Отчет IOSCO по исследованию финансовых технологий

Технологии распределенных баз данных (DLT)
(перевод)

Февраль 2017

OICV-IOSCO
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

Глава 5: Технологии распределенных баз данных

5.1. Введение

Распределенная база данных — совокупность копируемых, находящихся в совместном доступе и синхронизированных цифровых данных, географически распределенных по разным местам странам и/или институтам. Технологии распределенных баз данных (технологии РБД) — технологии, используемые для внедрения распределенных баз данных.

Существует широкий спектр технологий РБД. Для целей настоящей главы и в соответствии с подходом, используемым в сфере финансовых услуг, к указанному термину относится также технологии *блокчейн* и технологии распределенного реестра. Как поясняется ниже, базы данных основанные на технологии «распределенного реестра» *(shared ledger)* не основаны на концепции блокчейн.

Технологии РБД привлекли внимание в сфере финансовых услуг по нескольким причинам:

- Технологии РБД, с доступом на основе особых разрешений, могут предоставлять возможность снижения издержек в том случае если она используется для замены устаревших систем и связанных с ними процессов бэк-офиса.

- Технологии РБД с доступом без особых разрешений, возможно, несут в себе риски. Например, в том случае, если она используется для уменьшения числа посредников между финансовыми институтами и центральными контрагентами[106].

Рост значения технологий РБД наилучшим образом иллюстрируется цифрами, опубликованными на Международном экономическом форуме в августе 2016 г.[107]:

Более 1.4 млрд. долларов США было инвестировано в венчурные проекты с РБД с 2013 г.

Более 2500 патентов на РБД с 2013 г., многие из которых зарегистрированы финансовыми институтами;

Более 24 стран в настоящее время инвестируют в технологии РБД;

Более 90 центральных банков вовлечены в дискуссии по вопросами РБД;

Более 90 корпораций присоединились к консорциуму по технологиям РБД; и

Предположительно 80% банков в 2017 г. начнут проекты, связанные с технологией РБД[108].

---

106 Биткойн является примером исключения посредников из традиционных платежных систем, *Ethereum* DAO является примером исключения посредников из процесса привлечения венчурного капитала. См. §5.2(x)

107 См. *World Economic Forum*. Будущее финансовой инфраструктуры (*The future of financial infrastructure*) — амбициозная книга о том, как блокчейн может изменить финансовые услуги, 2016, http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

108 Более подробная литература:
U.K. Government Office for Science, Технология распределенных баз данных: после блокчейн (Distributed Ledger Technology: beyond block chain), 2016, www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
Gareth W. Peters and Efstathios Panayi, Понимание современных банковских распределенных БД с помощью технологии блокчейн (Understanding Modern Banking Ledgers through Blockchain Technologies), UCL, 2015, www.weusecoins.com/assets/pdf/library/Understanding%20Modern%20Banking%20Ledgers%20through%20Blockchain%20Technologies.pdf.
McKinsey & Co., Трезвый взгляд: блокчейны на рынках капитала (Beyond the Hype: Blockchains in Capital Markets), 2015, www.the-blockchain.com/docs/Blockchains%20in%20Capital%20Markets.pdf.
Goldman Sachs, Блокчейн — реализация теории на практике (Blockchain – Putting Theory in Practice), 2016, www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf.
блог R3CEV http://r3cev.com/blog/ и библиотека для исследователя, http://r3members.com/#Library.

(I) Традиционные и распределенные БД

Традиционная БД представляет собой централизованную информационную систему, которая доступна через определенных ее участников и которая находится под наблюдением одного или большего количества «системных администраторов». Последние регулируют доступ к данным, хранящимся в БД и контролируют их целостность. Системы управления традиционными базами данных, обычно используемые финансовыми институтами, обеспечивают возможность доступа к ее информации через доверенных и известных пользователей.

РБД представляет собой децентрализованную базу данных, доступную для использования и контролируемую множеством ее участников. Такие участники называются *«нодами»* децентрализованной сети базы данных. *«Полноправные ноды»* пользуются в отношении РБД системообразующими правами. С другой стороны, «легкие ноды» являются ее пассивными участниками[109]. Любое обновление данных подтверждается *полноправными нодами*, которые с помощью особого механизма *«консенсуса»* достигают согласия относительно текущего состояния базы данных.

(II) Технология блокчейн, как один из типов технологии РБД.

Технология блокчейн использует имеющие электронную подпись временные ряды данных или записей, объединенных в блоки, взаимосвязи между которыми также имеют цифровую подпись. Таким образом, усложняется возможность искажения данных.

Технология блокчейн примененная в проекте Биткойн является первой, наиболее распространенной и в наибольшей степени исследованной технологией РБД. Она использует очень сложный механизм «консенсуса» («майнинг», рассматриваемый как «опытное внедрение» *(proof of concept)* такого механизма объясняется далее в настоящей главе) для валидации и авторизации внесения новой информации в базу данных. Распределенная природа технологии системы Биткойн достигаемая за счет использования блоков и хэш-функций (в результате которых отпадает необходимость в центральном контрагенте или центральной базе данных) вместе со сложным механизмом консенсуса (решающую проблему доверенных участников, характерную для интернета и иных сетей при взаимоотношениях между неизвестными, распределенными сторонами) являются наиболее важными и поэтому наиболее исследованными инновациями внедренными Биткойн.

Доклад *Goldman Sachs* содержит краткие выводы, объясняющие основные концепции функционирования механизма консенсуса в блокчейн[110]:

1) Это база данных содержащая информацию о транзакции между двумя или большим числом ее сторон, резервные копии которой хранятся во многих точках на соответствующих компьютерах, являющихся узлами информационной системы – *нодами (node)*.

2) Подобная база данных состоит из «цепочек блоков» (*blockchain*), каждый из которых содержит данные, такие как детали транзакции — продавец, покупатель, цена, условия транзакции и другие значимые детали.

3) Детали транзакции, содержащиеся в каждом из блоков, проходят валидацию со стороны всех *нодов* сети посредством алгоритма, называемого «хеширование». Транзакция подтверждается в том случае, если результат хеширования подтверждается всеми *нодами*.

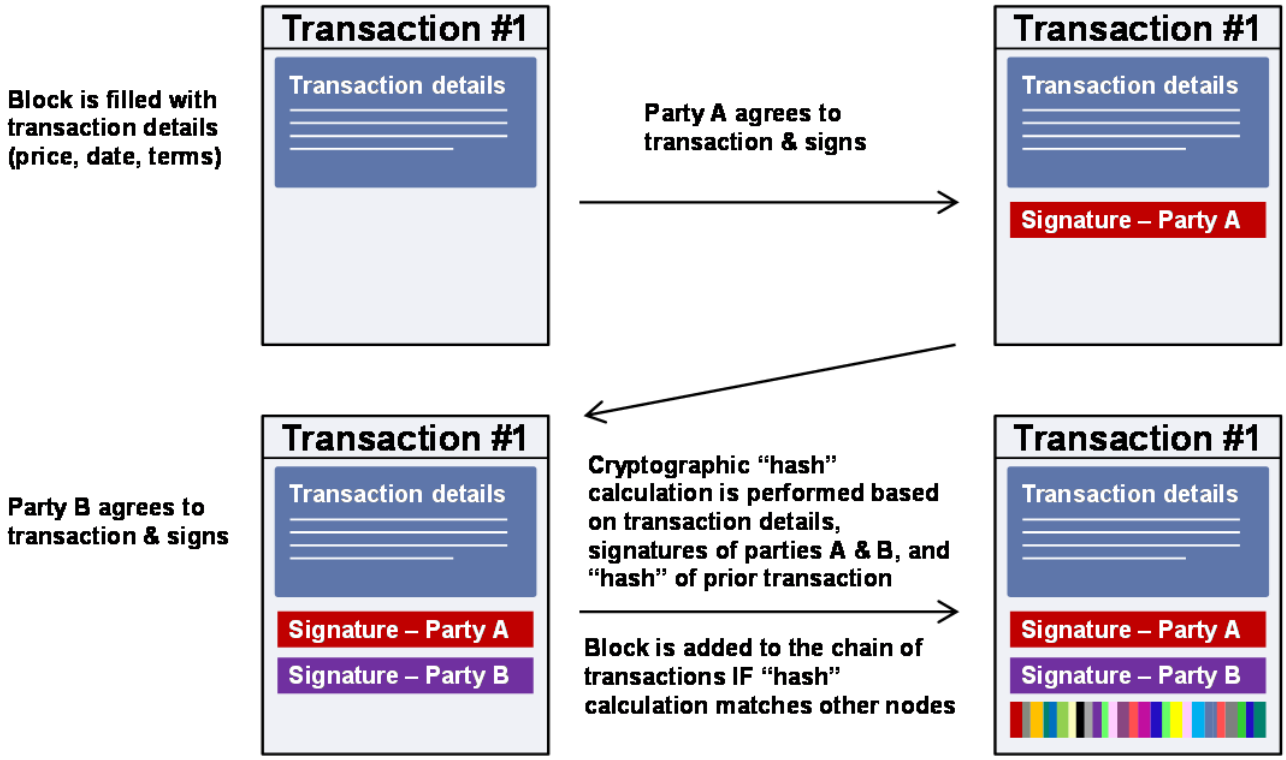
ЕСВ, Рассмотрение актуальных вопросов: технологии распределенных баз данных в сфере ценных бумаг (на посттрейдинговой стадии) (Occasional Paper Series: Distributed ledger technologies in securities post-trading), 2016, www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf ESMA, Документ для обсуждения (применение технологии распределенных баз данных на рынке ценных бумаг (Discussion Paper - The Distributed Ledgers Technology Applied to Securities Markets), 2015, www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf . .

109 См. Bitcoinwiki https://en.bitcoin.it/wiki/Full_node .

110 Goldman Sachs, Блокчейн — реализация теории на практике (Blockchain – Putting Theory in Practice), 2016.

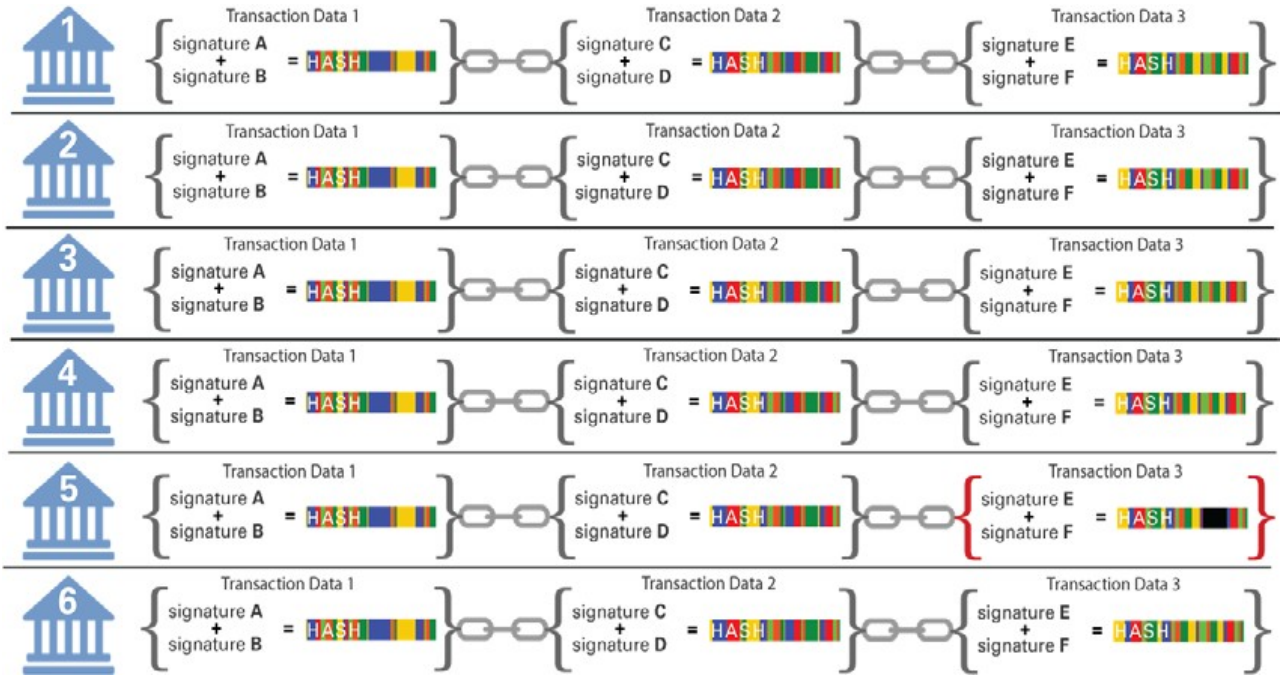
4) Новый блок добавляется к существующей цепочке транзакций только в том случае, если он успешно проходит валидацию.

Рисунок 10: Ниже показан процесс создания и валидации блоков, содержащих информацию о конкретной транзакции. Для обеспечения целостности передаваемых данных часто используются криптографические хеш-функции, такие как аутентификация и шифрование.



Источник: Глобальный инвестиционный доклад *Goldman Sachs*

Рисунок 11: База данных по технологии блокчейн размещена во многих точках (в данном примере в шести. Точек может быть больше.) и в каждом хранится собственная копия, которая отдельно обновляется при получении новых данных о транзакциях. В первых двух транзакциях данные и подписи надлежащим образом прошли валидацию со стороны всех шести нодов, т.е. были получены совпадающие значения хеша. В транзакции № 3 в точке № 5 значение хеша не совпало с другими и будет скорректировано другими сторонами с помощью механизма консенсуса.



Источник: Глобальный инвестиционный доклад Goldman Sachs

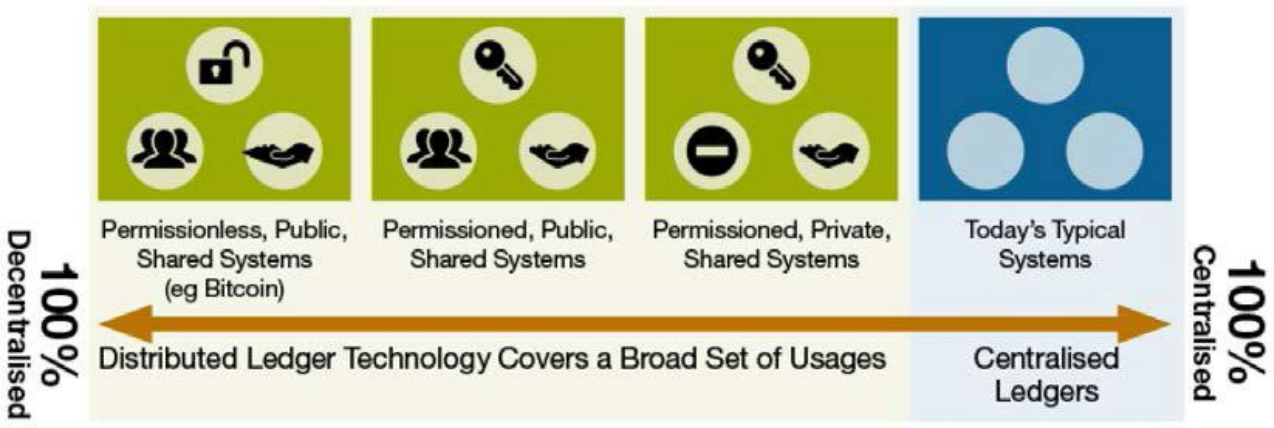
(III) Технологии распределенных БД, требующие и не требующие особых разрешений для доступа к ним

Не требующие особых разрешений для доступа РБД, например, блокчейны Биткойн и Этериум являются открытыми системами, которые не имеют ограничений на участие. Участники таких РБД выполняют функции *нодов* в сети, имеют права доступа к базе данных, права добавления информации в базы данных и участия в процессе валидации. Подобные базы данных не требуют наличия центрального контрагента или доверенных участников. Доверенные участники здесь замещаются математическим алгоритмом консенсуса, встроенным в РБД.

К РБД, требующим особых разрешений, относятся многие потенциальные сферы применения и «опытные внедрения» рассматриваемые в п. 5.2 ниже. Последние изучаются сферой финансовых услуг и представляют собой системы совместно используемые доверенными участниками, имеющими авторизованный доступ к системе. Управляющие узлы РБД (включая совместно используемые базы данных), осуществляют авторизацию каждого нового участника в соответствии с установленными критериями и определяют *ноды*, используемые в процессе верификации.

Как показано на рисунке 12 ниже, технологии РБД, требующие особых разрешений, не являются полностью децентрализованными и использует институт доверенной/обладающей особыми правами стороны. Этим они фундаментально отличаются от блокчейна Биткойн, который является полностью децентрализованной базой данных с анонимными участниками.

Рисунок 12: Степени централизации БД



о
нсенсуса

Алгоритмы консенсуса представляют собой технологии, которые устраняют необходимость в доверенных участниках РБД. Двумя наиболее часто используемыми алгоритмами консенсуса являются «*доказательство проведенной работы*» *(proof-of-work)* и «*доказательство доли*» *(proof-of-stake). Доказательство проведенной работы* требует наличия значительных компьютерных мощностей и является энергоемким, в то время как *доказательство доли* является капиталоемким. Таким образом, использование обоих алгоритмов не является бесплатным.

Алгоритм *«доказательство проведенной работы»* представляет собой алгоритм консенсуса, обычно используемый в технологиях РБД, не требующих особых разрешений (в том числе в блокчейн Биткойн). Указанный алгоритм использует некоторое количество «*полноправных нодов*» в сети, которые добровольно осуществляют валидацию данных. Определенные привилегии, как правило, в форме цифровых активов, даются тому *ноду*, который быстрее прочих закончил валидацию, завершив расчет значения хэша.

Алгоритм *«доказательство проведенной работы»* имеет свои сильные стороны и в достаточной степени обеспечивает защиту от искажений. Тем не менее, у него есть и слабые стороны, т.к. указанный алгоритм требует значительных вычислительных мощностей и электроэнергии. Чем шире блокчейн, не требующий особых разрешений для доступа, тем более централизованной становится сеть, т.к. все меньшее число *нодов* имеет достаточные вычислительные мощности для верификации транзакций. Кроме этого, длительность обработки увеличивается вместе с числом транзакций в каждом блоке.

Рисунок 13: Эволюция емкости блокчейн Биткойн с 2013 по 2106 гг.

	Август 2014	Август 2015	Август 2016
Подтвержденное количество транзакций в день	60 000	120 000	220 000
Среднее число транзакций в блоке	500	800	1 500
Средний размер (Мб) — лимит 1 Мб	0.25	0.55	0.80
Время подтверждения и время майнера (мин)	7	8	8.5
Общая стоимость транзакции (биткойн)	12	25	60

Источник https://blockchain.info . Прим.: данные являются приблизительными

Алгоритм консенсуса *«доказательство доли»* используется в некоторых технологиях РБД, требующих особых разрешений для доступа. Указанный алгоритм требует соединения (называемого *связывание*) некоторого числа цифровых активов для валидации и добавления новых блоков в блокчейн. Чем больше цифровых активов связано, тем выше вероятность быстрейшей валидации блоков и получения какого-либо поощрения. *Связанные активы* аналогичны концепции предоставления дополнительного обеспечения и получения финансовых ресурсов.

(V) Роль токенизации активов и бумажных денег.

Токенизация — процесс цифрового представления актива или собственника актива. *«Токен» (token)* представляет собой актив или его собственника. Такими активами могут быть деньги, товары, ценные бумаги или права собственности.

Для широкого использования технологий РБД в торгах и учете ценных бумаг, последние должны быть «*токенизированы*». Соответственно, *токены* должны быть предусмотрены законодательством для того, чтобы представлять собой легитимное подтверждение права собственности на активы. Кроме этого, и деньги должны быть *токенизированы* для того, чтобы они могли выполнять функции средства расчетов по транзакциям, обрабатываемым с помощью технологий РБД. Как будет объяснено далее в разделе 5.4, в настоящее время в качестве альтернативных решений отраслью рассматриваются т.н. *«расчетные монеты» (settlement coins)* для осуществления расчетов по транзакциям в рамках РБД, требующей особых разрешений для доступа.

(VI) Роль умных контрактов.

«Умные контракты» (smart contracts) — это компьютерные программы, работающие в распределенной сети. Они представляют собой предварительно написанную логику[111] проведения операций, хранящуюся и исполняемую *нодами* в РБД[112]. После исполнения и верификации действий, осуществленных *умным контрактом,* последнее состояние информации (результат действий), связанной с деловой операцией будет записано и сохранено в блоке[113].

Исследуемыми в настоящее время возможностями применение *умных контрактов* на рынке ценных бумаг являются торги ценными бумагами, расчеты и клиринг, корпоративные действия и управление маржинальными позициями и обеспечением.

Для того, чтобы *умные контракты* могли использоваться, должна иметь место четкая правовая определенность, а сами умные контракты должны быть предусмотрены законодательством[114,115]. Сложность также представляет тот факт, что *умные контракты*

111 Например, «Если…, то...», утверждение говорящее о том, что «Если произойдет X, сделайте Y, в ином случае F»

112 Первое поколение блокчейн было создано для осуществления небольшого набора простых операций - в основном сделок с обладающими признаками платежного средства *токенами*. Технологии развивались и сейчас позволяют выполнять более сложные операции, подразумевающие использование полноценного программирования. Это означает появление трех новых особенностей:

Программа записывается в блокчейн . таким образом обеспечивается устойчивость информации и защита от искажений.

Программа может контролировать активы базы посредством передачи цифровых активов, учитываемых в блокчейн.

Программа исполняется блокчейн.

113 Энтони Льюс, автор портала Bitsonblocks.net, отмечает «если блокчейн дает нам заслуживающее доверия распределенное хранилище, то умные контракты обеспечивают нас заслуживающими доверия распределенными вычислениями» См.: https://bitsonblocks.net/

114 См., например, список правовых вопросов на стр. 57 совместного документа HKMA и ASTRI: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf .

являются детерминированными по своей природе и исключают гибкость и опциональность, свойственную документарным контрактным соглашениям. Таким образом, имеется необходимость наличия механизмов, позволяющих приостановить или отменить действие контрактов в определенных случаях [116].

5.2. Эволюция рынка / потенциальные сферы применения

В финансовой сфере имеет место большое количество подготавливаемых *«опытных внедрений»* концепций РБД, включающих инновационные хабы, акселераторы, инкубаторы и консорциумы и партнерства со стартапами. Но, несмотря на это, еще только предстоит выяснить то, в какой степени технологии РБД (и какие именно технологии РБД) решают анализируемые проблемы.

Ниже приведенные примеры представляют собой наиболее известные публично анонсированные *опытные внедрения* концепций РБД. Следует отметить, что большинство из них представляют собой технологии РБД, требующих особых разрешений на доступ (включая технологии *распределенного реестра*).

Технологии РБД, требующие особых разрешений, являются более простыми для внедрения т. к. указанные базы данных распределяются между известными, идентифицированными и доверенными сторонами. Кроме этого, некоторые финансовые институты могут рассматривать подобные технологии как более предпочтительные для регулируемой в существенной степени сферы ценных бумаг: несмотря на то, что могут осуществляться (и уже осуществляются) и небольшие переводы и транзакции с помощью баз данных, не требующих особых разрешений, деятельность межбанковского рынка и глобального рынка ценных бумаг связана с большими объемами денежных средств и не может осуществляться без доверия между его участниками.

Многие из упомянутых *опытных внедрений* технологий РБД, требующих специальных разрешений и находящихся в *совместном доступе* БД вдохновлены технологией Биткойн. На рис 12 показано, что они существенно отличаются от первоначальной концепции блокчейн Биткойн (как полностью децентрализованной и не требующей особых разрешений для доступа РБД). Технологии РБД и *распределенного реестра* зачастую рассматриваются как применения концепции баз данных в формирующихся бизнес-моделях с одинаковыми или похожими посредниками и контрагентами.

В то же время, в другой части децентрализованного спектра (см. рис.12), компании, такие как *Ethereum, Ripple, Circle* и *TransferWise* продолжают исследовать широкие возможности опытных внедрений концепций и приложений, применимых в технологиях РБД, не требующих особых разрешений для доступа, включающих потенциальные области применения вне сферы финансовых услуг, таких как права на фильмы, хранение записей по происхождению предметов искусства, драгоценных камней и других ценностей; и частная торговля солнечной энергией.

---

115 См. блог Oxford University *Умные контракты: совпадение ожиданий и реальности* в котором предлагается «оболочка»: «правовая оболочка должна предусмотреть код умного контракта с помощью ссылки на него в простом контракте, но простой контракт должен иметь преобладающую силу в случае несоответствия между ними» https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality .

116 См. Блог Oxford University *Умные контракты: совпадение ожиданий и реальности*, отмечающий: в коде *умного контракта* должен быть предусмотрен механизм защиты от ошибок, при котором сторона контракта могла бы осуществить приостановку или отмену выполнения кода *умного контракта* при наступлении согласованных сторонами событий (например, доверенный орган управления, обладающий универсальным ключом электронных подписей).

См. также http://www.nortonrosefulbright.com/files/smart-contracts-coding-the-fine-print-excerpt-137900.pdf ; and http://f.datasrvr.com/fr1/416/66238/2.pdf .

Данный раздел подчеркивает известные публично анонсированные *опытные внедрения* технологии РБД в сфере ценных бумаг. Примеры соответствуют выводам из исследования *WFE/AMCC*[117].

(I) Ведение корпоративных реестров

В октябре 2015 г. *NASDAQ* продемонстрировала *LINQ* — платформу использующую блокчейн для ведения электронных реестров собственников акций, эмитированных частными компаниями на стадии до IPO[118].

LINQ представляет собой РБД, использующую особые разрешения для доступа. В декабре 2015 г. *Chain.com*, частная компания, занимающаяся развитием технологии блокчейн опубликовала пресс-релиз, в котором сообщала об эмиссии акций для частных инвесторов с использованием платформы *LINQ*[119].

Некоторые краудфандинговые платформы используют технологию блокчейн для учета собственников ценных бумаг. Комбинирование технологии блокчейн и концепции краудфандинговой платформы потенциально может снизить издержки, связанные с процессом андеррайтинга, учетом прав собственности и корпоративными действиями.

Другим примером можно считать онлайн ритейлера *Overstock.com*, который объявил, что с помощью своего дочернего финансово-технологического подразделения T0 в июле 2015г. было осуществлено размещение корпоративных криптооблигаций в объеме 5 млн. долларов США[120].

(II) Повышение эффективности корпоративных процессов

Корпоративное действие представляет собой событие, инициированное компанией, оказывающее влияние на собственников эмитированных компанией ценных бумаг. К типичным корпоративным действиям относятся выплаты дивидендов или купонов по облигациям, досрочное погашение ценных бумаг, выпуск дополнительных акций, дробление ценных бумаг и голосование по доверенности.

Для осуществления корпоративных действий необходим информационный обмен между множеством сторон, например между компаниями-эмитентами, инвесторами,

---

117 Исследование показало, что «биржи и посттрейдинговые инфраструктуры изучают множество возможных вариантов использования РБД. В том числе: клиринг и расчеты (та область на которую, по мнению респондентов, технологии РБД окажут наибольшее влияние); мэтчинг и подтверждение торгов (не в традиционных секциях (торги осуществляются на бирже), а в активах сравнительно меньшего объема, например, с фиксированным доходом, внебиржевые деривативы, рынок репо и частный рынок ценных бумаг; корпоративные действия (голосование и дивидендные платежи)corporate actions (voting rights and dividend payments); эмиссия ценных бумаг для частных приобретателей; краудфандинг, регистрация на торгах; отчетность регулятору и прозрачность, базы данных по индентификации клиентов/ противодействию отмыванию доходов; финансирование торгов; регистрация активов (например, недвижимости), цифровые активы и связанные продукты www.world-exchanges.org/home/index.php/files/18/Studies%20-%20Reports/349/WFE%20IOSCO%20AMCC%20DLT%20report.pdf .

118 http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326 и http://ir.nasdaq.com/releasedetail.cfm?releaseid=938667

119 см. выше

120 Overstock размещает корпоративные облигации, объявляя себя первой компанией по криптобезопасности (Overstock Launches Corporate Bond Billed as World's First Cryptosecurity) (Wall Street Journal; June 5, 2016), http://www.wsj.com/articles/overstock-launches-corporate-bond-billed-as-worlds-first-cryptosecurity-1433549038 .

Ритейл-гигант Overstock эмитирует собственные ценные бумаги на платформе блокчей (Retail Giant Overstock to Issue its Own Stock on Blockchain Platform) (Coindesk; March 16, 2015), http://www.coindesk.com/overstock-blockchain-stock/ .

Принадлежащий Overstock TØ эмитирует первые ценные бумаги на платформе блокчейн (Overstock's TØ to Issue First Public Blockchain Equities) (Bitcoin.com; September 17, 2016).

посредниками (кастодианами и регистраторами), биржами и регуляторами. Подобный информационный обмен, как правило, приводит к дублирующим процессам и к обмену, верификации и обновлению одних и тех же данных в разных БД.

С помощью технологий РБД и *умных контрактов* исследуются возможности повышения эффективности вышеупомянутых процессов. Например:

- Корпоративные действия, приводящие к изменению стоимости ценных бумаг или имущества инвесторов, в частности, дробление акций, дивиденды и купонные выплаты могут быть запрограммированы в рамках *умных контрактов* для автоматизации подобных изменений.

- Корпоративные действия, требующие принятия решений, таких как голосование по доверенности или приглашение к участию в дополнительном выпуске ценных бумаг, могут быть обработаны с использованием технологий РБД.

NASDAQ и Республика Эстония обеспечили возможность использования платформы электронных госуслуг для предоставления возможности электронного голосования (основанного на технологии блокчейн). Данная платформа обеспечивает возможность голосования на общих собраниях акционеров для владельцев ценных бумаг компаний, прошедших листинг на единственном регулируемом эстонском рынке ценных бумаг *Nasdaq's Tallinn Stock Exchange*[121].

Делавар, штат в котором зарегистрировано большинство компаний США, также объявил о работе над проектом блокчейн для автоматизации процессов, связанных со значительным использованием документов на бумажном носителе. В частности процессов ведения реестров акционеров, управления капитализацией компании и взаимодействие с акционерами частных компаний[122].

(III) Совершенствование пост-трейдинговых операций по ценным бумагам, торгующимся на бирже.

В январе 2016 г. австралийская фондовая биржа *(ASX)* и использующий технологию РБД стартап *Digital Asset Holdings* объявили о проекте по улучшению клиринговых и расчетных процессов по обыкновенным акциям (*CHESS)*[123]. Целью проекта является упрощение и ускорение пост-трейдингового процесса, который на австралийском фондовом рынке осуществляется в течении двух дней. *ASX* также объявила о взаимодействии со *SWIFT* в части определения функциональности, приведения в соответствие технических требований и бизнес-процессов использующихся в CHESS сообщений к эквиваленту сообщений стандарта *ISO 20022* на предварительной стадии проекта[124].

Данный проект опирается на использование технологии РБД, в процессах клиринга, расчетов и обслуживания активов. Благодаря стандартизации данных и автоматизации процессов обеспечивается снижение операционных рисков. Затраты на комплаенс и на аудит таким образом также уменьшаются в разы, благодаря неизменности и прозрачности характеристик блокчейн.

121 http://ir.nasdaq.com/releasedetail.cfm?releaseid=954654

122 http://global.blogs.delaware.gov/2016/06/10/delaware-to-create-distributed-ledger-based-share-ownership-structure-as-part-of-blockchain-initiative/ .

123 www.asx.com.au/documents/about/ASX-Selects-Digital-Asset-to-Develop-Distributed-Ledger-Technology-Solutions.pdf ; http://www.asx.com.au/documents/public-consultations/ASX-Consultation-Paper-CHESS-Replacement-19-September-2016.pdf ; https://digitalasset.com/press/asx-selects-digital-asset.html

124 См. Также https://www.swift.com/insights/press-releases/swift-examines-application-of-financial-business-standards-to-distributed-ledger-technology-and-smart-contracts .

(IV) Торги и расчеты по внебиржевым деривативам

Контракты по деривативам представляют собой финансовые инструменты, стоимость которых обеспечивается *связанными* активами, например, акциями, облигациями, товарами или процентными ставками. Стороны контрактов по деривативам должны привести денежные потоки в связи с изменением стоимости контракта и связанными с ней маржинальными или обеспечительными позициями. Кроме этого существует множество каналов ежедневного информационного обмена между сторонами для оценки и движения денежных потоков в течение срока действия контракта по деривативам.

С помощью трансформирования внебиржевых деривативов в *умные контракты* и учета денежных потоков в РБД, может быть достигнуто упрощение информационного обмена и денежных потоков. Таким образом, могут быть снижены операционные и расчетные риски.

Barclays сообщил об изучении использования технологии блокчейн и *умных контрактов* для торгов деривативами в апреле 2016г[125]. Некоторые клиринговые организации, например *DTCC* также объявило об исследованиях в указанной сфере[126].

(V) Упрощение процесса синдицированного кредитования

Стандартный цикл организации кредитования от его инициирования через *дью дилидженс*, андеррайтинг, к закрытию сделки и посттрейдингу занимает недели и требует большого числа неавтоматизированных процессов. Кроме этого, не существует общей технологической платформы, предназначенной для записи и обмена соответствующей информацией, что ведет к дублированию процессов.

Умные контракты, используемые в РДБ, требующих особых разрешений, тестируются на предмет сокращения операционных рисков, временных затрат и издержек затрат и времени на различные процессы.

В январе 2016 г. *JP Morgan* объявил о запуске совместно с *Digital Asset Holdings* пробного проекта блокчейн, предназначенного для упрощения процесса синдицированного кредитования.[127]

(VI) Учет сделок репо и повторного залога

Соглашение об обратном выкупе (репо) представляет собой метод получения краткосрочного финансирования у финансовых институтов с использованием ценных бумаг в качестве обеспечения обязательств. Процесс сделки репо включает в себя ведение записей о передаче фондов заемщику и об обеспечении позиции у кредитора. Рыночная практика повторного залога позволяет получателю обеспечения передать то же самое обеспечение от одного финансового института другому и так далее в рамках лимита, установленного регулятором.

Токенизация обеспечения займа и ведение учета сделок репо и транзакций последующего залога в рамках распределенной БД может улучшить прозрачность обеспечительных позиций, а также автоматизировать соблюдение лимитов регулятора.

DTCC и *Digital Asset Holdings* анонсировали изучение применения технологии РБД для управления сделками репо[128]. Некоторые регуляторы финансового рынка также

125 http://www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html .

126 http://www.dtcc.com/news/2016/january/25/new-dtcc-white-paper-calls-for-leveraging-distributed-ledger-technology ; http://www.dtcc.com/news/2017/january/09/dtcc-selects-ibm-axoni-and-r3-to-develop-dtccs-distributed-ledger-solution

127 www.ft.com/cms/s/0/2d3f9296-c5ef-11e5-b3b1-7b2481276e45.html#axzz4HJQwkme5 .

128 https://digitalasset.com/static/documents/PRESS_RELEASE_DTCC_Digital_Asset_Repo_POC.pdf

выражали интерес в *опытном внедрении* концепции, которая могла бы обеспечить прозрачность сделок репо и повторного кредитования (которые иногда рассматриваются как форма «теневого банкинга»)[129].

(VII) Торги краткосрочными долговыми обязательствами

R3, - консорциум технологий РБД взаимодействовал с сорока финансовыми институтами в начале 2016 г. для исследования различных решений в сфере применения блокчейн для транзакций с коммерческими ценными бумагами (векселями)[130]. Вексель был выбран для пилотного проекта в связи с коротким жизненным циклом (расчеты осуществляются в тот же день, а погашение в течении 270 дней).

Целью проекта была стандартизация транзакционного процесса с помощью отслеживаемых записей и сокращения периода расчетов до 1 часа. Участвующие финансовые институты моделировали транзакции, путем кодирования *умных контрактов*, использующих разные подходы и анализа того, какой из них наиболее увеличивает эффективность эмиссии, торгов, передачи и выкупа векселя.

(VIII) Автоматизация финансовыми институтами комплаенс-процессов идентификации клиента и противодействия отмыванию доходов

Информация о клиенте и история транзакций, как правило, хранится в отдельных информационных системах финансовых институтов. Выполнение комплаенс-процессов идентификации и противодействия отмыванию доходов требует существенных неавтоматизированных действий для получения, агрегирования и проверки информации из разных источников.

Согласно концепции, технологии РБД могут быть использованы для упрощения комплаенс-процессов благодаря тому, что: a) осуществляется обмен информацией о клиенте между финансовыми институтами для уменьшения числа дублирующих действий при работе с клиентом; b) производится кодирование счетов клиентов для увеличения прозрачности в процессе изучения транзакций; c) хранение всех записей о транзакциях в одной базе данных для упрощения процессов изучения и аудита[131]. Тем не менее, для получения подобного результата должны быть решены вопросы конфиденциальности персональных данных.

(IX) индивидуальный цифровой идентификационный код

Большое число стартапов в сфере блокчейн работают в направлении *опытного внедрения* концепции цифрового идентификационного кода. Концепция состоит в создании записи о физическом лице в блокчейн. Данная запись содержит не только традиционные идентификационные данные, например, адрес, копию документа, удостоверяющего личность и телефонный номер, но и биометрические данные, а также записи принятые/ верифицированные третьими сторонами (университеты, государственные органы, работодатели и финансовые институты)[132].

Рассматриваемую концепцию пока трудно реализовать без общественного/государственного участия, влекущего множество преимуществ, в том числе и

---

129 http://blogs.wsj.com/moneybeat/2016/06/07/blockchain-technology-gets-a-hearing-inside-the-feds-headquarters/ .

130 https://www.r3cev.com/press/2016/3/9/ex3a0t79rq7ddy3cfunvyszl47tbva

131 Goldman Sachs, Блокчейн — реализация теории на практике, 2016. См.также Hong Kong SFC: http://www.sfc.hk/web/EN/files/ER/PDF/Speeches/SFC%20Regtech%20and%20Fintech_07112016.pdf .

132 http://www.sfc.hk/web/EN/files/ER/PDF/Speeches/SFC%20Regtech%20and%20Fintech_07112016.pdf ; http://www.ibtimes.co.uk/consensys-digital-identity-wallet-system-uport-integrates-digix-gold-platform-1541580 .

для финансирования ее внедрения и лучшей идентификации клиентов финансовыми институтами[133].

(X) Альтернативное финансирование

Децентрализованная Анонимная Организация (ДАО) является первым в мире виртуальным, полностью децентрализованным венчурным фондом. ДАО начал работу на платформе блокчейна *Ethereum* в июле 2016 г. [134]. Объем инвестиций в фонд составил 150 млн. долл. США, путем обмена *Ethe*r (ETH, виртуальной валюты *Ethereum*) на *токены* ДАО. Указанные *токены* предоставляют право голосования и право собственности инвесторам в рамках виртуального венчурного фонда. Миссия ДАО состоит в предоставлении капитала для стартапов[135].

Разница между ДАО и другими частными фондами акционерного капитала или инвестиционными фондами состоит в отсутствии известного инвестиционного менеджера. Все инвестиционные решения являются полностью децентрализованными и принимаются использующими псевдонимы владельцами ДАО - *токенов* с помощью электронного голосования. Правила подобного голосования закодированы в *умные контракты*, управляющие работой ДАО. Другими словами, кодирование заменяет управление активами, устанавливая прямую связь между инвесторами и реализацией инвестиционной стратегии. Инвестиции в ДАО основываются на решениях принятых множеством инвесторов.

Подобная технологическая структура управления подняла ряд юридических вопросов, которые по-прежнему активно обсуждаются. К таким вопросам относятся:

(a) правовой статус ДАО;
(b) в какой юрисдикции находится фонд;
(c) может ли фонд законно заключать договоры;
(d) являются ли договоры действительными и могут ли они быть исполнены принудительно;
(e) можно ли подать иск к фонду и где это можно сделать;

Из всех рассмотренных выше экспериментов, ДАО является наиболее новаторским и наиболее сложным с юридической и регулятивной точек зрения.

Эти вопросы стали еще более актуальными, когда в июне 2016г. ДАО был взломан:[136,137] хакер использовал программную особенность в *умном контракте* для перевода средств (3.6 млн. ETH или около 41 млн. евро в тот период) «дочернему ДАО». Организация, заявляющая о том, что она в данном случае выступала в качестве хакера, говорит о том, что подобные действия были правомерны, т. к. они стали возможны в результате программных ошибок/уязвимостей в *умных контрактах* ДАО[138].

Изложенный выше пример демонстрирует риски в результате исключения посредников, которое может быть результатом внедрения концепции ДАО. Также он

133 http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf .

134 Основанная не Ethereum распределенная анонимная организация (ДАО) представляет собой организацию, использующую блокчейн и действующую в соответствии с предопределенными правилами, которые позволяют ее членам управлять ДАО и принимать коллективные решения. ДАО принципиально создано как средство достижения общих целей, которая будет как получать так и распределять фонды (часто в форме криптовалют или других использующих блокчейн токенов). Также используются контрольные процедуры для достижения общих целей ДАО. Создателем данного ДАО является компания, которая разрабатывает интернет и блокчейн решения в Германии.

135 www.coindesk.com/the-law-of-the-dao/?utm_source=CoinDesk+subscribers&utm_campaign=c82b48a412-EMAIL_RSS_CAMPAIGNT2&utm_medium=email&utm_term=0_74abb9e6ab-c82b48a412-79359605

136 Потенциальное внедрение распределенных БД и примеры использования (“Potential DLT Adoption and Use-Cases”), раздел section – Нарушение альтернативного финасирования.

137 http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ https://blog.slock.it/white-hat-siphoning-has-occurred-what-now-f7ba2f8d20ef#.4hp1wro05

138 http://pastebin.com/CcGUBgDG

демонстрирует уязвимость в программировании *умных контрактов* и поднимает вопросы применения норм законодательства к *умным контрактам*. См. также п. 5.1 (IV) выше.

5.3 Преимущества/возможности

Преимущества технологий РБД проявляются в результате опытных внедрений ее концепции. Подобная информация с трудом поддается обобщению. Ниже перечислено несколько наиболее часто упоминаемых потенциальных преимуществ применительно к финансовым услугам.

(I) Снижение издержек в расчетах

Различные исследования содержат выводы о том, что измеряемый объем издержек может быть уменьшен с помощью исключения неэффективных расчетов[139]. Экономия может достигаться за счет снижения вмешательства человека и снижения устанавливаемых регулятором лимитов в связи с уменьшением операционных и расчетных рисков.

(II) Более быстрые расчеты.

Одним из преимуществ технологий РБД является то, что они могут использоваться для обеспечения расчетов в реальном времени. Тем не менее, решения, относящиеся ко времени расчетов могут варьироваться в зависимости от типа актива, объема транзакций, требований ликвидности, влияния на маркет-мейкеров и текущей относительной эффективности конкретного сегмента рынка ценных бумаг. Таким образом, внедрение технологий РБД не обязательно приведет к осуществлению расчетов в реальном времени. Но указанные технологии могут привести время расчетов в соответствие с потребностями рынка, а не с технологическими ограничениями[140].

(III) Надежность и возможность отслеживания записей

Другим преимуществом технологий РБД является надежность и возможность отслеживания записей. В частности, при использовании базы данных, не требующей специальных разрешений для доступа, записи являются неизменяемыми. Любая попытка изменения сделанной ранее записи, например, блок истории изменений блокчейн, требует пересчета всех *хешей* блока, введенных последовательно в указанный блок. Если запись должна быть изменена или удалена, то необходимо осуществить операцию отмены, которая сама по себе является полностью отслеживаемым вводом данных. Если используется технология РБД, требующая особых разрешений для доступа к РБД, то каждый блок данных подписывается участником, добавляющим блоки. Для внесения изменений в запись об истории изменений, они должны быть приняты ограниченным перечнем участников. Подобные изменения являются отслеживаемыми.

---

139 Santander Innoventures, Документ финтех 2.0 — перезагрузка финансовых сервисов (The Fintech 2.0 Paper – rebooting financial services), June 2015, указал на ежегодную экономию от 15 до 20 млрд.долларов США на глобальных инфраструктурных издержках к 2022 г. www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf ;

Goldman Sachs, Goldman Sachs, Блокчейн — реализация теории на практике, май 2016, обозначил ежегодную экономию в сумме от 11 до 12 млрд. долларов США на глобальных затратах на расчетах по ценным бумагам.

140 См. FINRA, Доклад по технологии распределенных баз данных: внедрение технологии блокчей в сфере ценных бумаг (Report on Distributed Ledger Technology: Implications of Blockchain for the Securities Industry), 2017: http://www.finra.org/industry/report-distributed-ledger-technology-implications-blockchain-securities-industry

(IV) Автоматизированная отчетность регуляторам в реальном времени

Многие сторонники технологий РБД отмечают, что одним из преимуществ данной технологии является то, что регулятор может участвовать в качестве одного из *нодов* в РБД, таким образом, автоматически получая доступ ко всем данным. Это, в свою очередь, позволит регуляторам вести учет изменений информации в реальном времени.

(V) Включение новых типов активов

Многие эксперты в сфере технологий РБД отмечают, что одним из преимуществ данной технологии является то, что активы, имеющие значительную стоимость производства, осуществления транзакций с ними и доставки, например товары, энергия, предметы искусства, недвижимость и ценные бумаги, могут быть *«токенизированы»* для сохранности собственности на них. В свою очередь, *токенизация* делает возможным использование активов в качестве обеспечения.

(VI) Повышение эффективности

РБД могут заменить множество централизованных баз данных для улучшения обмена информацией и данными. Время, необходимое для валидации данных, варьируется в зависимости от структуры сети и механизма валидации. При использовании технологии РБД расчеты с ценными бумагами сокращаются с дней до минут. Перевод денег с использованием блокчейн Биткойн осуществляется в течении нескольких секунд или минут в отличии от действующий практики банковского обслуживания, при которой он занимает 2 или 3 дня.

(VII) Улучшение безопасности

Безопасность в блокчейн обеспечивается посредством шифрования блоков и связей между ними. Кроме этого, хакерская атака на каждый из *нодов* в блокчейне является более сложной для осуществления на текущей стадии технологического развития, чем атака на централизованную базу данных.

5.4 Угрозы/риски

Как продемонстрировано выше, большое число опытных внедрений рассматриваемых концепций в настоящее время еще находится на стадии тестирования. Даже если тестирование пройдет успешно, внедрение технологий РБД на рынке ценных бумаг, скорее всего, поднимет различные технологические и операционные вопросы, а также вопросы в части ведения бизнеса и регулирования. Угрозы/риски рассматриваемые ниже исследованы WFE[141]/AMCC[142] в отношении своих членов[143,144].

---

141 Всемирная федерация бирж, ВФБ (англ. World Federation of Exchanges, WFE, ранее FIBV) — мировая отраслевая ассоциация организаторов торговли ценными бумагами и производными инструментами.

142 Консультативный комитет аффилированных членов IOSCO.

143 Респонденты исследования WFE/AMCC выражали озабоченность вопросами безопасности, масштабируемости, мощности и возможности обеспечения сохранности персональных данных как потенциальные препятствия для полномасштабного внедрения технолгии распределенных БД. Один из респондентов, тем не менее отметил «Мы прилагаем усилия для выявления, понимания и решения известных технических ограничений. Насколько мы смогли изучить ограничения, они не вызывают серьезной озабоченности». Другой респондент был менее обеспокоен технологическими вопросами и более беспокоился об интеграции с существующей инфраструктурой и получением всеобщего согласия на переход на новое решение.

144 См.также Euroclear и Slaughter и May, Расчеты в среде блокчейн: регулирование, инновации и применение (Blockchain Settlement: Regulation, Innovation and Application), ноябрь 2016, https://www.euroclear.com/en/campaigns/Blockchain-settlement-Regulation-innovation-and-application.html .

Большинство экспертов отмечают, что технологии РБД находятся еще на очень ранней стадии развития и не являются зрелыми, подразумевая, что их широкое внедрение осуществится не в краткосрочной перспективе. Кроме этого, любое применение технологий РБД, связанное с использованием *умных контрактов* несет в себе риски, т. к. является новым методом и правовой статус таких контрактов еще не определен.

(I) Технологические вопросы

Масштабируемость

В зависимости от используемого типа технологии РБД, в том числе от механизма консенсуса, необходимо учитывать проблему масштабируемости. Например, в блокчейн Биткойн, как РБД, не требующая специальных разрешений для доступа, сталкивается с проблемами масштабируемости (показано на рис. 13 выше). Число транзакций, которое может быть обработано системой в секунду не является достаточной для расчетов по ценным бумагам в режиме реального времени. С другой стороны в БД, требующей особых разрешений, масштабируемость не является столь существенной проблемой.

Совместимость

Финансовые институты не намерены в агрессивной манере заменить существующую инфраструктуру, а наоборот стремятся постепенно внедрять изменения параллельно с уточнением правовых систем. Поэтому каналы взаимосвязи между технологиями РБД и правовыми системами являются критически важными. При отсутствии такой совместимости, совместное существование приведет к дополнительным издержкам, уменьшая преимущества от перехода к технологиям РБД, Например, в потенциальной сфере применения технологии для посттрейдинговых расчетов, необходимо обеспечить операционную совместимость между системами всех участников рынка (брокеров, эмитентов, инвесторов, торговых площадок, операторов инфраструктуры финансового рынка).

Помимо этого, необходимым является взаимодействие различных сетей, использующих технологии РБД, между собой. До того, как технологии будут стандартизированы, вероятно, многие сети и приложения будут решать задачи параллельно. Действующие протоколы взаимосвязи еще только предстоит разработать. Рассматриваются возможности использования *счетов эскроу* или *умных контрактов* для обеспечения взаимодействия при передаче данных или цифровых активов между разными сетями, использующими технологии РБД.

Кибербезопасность

Шифрование обеспечивает частичную защиту от рисков кибермошенничества. Например, с учетом опыта использования метода *доказательство проведенной работы в* блокчейне Биткойн, вредоносный *нод* должен обладать более чем 50% вычислительной мощности сети для контроля за блокчейном и процессом валидации[145]. Опыт эксплуатации блокчейна Биткойн показывает, что приобретение подобных мощностей является дорогостоящим.

Процесс валидации в соответствии с методом *доказательство доли* распределяет валидационные права в соответствии с долей участников в сети. Подобный процесс валидации является гораздо менее дорогостоящим, чем метод *доказательство проведенной работы.* При использовании указанного метода, издержки на вычислительные мощности, учитываемые методом *доказательство проведенной работы* трансформируются в

145 Тем не менее, по мнению Eyal и Sirer (2014), может быт достаточным обладать 25% вычислительных мощностей для валидации вредоносной транзакции http://fc14.ifca.ai/papers/fc14_submission_82.pdf .

репутационные издержки или потерю обеспечения, в том случае, если *ноды*, осуществляющие валидацию, попытаются фальсифицировать данные в РБД.

Наиболее распространенными угрозами являются не атаки на сети, а кражы или потери персональных ключей. Персональные ключи позволяют владельцам контролировать свои цифровые активы и, в случае их потери, контроль над активами также теряется. Кражи персональных ключей осуществляются различными способами. Например, хакеры смогли украсть биткойны на сумму около 500 млн.долларов США на бирже *Mt.Gox* в 2014г., не нарушив протокол блокчейна Биткойн, что в результате привело к закрытию данной биржи[146]. В упомянутом выше случае с ДАО, хакер использовал другой метод для кражи фондов: использовал ошибку в программном коде. Организация, заявляющая о том, что она выступала в данном случае в качестве хакера, утверждает, что ее действия были правомерны из-за ошибок/уязвимостей в умных контрактах ДАО[147].

Следует отметить, что квантовые компьютеры (несмотря на то, что находятся в экспериментальной стадии разработки), в теории, используя свои вычислительные мощности, смогут взломать криптографические технологии, в частности, *RSA*[148], *DSA*[149] и все процедуры, основанные на *ECC*[150]. Организации, обладающие подобным оборудованием, теоретически могут угрожать системам, опирающимся на использование указанных криптографических технологий и, в свою очередь, создавать риски для глобальной экономики[151]. Тем не менее, технологии распределенных БД являются не более уязвимыми для подобной возможной эволюции, чем любая существующая централизованная база данных.

(II) Операционные вызовы

Управление

Технологии РБД могут снизить операционные риски благодаря исключению дублирования информационных потоков и сохранения единого неизменяемого источника данных, записанных в хронологической последовательности. Тем не менее, если ошибка происходит, ее сложно отследить или исправить.

Кроме этого, как было отмечено в разделе про масштабируемость, операционные риски, уникальные для РБД, требующей специальных разрешений, включают в себя управление и устойчивость сети. *Ноды*, осуществляющие верификацию могут выйти из сети в том случае, если преимущества от валидации транзакций не являются достаточными или если требуемые вычислительные мощности становятся слишком дорогими.

Указанный риск ниже в распределенной базе данных, требующей специальных разрешений, т. к. у управляющего органа имеется контроль над операциями и управлением

146 http://www.wired.com/2014/03/bitcoin-exchange/

147 http://pastebin.com/CcGUBgDG

148 Rivest-Shamir-Adleman (RSA) является одной из первых реализованных на практике криптосистем. Широко используется для обеспечения безопасной передачи данных. В подобных криптосистемамх ключ шифрования является открытым и отличается от ключа дешифрования, который хранится в тайне https://en.wikipedia.org/wiki/RSA_(cryptosystem)

149 Digital Signature Algorithm (DSA) является федеральным стандартом обработки информации для цифровой подписи. Генерация ключа осуществляется в два этапа. На первом этапе выбираются параметры алгоритма, который может совместно использоваться несколькими пользователями. На втором этапе происходит генерация открытого и персонального ключа для каждого пользователя. https://en.wikipedia.org/wiki/Digital_Signature_Algorithm

150 Elliptic curve cryptography (ECC) подход к криптографии открытых ключей, опирающийся на математические структуры эллиптических кривых над конечными полями https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

151 В последние годы ученые в сфере IT и физики также разрабатывают квантовую криптографию для использования квантовых механических свойств для решения криптографических задач https://en.wikipedia.org/wiki/Quantum_cryptography

сетью. В распределенной базе данных, не требующей специальных разрешений, для уменьшения операционных рисков вызываемых любым из *нодов*, управляющий орган должен определить общие правила и принципы управления, в том числе и правила для менеджмента, критерии для участия и правила поведения

Умные контракты

В теории *умные контракты* уменьшают количество человеческих ошибок с помощью автоматизации. Тем не менее, если ошибка происходит, ее становится сложнее исправить т. к. операции связаны друг с другом и встроены в блокчейн, которые к тому же исполняются сами по себе в соответствии с программным кодом прописанном в умном контракте.

Помимо этого, *умные контракты* продемонстрировали другой тип человеческих ошибок: ошибки программирования. Программный код *умного контракта* не обязательно должен точно отражать человеческое намерение подписать контракт и может быть источником операционного риска. См. также п. 5.1(IV) и 5.2 (X) выше.

(III) *Вопросы при осуществлении торгов и расчетов.*

Ниже приведены специфические вопросы, возникающие при внедрении технологии РБД в сферу торгов ценными бумагами и расчетов по ним.

Управление кредитным плечом транзакций.

Транзакция с ценными бумагами связана с обменом актива на деньги. Для достижения полноценных расчетов по модели «поставка против платежа» в рамках сети РБД, как кредитование активом, так и кредитование денежными средствами должно осуществляться одновременно. Если денежные средства не *токенизированы*, необходимо иметь отдельную базу данных по деньгам для расчетов. Это, в свою очередь, сокращает эффективность внедрения технологий, использующих РБД.

Альтернативным решением, рассматриваемым в настоящее время отраслью является использование *расчетных монет* для осуществления транзакций в распределенной сети, требующей специальных разрешений для доступа в нее. *Расчетные монеты* представляют собой *токены*, эмитированные контролирующим или выделенным *нодом (нодами)* для содействия расчетам при отсутствии *токенизированных* денег. *Расчетные монеты* обеспечиваются денежными депозитами, осуществляемыми эмитирующим *нодом (нодами)* доверенной третьей стороне, например, банку-кастодиану в той же сети. Когда участникам распределенной сети, требующей специальных разрешений требуются наличные деньги, они могут обменять свои *расчетные монеты* у доверенной третьей стороны. Существуют различные исследуемые доказательства работоспособности концепции расчетных монет, например *Citicoin* от *Citigroup, SETLcoin* от *Goldman Sachs, Utility Settlement Coin* от *UBS* с партнерами*: BNY Mellon, Deutsche bank, ICAP и Santander.*

Механизм отмены

Одной из наиболее важных особенностей технологий РБД является безотзывность транзакций: после валидации и загрузки в блокчейн, транзакция не может быть модифицирована, отменена и или отозвана. Поскольку ресурсный механизм отсутствует, то контрагент, который осуществил ошибочную транзакцию может модифицировать ее только осуществив обратную транзакцию. Поэтому механизм отмены требует дальнейшей проработки. См. п. 5.1 (IV) выше.

Неттинг

Программа поддержки РБД записывает и рассылает информацию о каждой транзакции в общей группе ее участников без взаимозачета и неттинга. Это механизм расходится со стандартной практикой на рынке ценных бумаг для определенных продуктов, таких как деривативы, маржинальные и обеспечительные требования к которым проходят неттинг. Отсутствие неттинга приводит к увеличению требований к обеспечительному и операционному капиталу. Тем не менее, в настоящее время предпринимаются попытки со стороны финансовых институтов по внедрению неттинга в РБД.

Прозрачность

Технологии РБД позволяет раскрывать некоторые детали транзакции (такие как личность контрагента, баланс денежных средств и активов и тип активов) для целей валидации. Это также не соответствует стандартной рыночной практике, когда подобные данные считаются конфиденциальными. Несмотря на то, что предпринимаются определенные усилия для решения этой проблемы, добавление защиты конфиденциальной информации в блокчейн может негативно повлиять на другие преимущества, в частности, прозрачность.

(IV) Правовые вызовы

Внедрение технологий РБД и *умных контрактов* на рынке ценных бумаг может поднять множество важных юридических вопросов. В том числе, но не ограничиваясь этим, действительность *токенов* в качестве представления права собственности и правовой завершенности *умных контрактов*. См. Также п. 5.1 (IV)

(V) Идентификация клиента и противодействие отмыванию доходов

В РБД, требующих особых разрешений для доступа, есть, как минимум, одно регулирующее лицо, хранящее все записи и информацию обо всех участвующих *нодах*. Поэтому для регуляторов относительно просто отслеживать действия участников такой сети. В РБД, не требующей особых разрешений, обычно невозможно выяснить, кто осуществляет те или иные действия, если не инициирована соответствующая процедура. Также сложно определить, кто может быть лицом, осуществляющим надзор за подобной базой данных, т. к. она состоит из *нодов*, которые могут находится в разных юрисдикциях.

Рисунок 14: Визуализация проблемных вопросов развития технологий РБД.

5.5. Актуальность регулирования/ответные действия регулятора

(I) Нод регулятора

Как было отмечено выше, сторонники технологий РБД отмечают, что одним из их преимуществ является то, что регуляторы могут участвовать в качестве одного из *нодов* РБД и, таким образом, получать доступ ко всем данным. Это, в свою очередь, позволит регуляторам иметь более полные, отслеживаемые записи, осуществляемые в реальном времени.

Сами регуляторы, тем не менее, должны оценить, хотят ли они иметь доступ расширенному объему данных, обновляемых в реальном времени, или же им достаточно отчетности. В последнем случае, если регуляторы хотят стать *нодом* в РБД, необходимо разработать в значительной степени автоматизированную функцию мониторинга и осуществить наем экспертов по соответствующим технологиям.

(II) Текущие примеры ответных действий регулятора

Несмотря на то, что технологии РБД находятся на начальном этапе развития, ряд органов власти уже зафиксировали свою точку зрения на них[152].

152 Кроме этого, многие глобальные регуляторы подготовили руководства по рискам, связанным с виртуальной валютой. Некоторые регуляторы подготовили положения, регулирующие Биткойн, например Монетарное агентство в Сингапуре. www.mas.gov.sg/~/media/resource/publications/consult_papers/2016/Proposed%20Activity%20Based%20Payments%20Framework%20and%20Establishment%20of%20a%20National%20Payments%20Council.pdf .

В июне 2016 г. Европейское агентство по рынкам ценных бумаг *European Securities and Markets Authority (ESMA)* опубликовала свою работу, которая включала в себя анализ того, насколько РБД будут (или не будут) соответствовать существующей в ЕС практике регулирования (в основном, по пост-трейдинговым вопросам) для того, чтобы привлечь внимание заинтересованных сторон к ключевым требованиям, которые скорее всего будут предъявлены к организации или группе организаций, использующих РБД. Требования могут быть обусловлены типом ценных бумаг, связанной с этим деятельностью, которую общества планируют осуществлять[153].

В июне 2016 г. французский парламент принял закон, разрешающий эмиссию ваучеров ценных бумаг и их торги в системе РБД (называемой «электронное средство учета и распределенной записи»). Закон утвердил полномочия правительства по разработке положения, которое бы проясняло то, каким образом в отношении указанных ваучеров ценных бумаг и самих ценные бумаги, не прошедшие листинг на торговой площадке и не допущены к обслуживанию в Центральном депозитарии, осуществляется их рыночный оборот с помощью РБД. Это, в свою очередь, приведет формированию регулятивной структуры для технологии распределенных БД.

В январе 2017 г. *FINRA* подготовил документ, который должен был стать вкладом в продолжающийся диалог по использованию технологий РБД в сфере ценных бумаг. Были запрошены комментарии, по вопросам соответствия принципам защиты инвесторов и целостности рынка, основывающимся на применении технологий РБД и их последствиях для правил *FINRA*[154].

Кроме этого, многие регуляторы знакомятся с применением технологий РБД с помощью исследований, исследовательских лабораторий, инновационных кластеров и проектов опытных внедрений их концепций. Кроме этого, международные организации, например, *IOSCO, FSB и BIS* следят за развитием технологий РБД в соответствии со своими целями.

153 www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies

154 Доклад FINRA Доклад по технологии распределенных баз данных: внедрение технологии блокчейн в сфере ценных бумаг (Report on Distributed Ledger Technology: Implications of Blockchain for the Securities Industry), январь 2017, http://www.finra.org/industry/report-distributed-ledger-technology-implications-blockchain-securities-industry