Про блокчейн

Михаил Петров, Дмитрий Болотюк

С появлением беспроводных систем вся Земля превратится в один огромный мозг. Мы сможем общаться друг с другом практически мгновенно, невзирая на расстояния.

Никола Тесла
1926 г.

Что такое технология блокчейн. Виды блокчейн

Блокчейн[1] (от англ. Blockchain или block chain, — цепочка блоков) – выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.

Концепцию цепочек блоков предложил в 2008 году Сатоши Накамото (Satoshi Nakamoto), если, конечно, такой человек реально существовал. Впервые она была реализована в 2009 году как компонент цифровой валюты – Биткоин, где блокчейн играет роль главного общего реестра для всех операций.

Хотя первое использование Блокчейн в современной отрасли зафиксировано в механизме цифровых денег Биткоин, необходимо разделять данные понятия. Использование технологии Блокчейн может быть гораздо шире, чем создание цифровых денег.

Блок – запись нескольких транзакций в определённом формате. Транзакция – минимальная логическая операция, которая может быть совершена только полностью (т.е. транзакция либо выполнена, либо нет; состояния, например, в 62% выполнения транзакции быть не может).

К примеру, в сети Биткоин транзакции объединяются в одиночные блоки и проверяются на математическую верность (сеть Биткоин автоматически поддерживает сложность алгоритма, чтобы подобная операция осуществлялась в среднем раз в 10 минут) с помощью операции ***майнинг***. Каждый последующий блок дополнительно проверяет предыдущие блоки и делает дупликацию транзакции биткоин невозможной. Транзакция, получившая подтверждение, уже не может быть отменена или проведена вторично.

Если кто-то захочет поменять местами события, записанные в блокчейн, или внести изменения, то ему придется заново пересчитать хеш всех последующих событий.

Получаем упрощенное Хеш-дерево, или дерево Меркла[2] (англ. Merkle tree) - полное двоичное дерево, в листовые вершины которого помещены хеши от блоков данных, а внутренние вершины содержат хеши от сложения значений в дочерних вершинах.

Дерево Меркла применяется для эффективного хранения транзакций в блокчейн. Оно позволяет получить «отпечаток» всех транзакций в блоке, а также эффективно верифицировать транзакции.

---

[1] https://bitcoin.org/bitcoin.pdf

[2] https://ru.wikipedia.org/wiki/Дерево_хешей

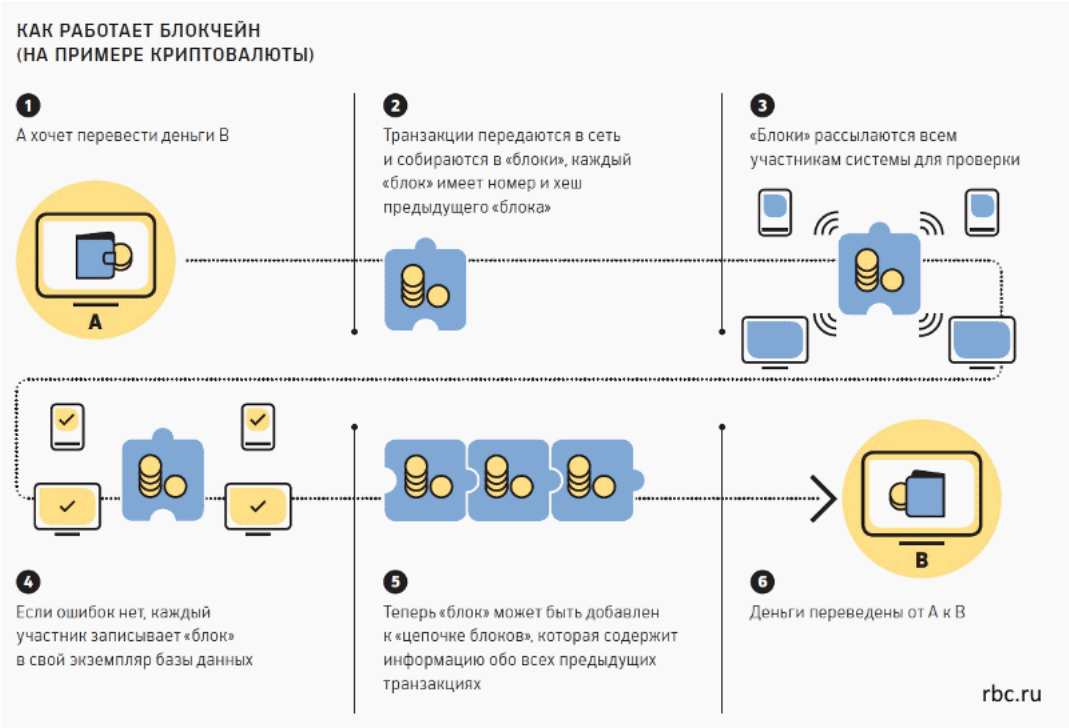

Рисунок 1 – Как работает Блокчейн.

Ключевым аспектом блокчейн-сетей является ***децентрализация***: информация хранится в зашифрованном виде, распределённо – на сотнях и тысячах компьютеров (узлов сети).

По степени децентрализации блокчейн-сети разделяются на два типа: **открытые** блокчейны и **приватные**.

Открытая блокчейн-сеть полностью децентрализована:

- все узлы равнозначны, отсутствует орган или компания, которая управляла бы этой сетью, нет ролевых механизмов и т.п.;
- нет механизмов запрета на подключение к сети новых узлов;
- нет механизмов управления децентрализованной логикой (смарт-контрактами) для каких-либо участников сети;
- нет механизмов ограничения области видимости данных и инструментов репликации данных на узлах.

В приватных блокчейн-сетях добавляются упомянутые механизмы выделения узлов; как правило, применяются ролевые механизмы; появляются механизмы ограничения подключений новых узлов и механизмы ограничения областей видимости. Конкретные механизмы отличаются у разных производителей — и даже версий блокчейнов.

К примеру, открытая блокчейн-сеть Биткоин основана на пиринговом (P2P) протоколе, в котором все пользователи в сети работают и взаимодействуют непосредственно друг с другом, вместо того чтобы передавать свои данные через посредника, как, например, банк или кредитная компания.

В блокчейн хранятся не только все транзакции с момента его старта, но и хеш-функции каждого блока, причём каждая хеш-функция содержит хеш предыдущего блока.

Хеш-функция – функция, которая преобразует сообщение произвольной длины в число («свёртку») фиксированной длины. Ключевой особенностью хэш-функции является отсутствие обратной функции (имея хэш, нельзя восстановить начальные данные, из которых он был подсчитан).

Благодаря описанным свойствам хеш-функций и достигается целостность блокчейн. В таких условиях подделка информации становится практически невозможной. Единственным механизмом «отката» данных в блокчейн-сети будет согласованный со всеми узлами переход на альтернативную цепочку блоков, так называемый механизм «хардфорка».

В открытых блокчейн-сетях отсутствует идентификация участников, применяется только механизм управления владением криптоактивом с помощью асимметричной криптографии. Причем в открытых блокчейн-сетях участник может генерировать ключевые пары в неограниченных количествах и применять их по своему усмотрению в любых транзакциях. Владелец криптоактива получает доступ к его изменению за счет использования приватного ключа. Утрата приватного ключа приводит фактически к утрате криптоактива. Например, если вы потеряете ключ от биткоин-кошелька, то доступ к хранящимся в нём средствам технически невозможно восстановить.

В некоторых дистрибутивах приватных блокчейнов начинают добавляться механизмы идентификации узлов на аналогичных принципах (асимметричная криптография), однако сейчас эти возможности ещё недоступны. По состоянию на 2018 год к приватным блокчейн-сетям имеет смысл применять дополнительные (внешние) технологии ограничения доступа (файерволы, шифраторы трафика и т.п.).

Свойства блокчейн[3]:

1. **Невозможность подмены данных в блокчейне.** Если мы поменяем транзакцию в цепочке блоков, то необходимо будет переписать и все последующие блоки, иначе подобная транзакция не будет подтверждена узлами сети.
2. **Распределённый реестр информации.** Одна и та же база хранится на всех компьютерах, подключенных к системе, и любая необходимая информация доступна без задержки. База обновляется через заданные промежутки времени, актуализируя транзакции.
3. **Устойчивость к воздействию вирусов, катастроф и других факторов.** Благодаря распределённому реестру база блокчейна хранится на тысячах или миллионах компьютеров в разных частях света.

Виды блокчейн:

1. **Блокчейн без необходимости в разрешениях (Permissionless Blockchain)**. База хранится на любом компьютере в мире. Публичный блокчейн подразумевает абсолютную децентрализацию. Нет человека, который управляет всем этим и подтверждает транзакции, а значит, нет необходимости и в авторизации. Примером как раз и служит Биткоин. Если отправить кому-то несколько биткоинов, то об этом (о факте перевода, но не о личностях отправителя и получателя) узнает вся сеть.
2. **Открытый блокчейн с разным уровнем разрешений (Public Permissioned Blockchain).** База может храниться на любом компьютере, любой пользователь может создать свой собственный блокчейн для своих целей, установив разные уровни разрешений для его пользователей. Определённые пользователи (управляющий орган, правительство, учреждение) обладают правом подтверждать транзакции, а остальные пользователи могут просматривать данные. Таким пользователям необходима авторизация.

   К примеру, производители товаров могут создать свой блокчейн для исключения подделок, в котором любой пользователь сможет отследить, когда и где выпущен тот или иной продукт — но не сможет изменять записанные данные самостоятельно.
3. **Закрытый блокчейн с разным уровнем разрешений (Private Permissioned Blockchain).** Доступ к просмотру реестра имеет ограниченное количество пользователей. База хранится распределённо, но только на компьютерах, которые входят в конкретную блокчейн-систему. К таким случаям можно отнести, например, блокчейны, применяемые банками для проведения расчётов.

[3] http://www.imponderablethings.com

Майнинг. Консенсус

Не важно, какой вид блокчейна рассматривается, в любом случае любая транзакция должна быть подтверждена. Для подтверждения транзакций проводится проверка математической верности данных и выстраивание транзакций в блоки. Транзакция, получившая подтверждение, уже не может быть отменена или проведена вторично.

Основным механизмом записи новых транзакций в цепочку блоков в открытых блокчейнах является механизм майнинга (от англ. Mine — добывать полезные ископаемые). Это подход основан на организации конкуренции участников сети, которые выполняют математические операции для нахождения хэша нового блока и конкурируют по времени выполнения такого подбора. В случае, когда участники-«майнеры» увеличивают (или уменьшают) свои вычислительные мощности, сеть регулирует сложность алгоритма таким образом, чтобы поддерживать примерно одинаковое время формирования новых блоков в цепочке. При таком подходе «сгенерировать» блок, соответствующий условию подтверждения, достаточно сложно. Необходимо перебрать огромное количество «случайных» комбинаций, пока блок не получит статус подтвержденного.

За каждый подтвержденный блок в публичном блокчейне выдаётся вознаграждение в валюте конкретного блокчейна. Этот процесс получил название майнинга.

Майнинг[4] – деятельность по созданию (генерации) новых блоков для обеспечения функционирования сети блокчейн, сводится к серии вычислений с перебором параметров для нахождения хеш-функции с заданными свойствами.

Майнеры – узлы, которые генерируют блоки и получают награду за каждый проверенный блок, прошедший подтверждение.

С помощью такого параметра, как сложность (Difficulty Target), в блокчейн обеспечивается определённая скорость (время) подтверждения транзакций. К примеру, сеть Биткоин регулирует сложность майнинга в проверке блоков каждые 2016 блоков. Сложность автоматически регулируется так, чтобы поддерживать время проверки (верификации) блоков на уровне 10 минут.

В процессе подтверждения транзакций майнеры (разумеется, не люди, а их вычислительные мощности) соревнуются в своеобразной «хеш-игре». Чтобы выиграть «игру», майнер должен угадать число, называемое «нонс» (nonce), которое в комбинации со всеми предыдущими данными блокчейна даёт определённый хеш.

Угадывание происходит простым перебором значений нонс, для обеспечения безопасности нужно «работать», то есть производить доказательства работы (Proof of work, PoW).

Существуют и другие алгоритмы консенсуса, которые не требуют производить интенсивные расчеты: proof-of-space, proof-of-stake. Последняя – самая популярная категория таких алгоритмов, основанная на доказательствах доли (proof-of-stake[5], PoS). Принцип доказательства доли во многом похож на доказательство работы, только вместо совершения определённой работы автор показывает, что у него есть доля в системе (например, в виде ненулевого баланса криптовалюты).

Если изначально майнинг был эффективен даже на обыкновенных бытовых компьютерах, то со временем, с процессом повышения сложности «угадывания», требования к вычислительным мощностям для майнинга стали возрастать. Причём требовались все более и более специфические алгоритмы. В какой-то момент выяснилось, что нуждам майнинга оптимальным образом отвечают мощности графических процессоров (GPU), и «фермы» для майнинга стали собирать на видеокартах.

---

[4] https://ru.wikipedia.org/wiki/Майнинг

[5] https://en.wikipedia.org/wiki/Proof-of-stake

Однако, в настоящее время появились специальные устройства — ASIC (application-specific integrated circuit, интегральные схемы специального назначения), т.е. вычислительные устройства, спроектированные на уровне «железа» для выполнения конкретной задачи. В случае с майнингом они узко «заточены» под максимально эффективный поиск хешей блокчейна, при этом их майнинг-мощность несопоставимо больше мощности обычного (домашнего или офисного) компьютера, оптимизированного на широкий спектр задач.

Во многих странах, активно использующих инструменты блокчейн, строят огромные промышленные «фермы» на базе ASIC. Очевидно, что выгоднее всего располагать подобные «фермы» как можно ближе к источникам электроэнергии (ГЭС, АЭС) и размещать ее в условиях, где сама природа «заботится» об ее охлаждении, например, в шахте глубоко под землей — таким образом минимизируются затраты на питание и охлаждение системы.

«Бытовой» же майнинг (например, на базе домашних компьютеров или небольших «ферм» на 6-8 видеокарт) сегодня может быть эффективен только на вновь запускаемых блокчейн-инструментах (например, на новых криптовалютах), под алгоритмы которых производство ASICов ещё не налажено.

Смарт-контракты и оракулы

Как мы уже говорили, технология Блокчейн может быть использована не только для выпуска электронных денег.

Смарт-контракт[6] (от англ. Smart contract – умный контракт) – это программный код, который позволяет автоматически выполнять определённые функции при наступлении конкретных условий и поддерживает коммерческие контракты в технологии блокчейн.

Например, при получении электронного билета на самолет, автоматически будут переведены средства на счёт авиакомпании.

На прикладном уровне смарт-контракт позволяет реализовать выполнение некоторой логики на децентрализованной сети блокчейна.

Как и в стандартном, бумажном договоре, к каким мы привыкли, при подписании смарт-контракта есть стороны, которые его подписывают.

Предмет договора – объект, находящийся внутри среды существования самого умного контракта (или должен обеспечиваться беспрепятственный прямой доступ умного контракта к предмету договора без участия человека).

Условия умного контракта должны иметь полное математическое описание, которое можно запрограммировать в среде существования умного контракта. Именно в этих условиях описывается логика исполнения пунктов предмета договора.

Однако нужно отметить, что для взаимодействия с реальным миром смарт-контракту необходимы датчики и приводы.

Приложения, опирающиеся на умные контракты, называются ***децентрализованными приложениями*** или DApps[7].

[6] https://bitfury.com/content/downloads/contracts-1.1.1.pdf

[7] https://www.stateofthedapps.com

Рисунок 1 – Как работает Смарт-контракт.

Основные достоинства смарт-контрактов:

1. **Независимость**. Для заключения сделки не нужны посредники.
2. **Безопасность**. Децентрализованная технология хранит данные в распределённом реестре.
3. **Прозрачность**. Каждый участник может отслеживать, как исполняется договор.

Главный недостаток умных контрактов – отсутствие внятных моделей взаимодействия с некоторыми реальными процессами: например, с помощью программного кода невозможно отследить или подтвердить физическую передачу товара от поставщика к покупателю[8].

Именно поэтому появились аппаратные и программные решения для связи блокчейн с реальным миром – их называют ***Оракулами***.

Оракулы используют различные источники данных[9] – от метеорологических ресурсов, предоставляющих данные о погоде, до информации Bloomberg о колебании цен на фондовом рынке, или данных о будущих событиях от рынка предсказаний Augur.

Рассмотрим типы блокчейн-оракулов:

Оракул как программный код – оракул, существующий в формате программного обеспечения, работает с информацией, которая находится онлайн. Такой оракул может предоставлять данные о погоде, температуре, ценах на услуги или товары, расписании транспорта и так далее. Эти данные оракул получает с сайтов компаний, обрабатывает и предоставляет смарт-контракту.

Аппаратный оракул – аппаратное решение для получения информации из реального мира о физическом выполнении определённых условий. Например, смарт-контракту могут понадобиться данные об автомобиле, который находится в зоне действия определённого датчика. Также аппаратный оракул может взаимодействовать с RFID-метками (метки радиочастотной идентификации) для работы смарт-контрактов в логистике.

---

[8] Возможно, дальнейшее развитие интернета вещей (Internet of Things) решит эту проблему.

[9] http://www.oraclize.it/#home

Входящий оракул – данный тип оракула работает непосредственно внутри самого смарт-контракта и предоставляет информацию из внешнего мира при определённых условиях. Например, для запуска автоматического ордера на покупку криптовалюты смарт-контракт должен знать, когда её курс достигнет той или иной отметки. Данную информацию предоставит входящий оракул.

Исходящий оракул – отправляет информацию во внешний мир. Так, система умной блокировки, которая существует в реальном мире, может автоматически предоставить пользователю доступ к товару или сервису, как только она получит информацию об успешном платеже от оракула.

Консенсус Оракулов – таким рынкам предсказаний, как Augur или Gnosis, необходимы оракулы для достоверного предсказания развития событий и конечных результатов. Однако, используя всего один источник информации, невозможно с точностью определить его надёжность. В связи с этим рынки предсказаний используют не одного, а несколько оракулов, чтобы предугадать последствия событий.

Разработкой проектов, связанных с развитием и внедрением блокчейн-оракулов занимаются несколько компаний: Oraclize, ChainLink, BNC (BraveNewCoin).

По мере развития блокчейн-экономики экосистема оракулов будет стремительно развиваться как надёжный способ связи цифрового мира с реальным. Именно блокчейн-оракулы смогут решить проблемы коммуникации блокчейнов, а также обеспечить более широкое применение смарт-контрактов в различных индустриях, заинтересованных в использовании децентрализованных сетей.

Бизнес-задачи, решаемые с помощью технологии блокчейн

Технология блокчейн – не панацея от всех проблем. Есть множество бизнес-ситуаций, в которых использование централизованных подходов к хранению и обработке информации будет вполне достаточным и эффективным. Давайте разберём условия, при выполнении которых действительно стоит задуматься о целесообразности применения блокчейна.

1. Самый первый, естественный вопрос – нужно ли хранение данных? Если данных для хранения нет, то и блокчейн не нужен.
2. Далее необходимо определить, доверяют ли друг другу участники сети и, если нет – то есть ли сторона-арбитр, которой доверяют все участники информационного обмена, и которая на 100% гарантирует и контролирует неизменность данных (как поступающих извне, так и уже произошедших). Если такая сторона есть – блокчейн не нужен. Если нет взаимного доверия и нет доверенного арбитра – то это показание в пользу использования блокчейна.
3. Следующий вопрос – сколько пользователей записывает данные? Здесь нет однозначной зависимости между ответом и нужностью блокчейна. Обычно стоит рассматривать блокчейн, если в системе значится множество пользователей, одновременно записывающих или изменяющих данные. Но, например, даже если пользователь только один – например, какой-то сертификационный центр, ведущий и выкладывающий в общий доступ базу сертификатов – здесь тоже может пригодиться блокчейн, если есть основания подозревать неконтролируемые вмешательства в базу.
4. Публичны ли хранимые данные? Если да – то, возможно, целесообразен публичный блокчейн, если нет – то приватный, либо публичной можно сделать только информацию о хэшах данных, хранимых в закрытых базах (современные решения позволяют предоставить информацию о возможных изменениях в базе без доступа к самой информации).
5. Проходят ли данные модерирование владельцем информационного ресурса перед публикацией? Если да – то целесообразность блокчейна сомнительна.

6. Важна ли скорость транзакций? Важно помнить, что низкое количество транзакций в секунду – на данный момент[10] одна из основных проблем блокчейна.
7. Важна ли сохранность информации? Особенность технологии блокчейн состоит в том, что вся информация одновременно хранится на нескольких узлах сети. Это, конечно, многократно повышает надёжность хранения информации, и с другой стороны, многократно повышает потребность в ИТ-ресурсах.
8. Даст ли применение смарт-контрактов и соответствующее исключение человека из бизнес-процессов критически значимое повышение эффективности?
9. Возможно ли организовать единую логику бизнес-операций для всех участников бизнес-процессов? На практике логика выполнения и/или учета операций отличается в разных организациях (а в крупных организациях могут отличатся и даже внутри разных подразделений), и не всегда соответствующие службы готовы их изменить.

Пример: исследование применимости технологии блокчейн в системах электронного документооборота

Рассмотрим с точки зрения перечисленных выше условий необходимость применения технологии блокчейн в системах электронного документооборота (СЭД) и определим бизнес-ситуации, в которых эффективно применять СЭД, построенный на блокчейн.

Проверяем первое условие – да, хранение данных необходимо.

Далее проверяем на доверие. В рамках одной организации – как правило, администратор системы является независимым арбитром, а вероятность его сговора с каким-то участником информационного обмена пренебрежимо мала. В рамках нескольких организаций – да, проблема доверия сторон друг другу существует. Соответственно, блокчейн может быть эффективен в «межорганизационном СЭД».

Данные записывает множество пользователей — проверка пройдена.

Публичность данных – нет, данные не публичны, поэтому можно говорить только о приватном блокчейне.

Централизованного модерирования – нет. Скорость транзакций – не критична. С этой точки зрения применение технологии блокчейн целесообразно.

Сохранность информации – как правило, централизованных решений по бэкапированию систем электронного документооборота вполне хватает.

Что следует из сказанного? СЭД на блокчейне эффективно применять в режиме приватного блокчейна при обмене информацией между организациями. Т.е. это может быть целесообразно, например, в рамках производственного холдинга, предприятия которого передают друг другу конструкторскую документацию, и необходимо гарантировать её неизменность после передачи.

Применимость технологии блокчейн в государственном управлении

Можно рассмотреть следующие области, в которых применение технологий блокчейн будет эффективно в государственном управлении:

- Открытые публичные государственные реестры (земли, недвижимости, прав, патентов, компаний и т.д.) и действия с ними (например – регистрация, передача объектов, прав), обеспечивая неизменность информации и подконтрольность изменений;
- Системы голосования (в случае тайного голосования – можно обезличивать данные голосовавшего);
- Благотворительные проекты – когда необходимо отследить, сколько собранных «криптоденег» ушло и на какой цифровой кошелёк;

[10] Здесь и далее в данном разделе информация актуальна по состоянию на лето 2018 года.

- Маркировка товаров (хотя по данному вопросу необходимо исследовать каждый бизнес-кейс отдельно);
- Хранение персональных и медицинских данных (опять же с соответствующим обезличиванием и шифрованием);
- Закупки;
- Таможенная очистка.

Что касается бизнеса, то здесь эффекты от применения блокчейна, помимо описанных выше, связаны в первую очередь с возможностью использования смарт-контрактов, т.е. автоматического исполнения сделок при наступлении тех или иных условий (например, выпуск аккредитива, освобождение залога, генерация электронного сертификата при условии проверки информации в ряде баз данных и т.п.).

Применимость технологии блокчейн в логистике

Приведём пример на стыке государства и бизнеса, где применение технологии блокчейн может дать существенный эффект.

Решение на блокчейне может вести учёт коносамента (соглашения, которое фиксирует условия транспортировки и доставки товара и определяет, какая компания несёт ответственность за товар во время транспортировки в любой момент времени) и истории передачи груза. Когда перевозчик принимает груз для дальнейшей транспортировки и подписывает соответствующие документы, информация может быть занесена в блокчейн, откуда эта запись практически мгновенно доступна любому участнику системы. Также в блокчейне все участники могут проследить цепочку перемещения товара и быстро определить, когда что-то пошло не так.

Естественно, данная система должна быть тесно интегрирована с государственными системами, контролирующими таможенную очистку грузов – поэтому и государственные таможенные системы в рамках пилотного запуска системы также должны быть оптимизированы под работу с блокчейн-технологией и принимать решения смарт-контрактов как директивы к действию.

Применимость технологии блокчейн в финансовом секторе

Помимо логистики, решения на блокчейне очень перспективны в банковской сфере, т.к. после их интеграции с автоматизированными банковскими системами можно добиться полного исключения человека из процесса исполнения финансовых транзакций, переведя их на алгоритмический язык смарт-контрактов. Очевидные кандидаты на такого рода оптимизацию – закладные, аккредитивы, банковские гарантии. Примерные функциональные архитектуры двух последних решений на основе «Мастерчейн» приведены ниже (по материалам www.tadviser.ru).

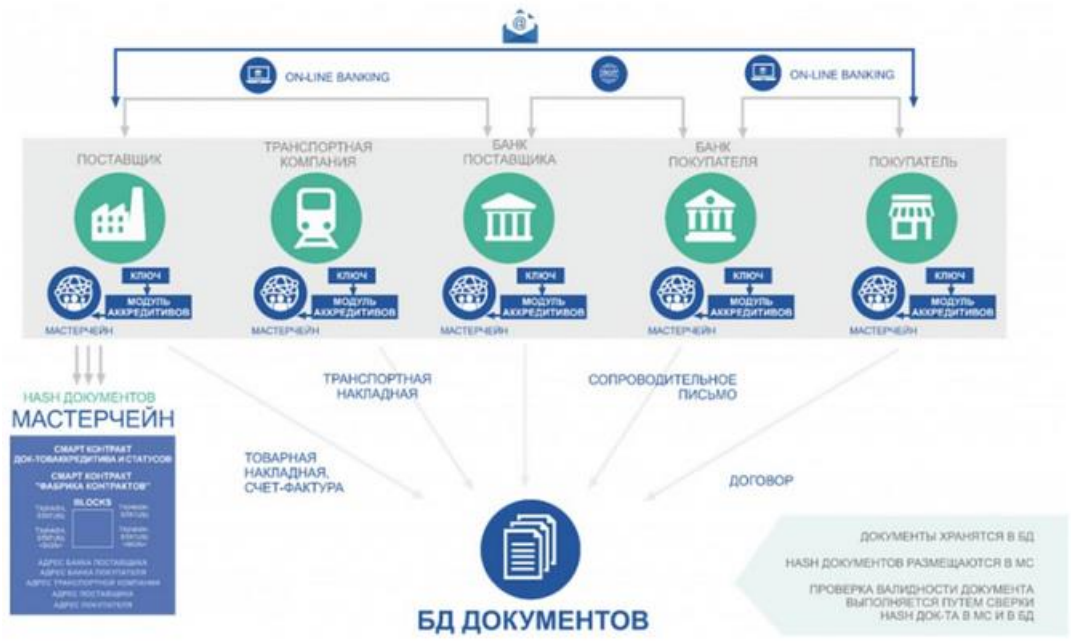

Рис. … - …

В частности, применение технологии блокчейн для учета электронных закладных (проект «Децентрализованная депозитарная система») дает до 80% снижения трудозатрат на депозитарные операции и снижает скорость выполнения операций с нескольких дней до нескольких минут. Однако в проекте потребовалось выполнить полный реинжиниринг бизнес-процессов депозитарного учета — если переложить бизнес-процессы на блокчейн в состоянии «как есть», то эффекта относительно «традиционных» технологий добиться будет невозможно.

Для многих стран в текущей экономической и политической ситуации становится важной задача проведения платежей без использования системы SWIFT (Society for Worldwide Interbank Financial Telecommunications), которая в течение уже долгого времени фактически является монополистом в сфере денежных переводов, и доступ к которой зачастую является средством политического и экономического давления. Такую задачу решает ряд стартапов,

самый известный из которых – Ripple. Зародившись в 2011 году, платёжная система Ripple сейчас рассматривается рядом консорциумов ведущих банков, как альтернативный канал расчётов. Теоретически может настать такой момент роста экосистемы контрагентов, использующих альтернативные системы платежей, когда использование традиционной системы взаиморасчётов станет в принципе необязательным, что существенно изменит текущий баланс сил в финансовом мире. Но пока что это не вопрос завтрашнего дня.

ICO, White Papers – что это такое, зачем нужно, и как с этим работать

Вместе с развитием блокчейн появились ICO (Initial Coin Offering, дословный перевод – «первичное размещение монет»). В последнее время понятие ICO часто заменяется на более правильное по смыслу ITO (Initial Tocken Offering, дословный перевод – «первичное размещение токенов»). Стартап выпускает токены[11], которые продаёт покупателям за криптовалюту (или «фиатную», традиционную валюту через ряд финансовых схем и посредников в виде криптобирж) и использует полученные средства на своё развитие (в этом смысле ICO/ITO очень похоже на классическое IPO – Initial Public Offering).

Покупатели могут использовать приобретённые «токены» для получения товаров и услуг, предусмотренных организаторами ICO/ITO (и с этой точки зрения токен трактуется финансовыми регуляторами как как utility, товар), либо получать дивиденды от доходности токенов или продать их в случае выхода на биржу и дальнейшего роста их стоимости (и с этой точки зрения токен трактуется как security, акция, что тут же влечёт за собой применение регуляций, свойственных для классических финансовых рынков). Иногда проекты предусматривают выпуск обоих видов токенов.

ICO, как правило, проводится молодыми компаниями для получения финансирования, не связанного с большим количеством регуляторных ограничений, – но, в то же время, благодаря отсутствию этих ограничений организаторы ICO не несут никакой ответственности перед покупателями токенов. Поэтому покупатели токенов не имеют никакой правовой защиты и, действуя полностью на свой страх и риск, могут как получить доход на спекулятивном росте стоимости токена, так и потерять вложенные средства практически полностью — из-за обесценивания приобретённого токена. Последнее время ряд государств предпринимает активные меры по введению регулирующих мер — как в отношении рынка криптовалют, так и рынка ICO/ITO.

Для привлечения инвестиций организаторы ICO/ITO готовят т.н. White Paper («белую книгу») – описание ICO/ITO, которое по сути является бизнес-планом развития проекта.

[11] Цифровые купоны, которые выпускаются на блокчейне.

Основные блокчейн-консорциумы и направления их развития

Рис. … - …

Текущая проблематика технологии. Правовые аспекты использования технологии

Технологические проблемы

Основная технологическая проблема технологии блокчейн в данный момент – это ограничение масштабируемости, прежде всего по параметрам производительности.

Причем если для «монетарных» применений (реализация биллинга криптоактива) важен параметр «число транзакций в секунду», то для немонетарных задач критичны такие параметры как:

- суммарный объем бизнес-данных, который блокчейн-сеть способна реплицировать в минуту;
- объем вычислительной логики смарт-контрактов, которую способна обеспечить сеть в минуту;
- суммарный объем логики, который можно реализовать в одном смарт-контракте.

На начало 2018 г. данные по количеству выполнения транзакций за секунду шести самых крупных криптовалют мира относительно основных платёжных гигантов, таких как Visa и PayPal, таковы[12]:

- Visa: 24 000
- Ripple (CCC: XRP-USD): 1 500
- PayPal: 193
- Bitcoin Cash (CCC: BCH-USD): 60
- Litecoin (CCC: LTC-USD): 56
- Dash (CCC: DASH-USD): 48
- Ethereum (CCC: ETH-USD): 20
- Bitcoin (CCC: BTC-USD): 7.

Как видно из таблицы, в области производительности классическая система Visa пока остаётся вне конкуренции.

Разработчики блокчейн-платформ прилагают большие усилия по оптимизации архитектуры для достижения конкурентоспособных значений. Перспективные технологии в этом направлении – т.н. шардинг (sharding), который в случае публичного блокчейна означает распределение транзакционной нагрузки в сети на различные сегменты, состоящие из разных узлов, применение направленных ациклических графов (DAG, от directed acyclic graph) и другие.

Правовые проблемы

Из нетехнологических проблем стоит прежде всего отметить отсутствие какого-либо правового статуса смарт-контрактов, а также признания юридической значимости записей, удостоверенных с помощью технологии блокчейн.

Кроме того, не определены вопросы юрисдикции, в которой совершаются транзакции (она может быть любой, или их может быть несколько, в соответствии с размещением нод блокчейна), конфиденциальности данных в блокчейне, права собственности на эти данные, вопросы ответственности за риски при работе с данными (утечки или потери).

Технология блокчейн и цифровая трансформация

Исходя из описанной выше роли технологии блокчейн – можно сделать вывод, что она, скорее, более пригодна для локальной цифровизации определенных бизнес-процессов взаимодействия различных контрагентов (как непосредственного, так и в рамках создаваемых платформ), нежели для глобальной цифровой трансформации бизнеса.

По крайней мере, на данный момент неизвестны проекты, в которых использование технологии блокчейн кардинальным образом сказалось бы на принципиальном изменении продуктовой линейки, появлении бизнес-модели компании, смене или развитии нового рынка. При этом, понятно, особняком должны рассматриваться криптовалюты, которые пока являются по сути одним из финансовых деривативов – либо служащих предметом спекуляций, либо призванных определенным образом организовывать альтернативные методы расчетов. Но ни в одном из стартовавших крипто-проектов на данный момент пока так и не возникла экосистема, основанная на криптовалюте, смарт-контрактах, принципиально новых крипто-продуктах (финансовых, страховых, логистических и т.п.) – все это пока остается предметом разного рода мечтаний криптоэнтузиастов.

[12] https://howmuch.net/articles/crypto-transaction-speeds-compared.