: http://coinmarketcap.com/.

83

https://www.coinhouse.io

84

Smart contracts по Сабо: http://www.virtualschool.edu/mon/Economics/SmartContracts.html и http://szabo.best.vwh.net/smart_contracts_idea.html.

85

Bitcoin is not just digital currency. It's Napster for finance// Fortune. 2014. Январь.

86

См. С. *Бурк и С. Фунг Линг Цуй.* A Lawyer's Introduction to Smart Contracts // Scientia Nobilitat Reviewed Legal Studies. 2014.

87

Как и любая система децентрализованного реестра, проверка стоит дорого, и партнеры должны иметь стимулы для работы; отсюда возникает развитие системы фишек («token») или специфических очков Ethereum – эфира: следовательно, нет майнеров, в отличие от системы биткойн, в котором майнеры оплачиваются биткойнами.

88

https://solidity.readthedocs.io/en/develop/ и https://github.com/ethereum/wiki/wiki/The Solidity-Programming-Language

89

1 Код, используемый в проекте Ethereum, отличается от того, который применяется в биткойне, даже если это и не вдохновляет. Код был переписан полностью. Основным отличием от биткойна является то, что по хранящимся в цепочках блоков сделкам можно неоднократно посылать и получать деньги. В Ethereum имеется квазиязык Тьюринга и, следовательно, распределенная система вычислений: партнеры в сети Ethereum не просто проверяют целостность блоков и добавляют деньги, они выполняют произвольный код приложений, которые вы или я разрабатываем и отправляем по сети.

90

http://www.oraclize.it

91

https://www.codius.org.

92

Чтобы узнать больше о DAO, см. статью «DAO: Contractors и Curators», http://blogchaincafe.conn/dao-contractor-set-curators.

93

https://bitnation.co. – *Прим. овт.*

94

Страхование урожая: https://www.ethereum-france.com/livre-blancwhite-paper-ethereum-traduction-francaise/.

95

«Распределенные автономные организации – каков их правовой статус?», Тибо Вербьест, адвокат, партнер фирмы De Gaulle Fleurance & Associés.

96

В ГК РФ, Главе 53 «Доверительное управление имуществом», это звучит так: «По договору доверительного управления имуществом одна сторона (учредитель управления) передает другой стороне (доверительному управляющему) на определенный срок имущество в доверительное управление, а другая сторона обязуется осуществлять управление этим имуществом в интересах учредителя управления или указанного им лица (выгодоприобретателя)». – *Прим. ред.*

97

Hard fork, см. fork, ветвление: некий объект, имеющий общий корень со вторым объектом. Эти два объекта, поначалу являющиеся близнецами, впоследствии, после разделения, идут каждый своим путем развития.

98

Об этом можно прочитать в статье Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world // https://acnprod.accenture.com/us-en/insight-editing-uneditable-blockchain.

99

Читайте об этом: Виталик Бутерин. On Public and Private Block-chains // https://blog.ethereunn.org/2015/08/07/on-public-and-private-blockchains.

100

Неологизм Виталика Бутерина (эфириум).

101

NXT Whitepaper: https://nxtwiki.org/wiki/Whitepaper: Nxt#Proof_ of_Stake.

102

Источник: КРМС, Джордж Самман.

103

Механизмы консенсуса используются для того, чтобы убедиться, что все узлы сети обладают одной и той же информацией и что в распределенные регистры записываются только допустимые транзакции.

104

Система, которая связывает производительность майнинга с вычислительной мощностью.

105

https://decred.org

106

Метод, при котором цепочка блоков криптовалюты направлена на достижение распределенного консенсуса.

107

Проект БИагсЛпд: http://ethereum.stackexchange.com/questions/ 573/\л/ Ь|аЫ5-а-5Ьагс1.

108

https://peercoin.net

109

https://bitshares.org

110

https://bitshares.org/blog/2015/06/15/the-history-of-graphene

111

https://steem.io

112

https://raft.github.io

113

http://www.the-blockchain.com/docs/JP-Morgan-Juno-Distributed-Cryptoledger.pdf

114

http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf

115

https://lisk.io

116

SCP Stellar: https://www.stellar.org

117

https://ripple.com

118

Алгоритм протокола консенсуса Ripple: https://ripple.com/files/ripple_consensus_whitepaper.pdf.

119

https://www.iotatoken.com

120

DAG (от Directed Acyclic Graph), в переводе – направленный, или ориентированный, ациклический граф, в котором нет направленных циклов. – *Прим. ред.*

121

https://www.hyperledger.org

122

https://www.hyperledger.org/announcements/2016/11/30/hyperledger-хиты-00-member-milestone

123

https://interledger.org

124

TLA+ – акроним наименования «Темпоральная логика действий». Это система формализованных процедур для параллельных и распределенных алгоритмов.

125

https://tendermint.com

126

«Tendermint: консенсус без майнинга», http://the-blockchain.com/docs/TendermintConsensuswithoutMining.pdf.

127

https://monax.io

128

https://www.corda.net

129

http://www.beachain.com

130

http://beachain.com/BEACHAIN-QVO-Paris-NewYork.pdf

131

Для верных биткойнистов существует только один блокчейн блоков. По мнению некоторых эфириумцев, их всего два. Что же касается всех остальных, то, по их мнению, существует столько же блокчейнов, сколько существует распределенных регистров (01_T) с горизонтальными согласованными операциями P2P, не важно, публичных, смешанных или частных.

132

Эти распределенные организации лежат в основе проекта DAO эфириума. Мы впервые видим появление полностью децентрализованной компании, но на сегодняшний день она существует только в блокчейне эфириум, и его участники взаимодействуют друг с другом только в рамках цепочки блоков. Этот тип компании является на 100 % прозрачным, счета и товарообмен между участниками сети публичны.

133

https://openbazaar.org

134

https://arcade.city

135

Жиль Бабине – предприниматель и Digital Champion Франции в Европейской комиссии.

136

Чтобы узнать больше, прочитайте «Transparency Overlays and Applications» (http://dl.acm.org/citation.cfm?id=2978404), очень интересное исследование о прозрачности распределенных сред, в частности блокчейна биткойн.

137

http://cambridge-blockchain.com

138

PoC или *proof of concept* (доказательство концепции) – это демонстрация осуществимости, краткая или неполная реализация какого-либо метода или идеи, позволяющая продемонстрировать ее возможности. Это важный шаг на пути к полностью функциональному прототипу.

139

http://www.blockness.io

140

https://symbiont.io

141

Вы также можете найти ссылки на веб-страницы участников, работающих над этими приложениями, в приложении в конце книги.

142

См. также «Топ 250 компаний и стартапов, работающих с технологией блокчейн», который регулярно обновляется: http:// www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html.

143

Если бы мы могли окинуть взглядом перспективы, предлагаемые блокчейном (см. следующую главу), то следовало бы добавить, что умная сеть, если она связана с распределенной системой огромного числа маломощных микрогидроэлектростанций, должна упоминаться как один из пяти столпов «третьей промышленной революции», объявленной, в частности, Джереми Рифкином. Это означает, что созревающая революция блокчейна произойдет в мире энергетики.

144

https://www.rwe.eom/web/cms/en/8/rwe/

145

Партнерство Slock.it и RWE: https://blog.slock.it/partnering-with-rweto – explore-the-future-of-the-energy-sector-lcc89b9993e6#. cxxxl7p5m.

146

Умные микросети: производство электроэнергии в масштабах района.

147

http://lo3energy.com

148

https://consensys.net

149

http://www.navigantresearch.com/newsroom/worldwidennicrogrid-market-will-surpass-40-billion-in-annual-revenue-by-2020

150

http://www.h4ckenergy.com

151

https://scripts.veredictum.io

152

http://revelator.com

153

Читайте также Music On The Blockchain (Предисловие Nick Mason (Pink Floyd): http://www.blockchaindailynews.com/Music – On-The-BIockchain-Foreword-by-Nick-Mason-Pink-Floyd_ a24414.html.

154

Токенизация – это процесс, который позволяет заменить спорный элемент эквивалентным (или жетоном – токеном), который не будет иметь никакой ценности или смысла после запуска системы.

155

http://www.blockpharma.com

156

https://blockchainhealth.co

157

https://www.pubpub.org/pub/medrec/

158

http://www.enigma.co

159

http://landing.bitland.world

160

http://epigraph.io

161

https://shocard.com

162

https://onename.com

163

https://ripple.com

164

https://setl.io

165

По крайней мере для блокчейнов, работающих с доказательством выполнения работы *(proof of work),* а не с доказательством подтверждения доли *(proof of stake).*

166

В статье, опубликованной на Cryptos.net (http://www.cryptos.net/technologie-block-chain-future-democracie-number/), можно прочесть: «В 2012 году, в ходе выборов в США, результаты выборов в восьми штатах были признаны недействительными или неправильными – это 2,7 миллиона избирателей, зарегистрированных в различных штатах страны. Эти статистические данные ужасны для системы, которая используется для того, чтобы определить будущее страны, особенно для страны столь мощной, как США».

167

Перев.: Что если технология блокчейн произведет революцию в голосовании? – *Прим. ред.*

168

http://vote.belem.io

169

https://voatz.nimsim.com

170

http://www.kinno.fi/en

171

КеееХ, надежные решения с помощью блокчейна: ЬйрэУ/кееех. те/.

172

Learning on the block: http://www.knowledgeworks.org/learning-block-smart-transactional-models/. После обучения «важно, чтобы педагоги и другие заинтересованные стороны рассмотрели все возможные последствия, как положительные, так и отрицательные, которые блокчейн может оказать на обучение в будущем. […] От отслеживания пропусков занятий до реакции на задержку сдачи домашних работ, новые технологии в основном направлены на устранение проблем в школе или классе. Но что если вместо решения проблемы технология откроет двери к познанию?»

173

https://blockchainedu.org

174

UIT: Организация объединенных наций в области телекоммуникаций. Эта организация основана в 1865 году, она насчитывает около 180 стран-участниц. Ее роль заключается в гармонизации развития телекоммуникаций в мире. Штаб-квартира UIT находится в Женеве.

175

Руководитель консалтинговой фирмы Xavier Dalloz Consulting, специализирующейся на отслеживании информационных технологий, http://www.dalloz.com.

176

Организация, которая использует инновационные финансовые технологии для обеспечения или поддержки финансовых услуг.

177

Организация, которая использует технологии блокчейна: http://www.franceblocktech.org.

178

PoC (proof of concept или доказательство концепции) – это демонстрация осуществимости, краткая или неполная реализации какого-либо метода или идеи, чтобы продемонстрировать ее возможности. Это важный шаг на пути к полностью функциональному прототипу.

179

FOMO – это сокращение от английского fear of missing out – страх упустить что-то.

180

Перев.: «Бережливый стартап» – концепция предпринимательства, основывающаяся на научном подходе к менеджменту стартапов, обучению, проведению экспериментов, итеративному производству, измерению прогресса и получению обратной связи от клиентов. – *Прим. ред.*

181

Лоуренс Лессиг (юрист, США). Code is law, On Liberty in Cyberspace // Harvard magazine. 2000. Январь // http:// harvardmagazine.com/2000/01/code-is-law-html.

182

Посмотрите великолепную книгу: *Jeon-Froncois Blanchette.* Burdens of proof. Cryptographic Culture and Evidence Law in the Age of Electronic Documents, Hardcover, 2012.

183

Что касается использования блокчейна в операциях оплаты/поставок в финансовой сфере, то следует рассмотреть потрясения, которые может принести эта технология: частный децентрализованный реестр может завтра заменить центральные депозитарии, такие как Euroclear, DTCC и прочие, с учетом предварительного регулирования юридических вопросов, связанных с правами собственности владельцев ценных бумаг. См. *Поскаль Бувье.* Distributed Ledgers Part II: Clearing, Settlements and Legal frameworks // http://finiculture. com/distributed-ledgerspart-ii-clearing-settlements-and-legal-f ram e works/.

184

Теперь можно сохранить в блокчейне неопровержимое и неудаляемое доказательство с зафиксированной датой и временем о наличии документа, не раскрывая его содержание. *Proof of existence* включает в себя не сам документ в реестре, но его простой отпечаток, который позволяет доказать, что документ существовал в определенное время и был привязан к определенному адресу.

185

Джереми Рифкин – американский эссеист, специалист по научному прогнозированию в области науки и экономики. Jeremy Rifkin and the Foundation on Economic Trends: http:// www.foet.org.

186

Арно Пешу, компания Wavestone: https://www.wavestone.com/fr/

187

В перев.: Выход протокола блокчейна из тени. – *Прим. ред.*

188

«Технология блокчейн – то, что движет финансовой революцией сегодня» (изд-во «Эксмо», 2017 г.). Это третья книга Дона Тапскотта после Digital Economy, изданной в 1994 году и посвященной работе и совместному производству с помощью новых технологий связи, таких как Интернет, и «Викиномики. Как массовое сотрудничество изменяет все» (изд-во Best Business Book, 2009 г.), написанной в 2006 году, в которой автор подробно рассматривает проблему коллективного разума.

189

Цитата Юбера де Воплана, адвоката, из статьи, опубликованной в Finyear.

190

Либертарианство – это политическая философия крайнего либерализма в рамках системы собственности и универсального рынка, провозглашающая индивидуальную свободу краеугольным камнем естественного права.

191

Американский экономист: http://scholar.harvard.edu/rogoff/.

192

http://press.princeton.edu/titles/10798.html

193

http://www.economist.com/news/leaders/21677198-tech nologybehind–bitcoin-сои Id-transform– how-economy-works-trustmachine/

194

http://www.fondapol.org/wp-content/uploads/2016/06/ 083-SOUDOPLATOF-2016-05-26-webDEF.pdf

195

Пик завышенных ожиданий может быть определен как «раскрутка в средствах массовой информации, которая приводит к завышенным и нереалистичным ожиданиям. Проекты стартапа, созданные для развития и коммерциализации продуктов, основанные на новой технологии» (источник: «Википедия»).

196

Поколение Х объединяет людей, родившихся между 1966 и 1976 годами (примерно), поколение У – тех, кто родился в период с начала 1980-х годов и до середины 1990-х годов.

197

Филипп Эрлен, экономист и автор книги La Révolution du bitcoin et des monnaies complémentaires.

198

http://www.trustnomics.net

199

«Я публикую этот блог, чтобы все узнали о преимуществах разнообразия валютных систем, а также чтобы поставить под вопрос идею о том, что монополия евро желательна или необходима. Денежные обязательства, навязанные как единственно возможная валютная система, способствуют власти правящей олигархии и увеличению неравенства…»

200

Рейтинг обновляется каждый месяц: https://bitcoin.fr/acheter-bitcoin/.