Не только биткоин

или Как технология блокчейн меняет современный мир

Добыча криптовалют — это всего лишь один не самый интересный и эффективный путь использования гениальной технологии блокчейн. Помимо широко известного майнинга, «цепочки блоков» используются в финансах, медицине, торговле, государственном управлении — всего и не перечислить.

Блокчейн — явление относительно новое. Исторически первая массовая работающая реализация системы такого рода была создана для запуска криптовалюты Bitcoin в 2008 году. По преданию, разработал ее гений-одиночка Сатоси Накамото, но этого человека никто никогда не видел. Учитывая сложность и техническое совершенство разработки, очевидно, что в данном случае речь идет о псевдониме, под которым скрывается группа лиц или даже целая организация. Как бы то ни было, но сегодня тема криптовалют неимоверно разогрета, а биткоин является наиболее известным представителем этого семейства активов. Поэтому часто в массовом сознании происходит путаница понятий, в результате которой между такими терминами, как «блокчейн», «биткоин» и «криптовалюта» ставится знак равенства, хотя это верно лишь в одном частном случае. На самом деле сфера использования технологии блокчейн гораздо шире, чем создание и поддержка криптовалют.

Хотя, конечно, взглянув на цифры, причина упомянутой путаницы становится очевидной — общая стоимость всех криптовалют, функционирующих сегодня в мире, оценивается в сумму около $400 млрд (согласно данным специализированного сайта coinmarketcap.com) — конкретный показатель существенно зависит от курсовых колебаний. При этом рынок остальных блокчейн-решений, находящихся вне сферы криптовалют, по данным исследовательской компании Research and Market, должен преодолеть планку в $6 млрд лишь к 2023 году.

История развития блокчейн

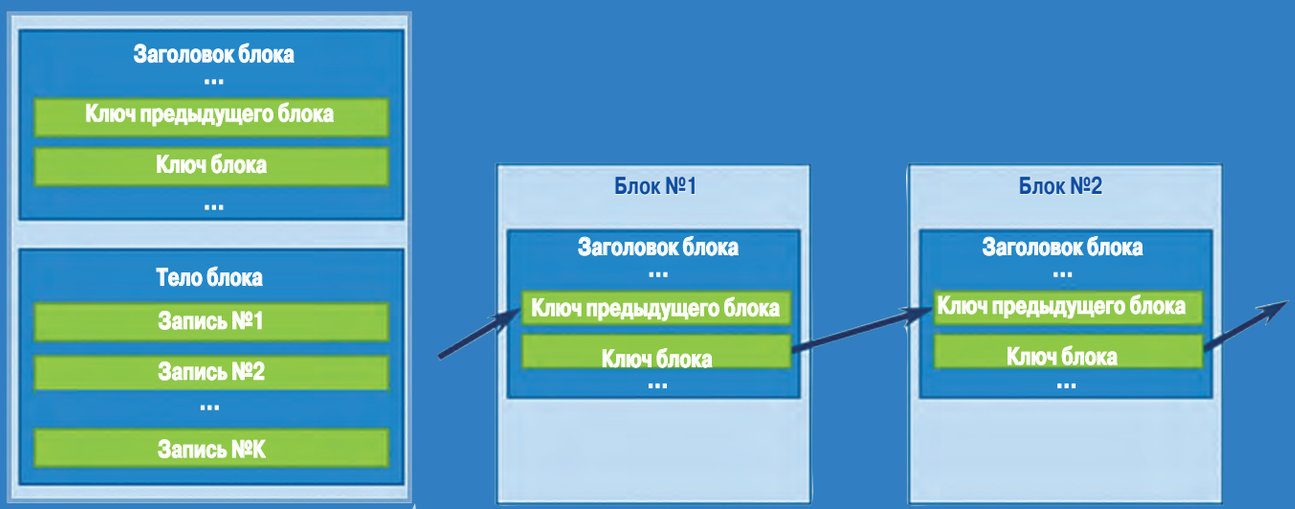
КАК РАБОТАЕТ БЛОКЧЕЙН

Термин «блокчейн» (blockchain) дословно переводится как «цепочка блоков», что очень точно отражает суть технологии. В ее основе – полностью реплицированная распределенная учетная база данных транзакций, информация в которую вносится в виде особых блоков. Каждый блок представляет собой запись о группе транзакций и к тому же содержит ключ предыдущего блока, благодаря чему выстраивается непрерывная взаимосвязанная цепочка данных.

Каждый блок содержит фиксированное число записей о транзакциях, происходящих в рамках определенной сети передачи данных, участниками которой являются два типа узлов – «ноды» и «майнеры». Первые могут только вносить записи, вторые занимаются добавлением блоков в общую цепочку по мере их заполнения.

Важным моментом является то, что когда новый блок добавлен – информация о нем передается всем участникам сети. В результате на каждом узле имеется актуальная база данных обо всех осуществленных транзакциях. Создать новый блок могут только «майнеры» путем решения особого математического уравнения с единственным возможным и неповторимым решением, результат которого содержит ключ предыдущего блока, сумму контрольных чисел транзакций, осуществленных за определенный период (например, в случае биткоин – 10 минут) и значение некоторого случайного числа. «Майнеры» фактически соревнуются в скорости решения уравнения. Выигрывает тот, у кого вычислительная мощность выше, он же получает эксклюзивное право записать новый блок в общую цепочку. Если речь идет о криптовалютах, то за каждую новую запись блока участник сети получает определенное вознаграждение. Скажем, в системе биткоин это – 25 условных «монет».

Поскольку блоки имеют последовательные ссылки друг на друга, любое несанкционированное изменение хотя бы в одном из них вызовет изменение ключа, и, как следствие, конфликт данных во всей цепочке, что будет моментально выявлено всеми участниками сети. Более того, любая транзакция обрабатывается всей сетью пользователей, что позволяет создать очень надежный механизм достижения консенсуса в определении надежности вносимых данных. Так что незаметно исказить уже имеющуюся информацию не получится. К тому же, поскольку у каждого участника имеется своя полная и актуальная копия БД, система будет оставаться работоспособной до тех пор, пока остается активным хотя бы один вычислительный узел. Также для защиты доступа к сети и данным используются специальные криптографические алгоритмы (SHA 256, Scrypt и другие).



Блок транзакций и связь блоков в цепочке

В широком смысле идея блокчейн долгое время лежала на поверхности, но лишь около десяти лет назад вычислительные мощности, доступные рядовому пользователю, стали столь существенны, что это сделало возможным практическую реализацию механизма. Первым известным продуктом, созданным на базе рассматриваемой технологии, стала криптовалюта биткоин, появившаяся в 2009 году. Поэтому нередко именно с ней ассоциируют и термин блокчейн. Первое время это действительно было так, но очень скоро выгоду нового механизма обмена данными оценили во многих сферах, таких как финансы, государственное управление, медицина — список постоянно расширяется, не говоря уже о том, что блокчейн используется для создания все новых криптовалют.

В общих чертах, технология блокчейн представляет собой полностью реплицированную распределенную базу данных, состоящую из выстроенных по определенным правилам непрерывных последовательных цепочек информационных блоков. Это значит, что на всех вычислительных узлах, участвующих в процессе работы системы, имеются актуальные копии БД, которые постоянно синхронизируются. Любое изменение сообщается сразу всем узлам, а значит, повреждение или отключение любого из них не сказывается на устойчивости и работоспособности всей базы данных. Более того, актуальные данные будут существовать до тех пор, пока имеется хотя бы один работоспособный узел. Второй важный фактор заключается в том, что любая запись (транзакция) вносится в БД по определенным правилам и защищена мощными криптографическими алгоритмами. Описанные принципы делают блокчейн поистине революционной и незаменимой технологией там, где требуется четкий контроль над внесением, изменением и хранением важных данных.

БИТКОИН И ДРУГИЕ

- В мире сегодня существуют более 1600 криптовалют, 99% из которых практически неизвестны широкому кругу людей.
- Общая капитализация всех криптовалют в мире составляет более $388 млрд.
- Самая «дорогая» криптовалюта – биткоин, ее капитализация составляет $145,6 млрд*), на втором месте – Etherium ($67,4 млрд*), на третьем – Ripple ($27 млрд*).
- Лишь 24 криптовалюты (1,5% от общего числа) имеют капитализацию свыше $1 млрд*).
- Китайские компании контролируют до 3/4 мировой добычи криптовалют.
- В мире действуют около 50 сервисов по обмену криптовалют (крупнейшие – в КНР).
- Самая популярная пара на криптовалютном рынке: юань-биткоин

*) Данные сайта coinmarketcap.com на момент подготовки публикации

Финансы, собственность и государственное управление

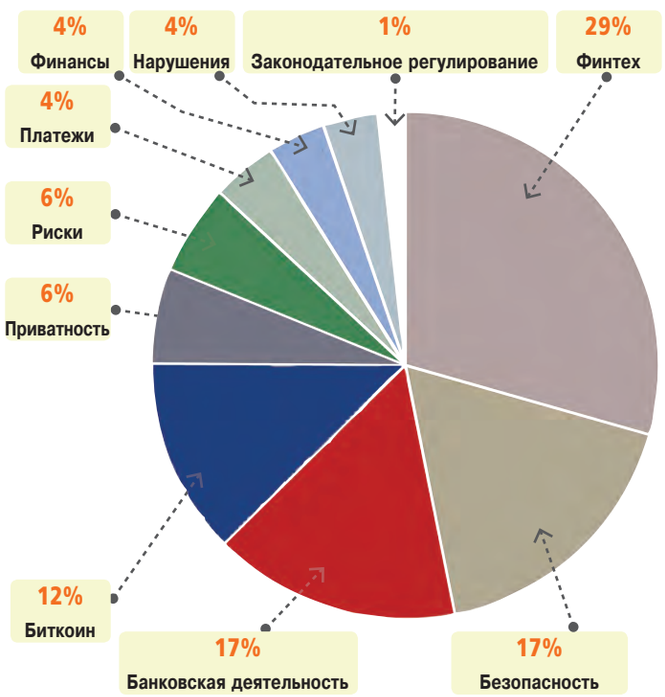
Если не брать в расчет сегмент непосредственного создания виртуальных денег, то сегодня технология блокчейн чаще всего используется в финансовой сфере, что неудивительно, учитывая важность корректной записи, учета и обработки транзакций. Например, на базе блокчейн создаются специальные виртуальные «кошельки» для операций с теми же криптовалютами — их хранения, обмена, конвертации и т.д. Создаются программные системы для осуществления защищенных банковских переводов, фиксирования залогов, ведения документооборота. Ряд компаний (в их числе R3, DAH) даже пробуют сегодня создать альтернативу международной межбанковской системе передачи информации и совершения платежей SWIFT.

По мнению экспертов, одним из наиболее перспективных направлений использования блокчейн в ближайшем будущем являются т.н. смарт-контракты (или «умные контракты»). Суть явления в том, что благодаря специальным математическим алгоритмам договор, заключенный между субъектами в рамках блокчейн-среды, исполняется автоматически, по достижении оговоренных условий. Иными словами, после подписания смарт-контракта всеми сторонами, не выполнить его условия уже невозможно. В этом заключается принципиальное отличие «умных контрактов» от обычной юридической практики, где речь главным образом идет о доверии или угрозе судебного разбирательства. В то же время, хотя смарт-контракт исключает нарушение договора, но для его исполнения требуется ряд специальных требований. Главная проблема заключается в том, чтобы корректно описать условия сделки в математических терминах и вести их в автоматизированную среду исполнения на базе блокчейн. Пока что это сложно и работает только для достаточно простых сделок. Поэтому случаи применения смарт-контрактов за пределами сферы операций с самими же криптовалютами пока что немногочисленны, но потенциал здесь очень велик. Если удастся сделать смарт-контракты удобными для применения, то это может радикально преобразить глобальную деловую среду — сделки будут совершаться быстро (минуты вместо дней), без ненужных посредников и гарантов исполнения.

Блокчейн может широко использоваться для нужд государственного управления и контроля. Причем в этом случае ценность и полезность технологии наиболее очевидна. Косвенным подтверждением этого является тот факт, что, по данным компании BitFury, сегодня в мире свыше 190 стран используют или пытаются внедрять блокчейн-технологии в работу своих госструктур.

Очевидной сферой использования блокчейн является создание различных реестров, регистрирующих права собственности (в т.ч. интеллектуальной) и исключающих при этом возможность подмены или несанкционированного искажения внесенных данных. Такие реестры используются сегодня во многих странах. Например, в нашей стране, Государственная служба Украины по вопросам геодезии, картографии и кадастра (Госгеокадастр) использует технологию блокчейн для предоставления сервисов «Регистрация земельного участка» и «Предоставление ведомостей из земельного кадастра». Технической основой решения является разработка американо-грузинской компании BitFury — Blockchain Exonum. Она же применяется в работе торговой платформы для реализации арестованного имущества OpenMarket.

Отметим, что система Exonum сначала была успешно опробована для таких же целей в самой Грузии еще в 2016 году — одним из важнейших результатов стало то, что стоимость регистрации земельного участка сократилась с $50–200 до $0,1, значительно уменьшилось



Темы, связанные с блокчейн, которые чаще всего обсуждались в мировом Интернет-сообществе. По данным компании Onalytica IRM

и время процедуры, она стала гораздо быстрее и удобнее. В дальнейшем проект был расширен на сферу госзакупок и нотариальных услуг. Столь существенная финансовая экономия была получена за счет того, что во многих случаях за счет применения доверенной технологии исчезла необходимость в заключении множества промежуточных договоров и контрактов с большим числом посредников, среди которых банки, юристы, риелторы и т.д. Вся цепочка покупки/продажи существенно сократилась, что радикальным образом сказалось на конечной стоимости процесса.

Собственные проекты регистрации прав собственности на землю и другие активы с использованием технологии блокчейн ведутся в Странах Африки, Южной Америки, Ближнего Востока, Швеции, Индии, России. Причем в последнем случае рассматривается возможность применения подхода для учета сделок с коммерческой и жилой недвижимостью, автомобилями и т.д. Отметим, что в мире существует целый ряд успешно работающих международных коммерческих блокчейн-сервисов, ориентированных на риелторские услуги (например, Ubitquity или Silvertown), которые позволяют сделать бизнес в сфере торговли и аренды недвижимости более удобным и безопасным, максимально исключив при этом традиционную бумажную волокиту. А в Арабских Эмиратах вообще принята госпрограмма, согласно которой к 2020 году весь официальный документооборот будет работать на блокчейн-платформе.

Если смотреть еще дальше, то на базе системы распределенных реестров в будущем можно создать платформу тотального учета государственных расходов по каждой структуре или реализовать систему для голосования, данные в которой будет чрезвычайно сложно фальсифицировать. На уровне государств такие решения еще не созданы, но вот в корпоративной среде они начинают успешно работать. Например, в 2018 году известная NASDAQ — одна из трех основных бирж США — внедрила у себя систему электронного голосования e-Voting, с помощью которой регистрируется волеизъявление акционеров компании при выборе должностных лиц и назначении их на ответственные посты. По сути, система представляет собой своеобразную криптовалюту, где каждый избиратель, обладающий правом голоса, получает некую сумму условных «монет», которую он может перечислить на счет кандидата. Побеждает тот, у кого по итогам раунда окажется больше «денег». При этом все операции прозрачны с точки зрения переведенных «сумм», но в то же время они позволяют обеспечить анонимность избирателя, сохраняя принцип тайного голосования.


Типичная криптовалютная ферма

В целом сфера корпоративного управления может стать некой подготовительной базой перед началом масштабного внедрения блокчейн в госорганах. Системы на базе распределенных реестров используются в некоторых крупных корпорациях уже сегодня. Например, в сфере управления и учета финансов

«СОЧЕТАНИЕ СЛАБОУМИЯ И БЕЗНРАВСТВЕННОСТИ»?

Термин «криптовалюта» состоит из двух частей: «крипто» (греч. kryptos – тайный, скрытый) и «валюта» (итал. valuta – стоимость, монета). Именно вторая часть вводит в заблуждение многих людей, полагающих, что это явление имеет отношение к истинным валютам или, например, к деньгам. На самом деле криптовалюта представляет собой специфический товар или актив, что роднит его, скорее, с акциями или даже товарами. Например, Томас Джордан – председатель Швейцарского национального банка, охарактеризовал криптовалюты скорее как инвестицию.

Есть и более жесткие оценки. Так, один из богатейших людей мира Уоррен Баффет – председатель и главный исполнительный директор Berkshire Hathaway – в начале мая 2018 года назвал биткоин «крысиным ядом». Чарли Мангер – вице-председатель этой же компании – охарактеризовал данную криптовалюту как «антисоциальный, глупый и безнравственный» продукт, а пропаганду цифровых активов назвал «сочетанием слабоумия и безнравственности».

Как бы то ни было, но сегодня любая криптовалюта, в частности биткоин, представляет собой исключительно спекулятивный актив с непрогнозируемой стоимостью. Это вносит в процесс работы на данном рынке столь высокий элемент неопределенности, что превращает последний в своеобразный вариант глобальной азартной игры.

существуют достаточно популярные сервисы BoardRoom и Otonomos. Интересным прообразом идеальной блокчейн-системы для госуправления можно назвать проект Bination, в рамках которого сегодня функционирует некое виртуальное трансграничное государство, стать гражданином которого может любой желающий. Оно имеет многие номинальные атрибуты настоящей страны — население, правительство, диппредставительства и т.д. Данные обо всех действиях, совершенные в рамках сообщества, хранятся в распределенных реестрах. Возможно, опыт работы подобной системы пригодится в дальнейшем при внедрении блокчейн в рамках настоящего государства.

Существуют также инициативы, призванные бороться с плагиатом и пиратством в сфере интеллектуальной собственности. Для музыкальных произведений уже сегодня работают блокчейн-проекты ASCAP, SACEM, dotBlockChain, JAAK, Paperchain, которые позволяют не только однозначно зарегистрировать автора, но и отследить корректное использование музыки потребителем в соответствии с оплаченными правами — для личного или публичного использования, озвучивания фильма и т.д. Имеются решения, ориентированные на видеоконтент, тексты, даже на отзывы и комментарии. Так, ресурс Ascribe предназначен для торговли произведениями визуального искусства (картины, дизайны и т.д.). Интересно здесь то, что с помощью блокчейн подтверждается не только авторство объекта, но и факт его продажи, передачи прав на использование и т.д. И подобных сервисов сегодня уже немало: Proof of Existence, Monegraph, Bitproof, Blockai, Stampery — лишь некоторые из них.

При этом если возникнет необходимость, данные из распределенного реестра могут стать доказательством в суде. Пока что ни одного подобного прецедента отмечено не было, но, похоже, это лишь вопрос времени.

Лекарства и другие товары

В числе насущных проблем, которые стоят в мире достаточно остро, особенно выделяется такое неприятное и даже опасное явление, как фальсификация различных важных или дорогостоящих товаров, в частности медикаментов. Бороться с этим явлением сегодня помогает технология блокчейн, с помощью которой удается полностью отследить всю цепочку поставок тех или иных лекарств — от производства до конечной точки реализации. В Израиле, США и ряде стран ЕС распределенные полностью реплицированные базы данных используются для ведения медицинских записей о пациентах. В этом случае блокчейн, во-первых, позволяет свести разрозненную информацию из разных баз данных, а во-вторых, исключить фальсификацию сведений (например, когда тот или иной факт вносится «задним числом»). Типичный пример решения такого рода — система MedRec, разработанная совместными усилиями клиники Beth Israel Deaconess Medical Center и MIT Media Lab. Единую базу медицинских карточек пациентов на базе технологии блокчейн реализует правительство Эстонии, есть похожий проект в Нидерландах, ведутся пробные запуски в других странах.

Кроме того, блокчейн позволяет вести учет особо ценных или потенциально опасных товаров. Так, сервис The Real Asset Company ориентирован на глобальный учет оборота металлического золота и позволяет отследить судьбу любого слитка массой от 1 грамма, информация о котором будет внесена в систему. Похожая разработка существует и для отслеживания движения алмазов.

НОВАЯ КАСТОВАЯ СИСТЕМА ПО-КИТАЙСКИ

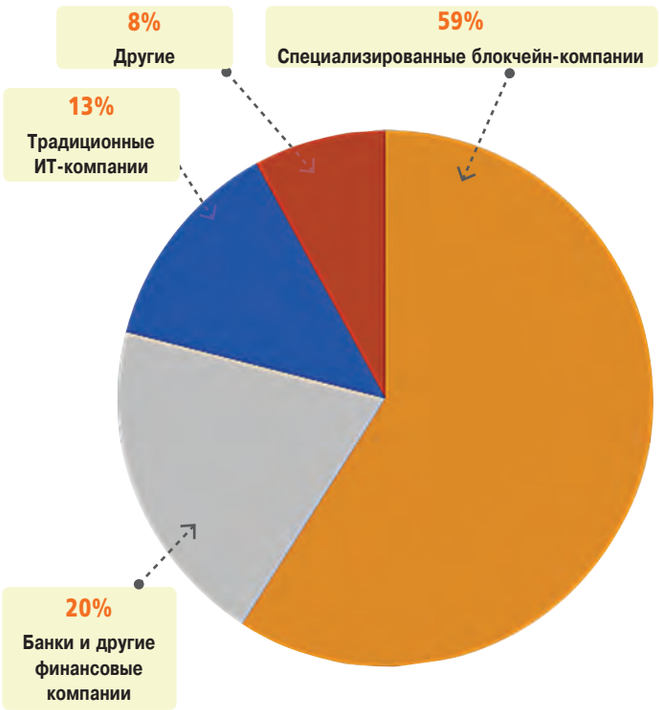
Китайская «система социального доверия» еще не вошла в фазу полноценного использования, поэтому структура баллов и рейтингов пока что носит экспериментальный характер. В разных городах используются различные подходы к оценке граждан, но общее направление мысли прослеживается уже сейчас. Для общего понимания ситуации приведем в таблице некоторые параметры системы оценок, применяемой на территории городского округа Вэйхай.

Таблица. Некоторые параметры экспериментальной «системы социального доверия», применяемой на территории городского округа Вэйхай (КНР)

Рейтинг	Кол-во баллов	Условный статус гражданина	Преференции/санкции
AAA	1050 и выше	«образцовый»	Потребительский кредит без залога и поручителей по сниженной процентной ставке. Приоритетное медицинское обслуживание, скидки на лечебные процедуры и образование. Беззалоговая аренда транспортных средств и т.д. Разница для разных категорий «А» заключается в сумме преференций
AA	1050–1000	«нормальный»	
A	1000–900	«лояльный»	
B	900–849	«требующий контроля»	Отсутствие преференций
C	849–599	«подозрительный»	Запрет на работу в госструктурах и СМИ, ограничение скорости доступа в Интернет, повышенные ставки по кредитам, запрет селиться в отелях высокой категории
D	599 и ниже	«изгой» (черный список)	То же, что и для рейтинга «С», а также запрет на любую квалифицированную работу, отказ в получении кредитов, запрет покупки билетов на скоростные поезда и самолеты, запрет выезда за границу, аренду транспортных средств. Закрыт доступ во многие общественные места.

Отметим, что ощутимое количество баллов гражданин может получить за прямые доносы на правонарушителей или «позитивную активность» в социальных сетях (под которой подразумевается прославление партии и правительства), а потерять, например, в случае общения с человеком из «черного списка» или «неправильных» высказываний, комментариев, репостов.

Аналогичный рейтинг предусмотрен и для юридических лиц – компании группы «А» платят меньше налогов, подают упрощенный пакет отчетных документов в надзорные структуры, получают более дешевые кредиты. Организациям с низким рейтингом запрещено осуществлять эмиссию ценных бумаг, выходить на биржу, они платят больше налогов и могут стать объектом усиленных проверок.



Основные владельцы патентов на технологии блокчейн. Данные Bloomberg со ссылкой на InvisionIP

Платформа Everledger ведет распределенный реестр драгоценных камней, присваивая каждому из них уникальный идентификатор. Эта инициатива тем более важна в свете того факта, что, скажем, бриллианты часто используются в качестве расчетных единиц в криминальных сделках (поскольку они обладают тремя главными достоинствами — анонимностью, компактностью, высокой стоимостью). Поэтому мировой учет этих камней — одна из приоритетных задач для структур, которые ведут борьбу с международным терроризмом и торговлей наркотиками.

Но с подобными угрозами большинство людей, к счастью, не сталкиваются — в современном мире гораздо легче стать жертвой некачественной пищи, чем пострадать от действий террористов. Поэтому учет и контроль продуктов питания в глобальном масштабе становится важной задачей во многих странах. Для решения этой задачи существует блокчейн-платформа Provenance («провенанс» — термин для обозначения истории владения предметом, обычно используется в контексте художественных произведений или антиквариата), которая позволяет отследить полный жизненный цикл любого продукта от момента получения первичного сырья для его изготовления до приобретения конечным покупателем.

Как ожидается, такое решение не только даст возможность сделать продукцию более качественной и безопасной, но и позволит более эффективно бороться с контрабандой, поскольку любая единица товара будет иметь свой уникальный идентификатор, благодаря которому можно отследить все этапы ее перемещения. Правда, для того чтобы это стало возможным, система должна быть внедрена на уровне государственных структур.

Большие данные для Большого брата

Благодаря своей универсальности блокчейн имеет множество применений — технология может быть использована как на пользу человечества, так и для исполнения не самых благих намерений, например, установления всестороннего контроля над каждым гражданином тоталитарной страны. Похожий проект — мечта любого диктатора — уже обретает реальные очертания в КНР. В рамках утвержденной правительством инициативы планируется присвоить каждому жителю Поднебесной индивидуальный рейтинг (оригинальный китайский термин наиболее корректно переводится как «система социального доверия»), который в дальнейшем определит положение человека в обществе. Граждане с низким показателем потерпят поражение в правах, а обладатели высоких рейтингов, напротив, получат определенные преференции. В реализации проекта помогают компании Alibaba, Baidu, SenseTime, Tencent и другие. Для осуществления такой программы требуется вся мощь современных технологий, ведь данные о каждом жителе Китая будут собираться из различных источников и аккумулироваться в единой базе. Для этого требуются поистине фантастические вычислительные ресурсы и системы хранения данных, технологии Big Data, «Интернета вещей» (для отслеживания сведений со всех возможных электронных устройств), наработки в области «искусственного интеллекта» и распознавания образов (для идентификации личности по данным камер видеонаблюдения) и т.д. Блокчейн в данном случае позволит свести всю информацию воедино и сделает невозможной ее фальсификацию.

Ввести «Систему социального доверия» в полноценную эксплуатацию по всей стране планируется в 2020 году. Тем не менее она уже работает в тестовом режиме на территории десятков городов КНР. Наиболее полная реализация идеи достигнута в округе Вэйхай (провинция Шаньдун). Здесь каждому жителю присваивается начальный рейтинг в тысячу баллов, который затем растет либо сокращается — в зависимости от действий конкретного гражданина. Алгоритм присвоения баллов не раскрывается (равно как и не существует каких-то нормативных документов, четко регулирующих данную сферу), однако известно, что для этой цели анализируются свыше 160 тыс. различных параметров, поступающих из более чем 140 учреждений.

Блокчейн также имеет большие перспективы использования в таких сферах, как идентификация пользователей, «Интернет вещей». Есть даже специализированные сервисы IoT, разработанные для нужд энергетической отрасли и работы в сетях Smart Grid (Energy Blockchain, Grid Singularity, TransActive Grid и другие). Список сфер приложений технологии ограничен только человеческой фантазией и техническими возможностями вычислительных платформ. Сейчас еще не до конца понятны все возможные преимущества и опасности, которые несет блокчейн, но уже очевидно, что это нечто особенное — технология, способная изменить жизнь современного человека.

Игорь КИРИЛЛОВ, СиБ