Автор: блокчейн биткоин криптовалюта децентрализация
22.11.2016 00:00 - Обновлено 24.11.2016 18:00

Модные ныне технологии блокчейна, децентрализации, финтеха будоражат умы сильных мира сего. Биткоин - плохо, блокчейн - хорошо! Такое мнение сейчас у отечественного регулятора, который, как и все централизованные органы исповедует подход: "там что-то новое возникает у масс, я не знаю что такое, но на всякий случай запрещу". Вокруг блокчейн стартапов сегодня много хайпа, и по настоящему реально никто не понимает, зачем это, где и как применить и что из этого будет. Но, веротяно, понимают, что это вторая серьезная революция после интернета, и не хотят ее упустить. Многие криптоэнтузиасты полагают, что блокчейн не имеет самостоятельной ценности без биткоина, ведь блокчейн просто технология для безопасной передачи цифровой наличности и гарантия отсутствия двойной траты и подделки криптоактива. Действительно, коллективное бессознательное под псевдонимом Сатоши Накамото не применил блокчейн для отслеживания тунца от моря до стола, не применил блокчейн для сохранения и ведения реестра документов или для хранения информации по пулям и оружию. Он использовал блокчейн только для работы биткоина. Имеет или не имеет частный блокчейн самостоятельную силу и ценность без биткоина покажет время. В рамках данной статьи мы расскажем понятным простым языком об этой технологии в целом и способам ее применения.

1. Введение

Блокчейн (Blockchain, Цепочка блоков транзакций) - децентрализованная база данных, устойчивая к попыткам злонамеренных и ошибочных манипуляций и предназначенная для упорядоченного хранения информации с привязкой ко времени. Исторически была впервые применена в 2009 году в криптовалюте Bitcoin в качестве механизма для хранения истории транзакций, где обеспечивает с одной стороны возможность внесения в неё новых записей произвольным пользователем (при условии наличия ненулевого баланса в системе и определенного количества вычислительных ресурсов и электроэнергии), а с другой - единственность базы данных для всех её пользователей.

2. Типы задач, для решения которых применим блокчейн

В общем случае применение блокчейн-технологий бывает оправдано в тех случаях, когда

возникает необходимость в создании механизма хранения информации, одновременно удовлетворяющего следующим требованиям:

1) Отказоустойчивость

Созданные с применением блокчейн-технологии средства хранения данных за счет распределенности практически всегда оказываются надежнее централизованных: даже в случае полного или частичного выхода из строя отдельных узлов системы, система в целом сохраняет работоспособность. В криптовалюте Bitcoin, например, ежесуточно включаются и отключаются сотни и тысячи узлов, но при этом сама сеть продолжает безостановочно работать уже на протяжении 7 лет.

2) Многопользовательность

Основанные на блокчейн-технологиях базы данных в силу своей распределенности по определению способны к использованию многими пользователями, причем благодаря тому что как правило каждый полноправный пользователь системы одновременно выполняет роль хранителя и источника информации, скорость чтения из базы данных в первом приближении не увеличивается по мере добавления новых пользователей.

3) Единственность

В распределенных базах данных, как правило, возникают проблемы с поддержанием единственности информации - в силу того что любой участник сети должен иметь возможность добавлять информацию в базу, возникает опасность возникновения множества различных версий одной и той же базы данных в результате ошибочного и/или злонамеренного её использования.

Применение блокчейн-технологий позволяет исключить возникновение таких проблем благодаря использованию PoW (Proof of Work), PoS (Proof of Stake) и других блокчейн-специфичных алгоритмов для подтверждения правильности полученного экземпляра БД.

4) Привязка данных ко времени

Базы данных, созданные с использованием блокчейн-технологий, хранят данные в виде последовательности блоков данных, порядок расположения которых определяется временем их добавления: таким образом изменение порядка их расположения практически невозможно. Как следствие, для любой записи в БД есть возможность с заданной во время создания БД точностью определить время её добавления, что крайне важно для ряда применений. Например, при создании базы транспортировки грузов, такой подход позволяет гарантировать что груз сначала прибыл в точку А и только потом в точку Б, и любая попытка сфальсифицировать запись будет почти наверняка обречена на провал.

5) Устойчивость к попыткам фальсификации данных участниками системы

БД, построенные с помощью блокчейн-технологий, обладают свойством устойчивости к попыткам фальсификации вносимых в них данных: так как для того чтобы новая внесенная в нее запись была принята системой необходимо согласие 51% пользователей этой системы, внесение ложных данных в систему практически невозможно.

Это позволяет, в частности, создавать системы взаиморасчетов, в которых участники не имеют возможности полностью или даже частично доверять друг другую.

Также основанные на блокчейн БД могут (но не должны) удовлетворять требованию

6) Общедоступности

Реализованная с использованием блокчейн-технологий система может быть частично или полностью общедоступной, что позволяет реализовывать крупные распределенные системы любого масштаба, в том числе глобального.

3. Принцип работы блокчейна

1) БД, созданная с использованием блокчейн-технологий представляет собой распространяемую через пиринговую сеть её участниками постоянно растущую последовательность записей (блоков), упорядоченных по времени их добавления.

2) В случае если пользователь получает от других пользователей системы несколько разных соответствующим остальным правилам версий БД, корректной считается та из них, длина которой больше.

3) В каждый блок добавляется временная отметка и т.н. хэш-сумма (в первом приближении хэш-сумму любого блока можно считать его уникальным отпечатком) предыдущего блока, что позволяет связать блоки в цепочку (chain) в строго определенном порядке: при попытке переставить местами блоки B и C в последовательности A -> B -> C блоки B и C перестанут быть корректными из-за того что, во-первых, порядок временных меток будет неправильным (они, очевидно, должны в каждом последующем блоке быть больше чем в предыдущем), а во-вторых хэш-суммы не будут соответствовать исходным данным что сделает их некорректными.

4) Очевидно, что изложенных в (3) правил недостаточно для обеспечения свойств единственности и привязки ко времени: любой желающий может изменить временную отметку и пересчитать хэш-суммы так, чтобы сформировать цепочку блоков, корректную с точки зрения системы использующей только принципы изложенные в (3).

Для предотвращения этого используется множество различных способов, большую часть которых можно разделить на две категории: Proof of Work (PoW, доказательство работы) и Proof of Stake (PoS, доказательство владения). В обеих системах основополагающим принципом является принцип дороговизны формирования блока, в частности в PoW-системах для создания корректного блока кроме условий изложеных в (2) блок должен удовлетворять ещё одному: для формирования корректного блока необходимо произвести вычислительно сложную и энергетически затратную операцию (как правило - подбор записи, при добавлении которой в блок его хэш-сумма будет удовлетворять некоторым заранее определенным условиям).

Таким образом, при условии, что значительное число участников сети формируют новые блоки, для перезаписи содержимого базы данных злоумышленнику потребуется сконцентрировать в своих руках вычислительные и энергетические мощности сопоставимые с вычислительной мощностью большинства участников сети.

Кроме того, существует альтернативный подход, в котором для формирования блока следует получить согласие большей части участников сети (как правило оно выражается посредством цифровой подписи каждого из участников). Такой подход малоприменим для создания глобальных блокчейн-систем со свободным доступом, но вполне пригоден для создания малых отраслевых блокчейн-баз, например, для системы взаиморасчетов разноуровневых поставщиков и крупных потребителей электроэнергии.

4. Примеры использования блокчейн-технологий

Приведем несколько примеров систем, использующих блокчейн-БД

1) В первую очередь это, разумеется, Bitcoin и другие криптовалюты. Как уже было сказано, блокчейн-системы были впервые разработаны и применены в рамках этих систем, что и сделало возможным само их существование. Используя алгоритмы ассиметричного шифрования совместно с блокчейн-БД, эти системы позволяют их пользователям (которыми могут стать любые желающие пользователи Интернет) осуществлять переводы внутренних единиц обмена (биткоины, лайткоины, и т.д.), причем для этих операций гарантируется их безопасность (система гарантирует что пользователь может переводить средства только со своих счетов, и что список транзакций существует в единственном экземпляре, т.е. его подмена практически невозможна).

На момент написания этих строк рыночная капитализация пяти самых популярных валют составила 11,5 млрд долларов США, что, по мнению автора, свидетельствует об успешности этих проектов.

2) Кроме того, в последнее время приобрели популярность проекты альтернативных

(т.е. не-Биткоин) криптовалют, позволяющих своим пользователям кроме осуществления транзакций задавать правила обработки этих транзакций с помощью специальным образом сформированного пользователем программного кода, который интегрируется в блокчейн-БД и выполняется всеми участниками сети при обработке этих транзакций. Такой подход дает возможность создавать значительно сложные финансовые приложения, сохраняющие при этом типичные свойства блокчейн-систем, т.е. распределенность, отказоустойчивость и устойчивость к внешним административным воздействиям.

В качесте примера такого проекта можно привести криптовалюту Ethereum, капитализация который составляет ~1 млрд долларов.

3) Также блокчейн-технологии находят применение в т.н. "интернете вещей": благодаря своей децентрализованности и способности несмотря на это сохранять единство данных для всех участников сети, БД, созданные с применением этих технологий находят свое применение в области отказоустойчивого управления и синхронизации работы подключенных к сети устройств, количество которых стремительно растет в последние годы.

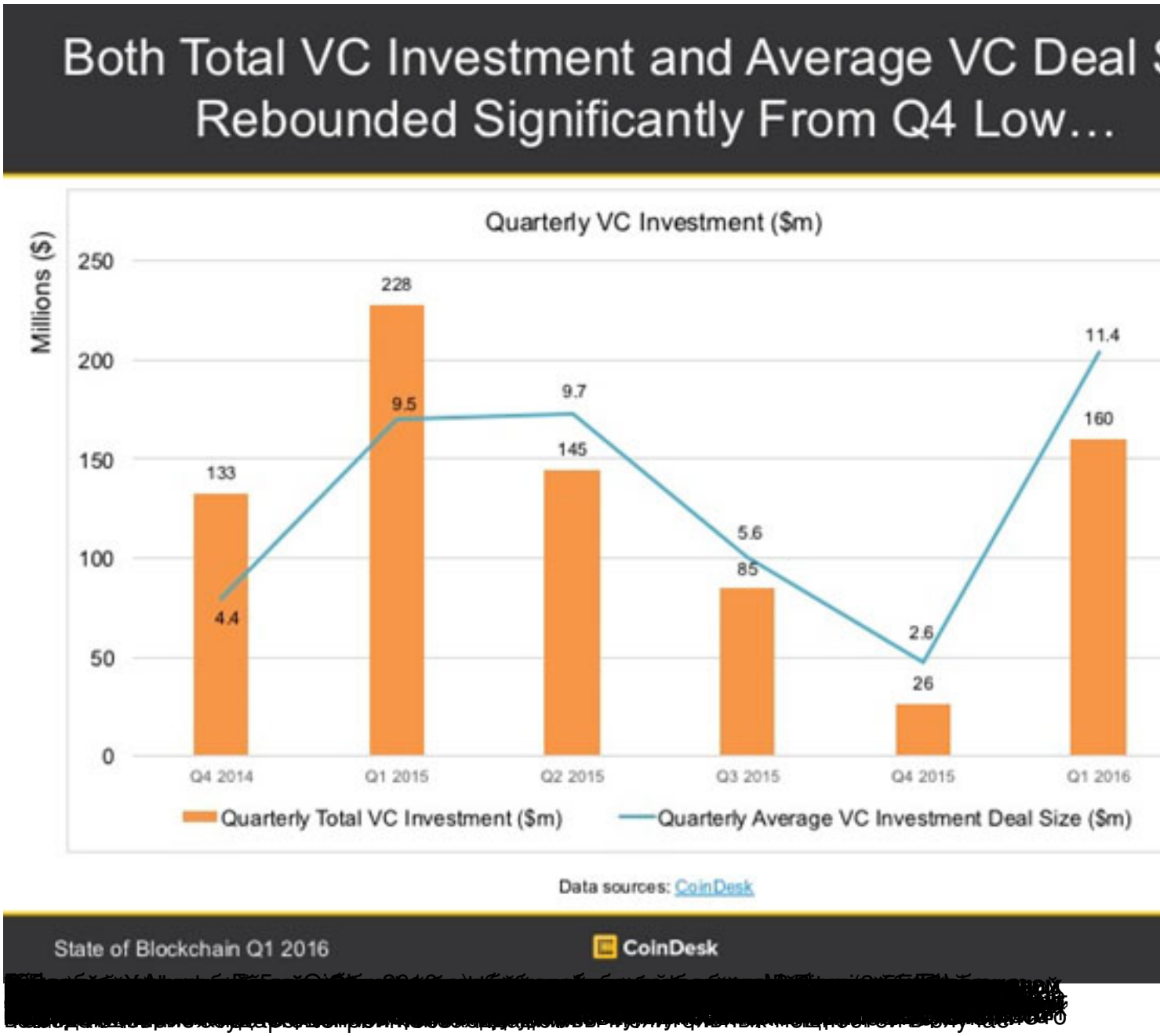
В совокупности с (2), возникает возможность создания комплексов устройств, способных самостоятельно, независимо от работоспособности центральных серверов компании-производителя, принимать оплату за оказание тех или иных услуг, в том числе и от других устройств, что создает возможность автоматического независимого обмена ресурсами (например, электроэнергией).

Кроме того, гарантированная единственность БД блокчейн-систем и возможность её локальной проверки позволяет осуществлять распространение криптографических ключей для такого рода устройств, что позволяет значительно увеличить её безопасность - ключи могут быть обновлены даже в случае выхода из строя серверов компании-производителя устройства (например из-за DDoS-атаки или из-за ухода компании с рынка).

4. Степень развития блокчейн-технологий и объемы инвестирования

По мнению многих экспертов, блокчейн-технологии на сегодняшний день находятся в зачаточной стадии развития, за которой последует бурный рост, подобный тому что происходило с сетью Интернет в середине-конце 90х годов, когда узкоспециализированная сеть ученых, корпораций и военных внезапно породила многомиллиардную индустрию. В качестве примера одного из таких мнений можно привести статью Марка Андресена (одного из основателей компании "Адресен Хоровитц", под управлением которой в 2014 году находилось около 4 миллиардов долларов).

Объем инвестиций в системы, построенные с использованием этих технологий, к первому кварталу 2016 года составил 1.1 млрд долларов США, что свидетельствует о том интерес к таким системам не ограничивается экспертными оценками, а реализуется и в виде вполне осязаемых и реальных денежных вливаний в компании, занимающиеся их разработками.


Both Total VC Investment and Average VC Deal
Rebounded Significantly From Q4 Low…
Quarterly VC Investment ($m)
Millions ($)
250
200
150
100
50
0
228
133
145
85
26
160
9.5
9.7
5.6
2.6
11.4
4.4
Q4 2014
Q1 2015
Q2 2015
Q3 2015
Q4 2015
Q1 2016
Quarterly Total VC Investment ($m)
Quarterly Average VC Investment Deal Size ($m)
Data sources: CoinDesk
State of Blockchain Q1 2016
CoinDesk