НАЦИОНАЛЬНЫЙ РАСЧЕТНЫЙ ДЕПОЗИТАРИЙ
ГРУППА МОСКОВСКАЯ БИРЖА

РЕАЛИЗАЦИЯ БЛОКЧЕЙН-ЭКОСИСТЕМ В ФИНАНСОВОЙ ИНФРАСТРУКТУРЕ РЫНКА: ОГРАНИЧЕНИЯ И ВОЗМОЖНОСТИ

Whitepaper | 2019

ВВЕДЕНИЕ

Национальный расчетный депозитарий (НРД) открыл собственную блокчейн-лабораторию в 2015 году. За это время был накоплен значительный опыт применения технологии распределенных реестров, включая практическое применение для работы в рамках текущих бизнес-процессов финансовой инфраструктуры России. В лаборатории реализовано несколько промышленных решений, таких как выпуски облигаций, распределенный цифровой депозитарий и сделки трехстороннего РЕПО. Сегодня на базе блокчейн-лаборатории НРД ведется анализ технологических возможностей: стресс-тестирование различных конфигураций распределенного реестра, использование доказательств с нулевым разглашением, применение различных схем токенизации. Рабочая группа, созданная НРД в рамках Международной ассоциации по вопросам обслуживания ценных бумаг (ISSA) и при участии крупнейших международных центральных депозитариев, представила целую серию рекомендаций и отчетов по работе с блокчейн для гармонизации требований, способствующих решению отраслевых задач.

Блокчейн пережил пик популярности, связанный со стремительным взлетом спроса на криптовалюты, проведением множества ICO с выпуском новых токенов в "серой зоне" правового поля, прошел первые проверки заявленных свойств в рамках пилотных сделок в корпоративной среде, попыток взлома блокчейн-сетей, кошельков и площадок, обеспечивающих обмен токенов, а также расследований в различных юрисдикциях и стремится занять свое место в рамках многообразия технологий, которые могут быть использованы в корпоративных и глобальных системах. Использование данной технологии позволяет перейти от передачи данных о перемещениях активов к непосредственной передаче активов с использованием криптографии, а также адаптировать финансовую инфраструктуру к работе с новыми типами активов, требующими более гибких подходов и фокусирования на технологической составляющей сервиса. Участники финансового рынка разрабатывают собственные решения на базе технологии распределенных реестров, а также активно принимают участие в работе консорциумов и проводят пилотные запуски проектов на различных блокчейн-платформах, чтобы определить на практике возможности, которые может предоставить технология блокчейн.

В этом документе мы обобщим результаты, полученные в рамках нашей работы, и представим описание возможных путей успешного внедрения блокчейн в отрасли в ближайшей перспективе. Особое внимание будет уделено методологии выбора распределенного реестра в качестве одного из вариантов архитектурного решения, а также техническим аспектам: обеспечению конфиденциальности в рамках работы сети, масштабируемости решений, а также вопросам, связанным со структурами управления блокчейн-сетями.

Что такое блокчейн?

Блокчейн (англ. blockchain, изначально block chain) — выстроенная по определенным правилам непрерывная последовательная цепочка блоков, содержащих информацию, и связанная криптографическими алгоритмами [1]. Каждый из блоков состоит из идентификатора, криптографически защищенной ссылки на предыдущий блок и набора данных. Первые шаги по созданию концепции цепочек блоков данных, связанных криптографическими механизмами в электронной базе данных, была предложена в 1991 году — это был механизм создания сертификатов, защищающих от подделки временные метки, встроенные в электронные документы [4]. Через год данная концепция была дополнена использованием деревьев Меркле [2,3], что позволило собирать несколько сертификатов документов в один блок [6].

Первая полноценная концепция блокчейн-системы была предложена в 2008 году [8]. Архитектура системы была дополнена использованием алгоритма добавления блоков в цепочку, который базируется на идее HashCash и не требует наличия подписей доверенного лица [7].

Первый публичный блокчейн был запущен в 2009 году, а выпущенный с его помощью нативный токен — биткоин — стал самым популярным нативным активом с использованием криптографии и идеологии блокчейн.

КЛАССИФИКАЦИЯ ИМЕЮЩИХСЯ ПРОБЛЕМ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

БЕЗОПАСНОСТЬ

Для финансовой инфраструктуры вопрос обеспечения безопасности является критическим. Технология должна обеспечивать максимальный уровень защиты самих активов, а также предоставлять механизмы предотвращения несанкционированного доступа к данным. Также актуальным является вопрос идентификации участника сети.

История развития финансовой инфраструктуры убедительно доказала необходимость разделения функций при работе с финансовыми инструментами: хранение, расчеты, клиринг и функционал заключения сделок (торговли). Тем не менее, при создании торговых площадок по обмену нативных токенов (криптовалют) даный опыт не был учтен, что привело к кражам непосредственно с централизованных площадок (2011-2019 гг.) более 6,5% общего объема первой глобальной криптовалюты — биткоина [25]. Реализованные торговые площадки с определенным уровнем децентрализации на текущий момент не демонстируют большого объема торговли по сравнению с централизованными решениями и занимают менее 1% общего объема торгов, что может быть обусловлено как нестабильностью их работы и высокими рисками манипуляций [26], так и проблемами идентификации участников в полностью распределенной открытой архитектуре сети [27].

Анализ взломов систем, работающих с активами, хранящимися и эмитированными непосредственно в блокчейн, показывает, что подавляющее большинство успешных атак происходит не через криптографические схемы и ставит целью получение доступа к закрытым ключам кошельков, на которых осуществляется хранение, и скорейший вывод средств. В качестве защиты от такого риска используются мультиподписи, аппаратные защищенные средства хранения ключей (HSM), а также программные криптографические решения для защиты от несанкционированного доступа к ключам.

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ

Обеспечение конфиденциальности данных не было целью при создании первых блокчейн-платформ. Это привело к появлению термина "псевдоанонимность" по отношению к некоторым блокчейн-платформам и позволило раскрывать владельцев приватных ключей, а также применять к ним различные методы влияния, предоставлять контроль над этими ключами и осуществлять передачу активов под управлением данных ключей [28].

Использование различных криптографических механизмов анонимизации (применение доказательств с нулевым разглашением и протоколов обеспечения конфиденциальности транзакций, реализация различных миксеров наборов транзакций) ограничивается трилемой масштабируемости [12, 36] — все реализации требуют серьезных вычислительных мощностей, передачи и хранения больших объемов данных. Несмотря на развитие фундаментальной и прикладной криптографии, технологических блокчейн-решений, обладающих необходимым набором свойств для внедрения в финансовой инфраструктуре, пока нет [29, 30]:

- технологии смешивания транзакций в общие пулы (миксеры) являются централизованными решениями с ограниченной анонимностью;
- применение кольцевых подписей приводит к проблемам масштабируемости из-за кратного увеличения размера данных в транзакции, требует алгоритмически сложной верификации;
- использование доказательств с нулевым разглашением требует серьезных вычислительных мощностей и наличия доверенных участников для инициализации сети, использует новые нестандартизированные криптографические примитивы;

- алгоритм конфиденциальных транзакций (протокол Mimblewimle) требует взаимодействия между получателем и отправителем, оставляет возможность мониторинга активности и не разрывает связи между транзакциями.

Текущий уровень развития прикладной криптографии и степень проработки технологических реализаций не позволяет рекомендовать использование той или иной технологии для обеспечения конфиденциальности в распределенных реестрах. Для обеспечения необходимого уровня конфиденциальности предлагается использование ограничений доступа к блокчейн-сети по аналогии с централизованными и облачными решениями, по типу роли и каналов подключения, а также проверенных в отрасли методов криптографии. Для повышения уровня безопасности блокчейн-решений, предлагаемых на рынке при работе с нативными токенами (криптовалютами), необходимо развитие регулирования и снижение рисков потери контроля над активами, хранящимися в виде токенов, в процессе хранения и торговли в соответствии с практиками, принятыми в традиционных финансовых институтах.

ВЗАИМОДЕЙСТВИЕ МЕЖДУ НЕСКОЛЬКИМИ БЛОКЧЕЙН-ПЛАТФОРМАМИ

Интеграция нескольких блокчейн-платформ является сложной задачей по ряду причин: различия в консенсусах, наличие/отсутствие в конкретной реализации возможности использовать мультиподписи или смарт-контракты и т.д. Также стоит отметить отсутствие спроса на интеграцию со стороны промышленности в силу малого количества внедрённых блокчейн-решений и необходимости их интеграции с централизованными системами.

К примеру, распределенная P2P-архитектура подразумевает отсутствие единой точки интеграции, часть платформ не обладает необходимым функционалом, также существуют сложности с использованием идентификации участников сети и наборов данных из одного блокчейн внутри другого и т.д.

В общем случае существуют три логические схемы интеграции [50]:

1. Нотариальная схема: использование набора участников, осуществляющих мониторинг стороннего блокчейн А и "нотариально" заверяющих действия в блокчейн Б, куда переносятся данные. В этом случае необходимо наличие выделенного блокчейн В для управления участниками нотариальной схемы (может совпадать с А или Б).
2. Схемы ретрансляции: с использованием смарт-контрактов или мультиподписи. Смарт-контракт или иной механизм блокчейн А может отслеживать и воздействовать на состояние блокчейна Б. В этом случае нет необходимости в выделенном блокчейне, как в предыдущем случае, но один из блокчейнов (А или Б) назначается ведущим. Существует две схемы ретрансляции:
    - Односторонняя схема ретрансляции, которая реализует связь только в одну сторону [51].
    - Двухсторонняя схема ретрансляции, которая реализует связь в обе стороны [55].
3. Блокировка с использованием хэш-функций. Блокчейн А и блокчейн В отслеживают одну и ту же хеш-функцию. В отличие от схемы ретрансляции здесь нет необходимости в функции ведущего — достаточно только обмена хешами. В этом случае минимизируется объем передаваемой информации, необходимой для интеграции.

В рамках задачи интеграции нескольких блокчейн-платформ могут быть реализованы следующие сценарии работы с токенами:

1. Передача токена из блокчейна А в блокчейн В и обратно.
2. Атомарный обмен. Механизм обеспечения гарантированного обмена токенами между двумя сторонами.
3. Мультиблокчейн-оракулы. Блокчейн В отслеживает с помощью смарт-контракта или иного механизма события в блокчейне А и выполняет определенное действие, если событие случается.
4. Мультиблокчейн блокировка токена. Токен заблокирован в блокчейн А, и разблокировка может произойти при определенном событии в блокчейн Б.

В результате сравнения возможных сценариев использования и механизмов реализации получается, что [53]:

- блокировка с использованием хэш-функций может использоваться только для атомарного обмена;

- односторонняя схема ретрансляции может использоваться для всех сценариев, кроме атомарного обмена;
- нотариальная схема и двухсторонняя схема ретрансляции могут быть использованы для всех четырех сценариев;
- при использовании блокировок с помощью хэш-функций общий объем эмитированных токенов в каждом из блокчейн остается неизменным, а при нотариальной схеме или ретрансляции вся работа с токеном может быть передана целиком из одного блокчейн в другой [52].

Применение механизмов интеграции между несколькими блокчейн-платформами в промышленных решениях в данный момент невозможно из-за ограничений их масштабируемости и малого опыта эксплуатации технологий. Тем не менее, стоит отметить несколько проектов, которые помогут наладить взаимодействие конкретных блокчейн-платформ в частном случае:

1. Реализацию двухсторонней схемы ретрансляции для двух выделенных блокчейн-сетей Dogethereum [56];
2. Реализацию протокола Interledger, осуществляющую атомарный обмен [57];
3. Проекты Cosmos [54] и PolkaDot [58], реализующие нотариальную схему работы с применением нативного токена для множества блокчейн-сетей. Эти технологии могут быть использованы преимущественно для закрытых (Cosmos) и открытых (PolkaDot) блокчейн-сетей, являющиеся отдельными блокчейн-платформами.

Текущие интеграционные проекты могут в ближайшей перспективе стать основой появления работающих решений.

ОТКРЫТЫЕ И ЗАКРЫТЫЕ БЛОКЧЕЙН-СЕТИ

Открытые блокчейн-сети с неограниченным числом анонимных участников не имеют структуры управления и идентификации пользователей и узлов сети. Соответственно, невозможно проведение процедур проверки AML/KYC непосредственно внутри блокчейн-платформы без привлечения стороннего сервиса.

Узлы таких сетей могут быть расположены в любой части мира, весь код и протоколы являются открытыми, и все данные доступны для верификации. Управление такой сетью осуществляется на основе консенсуса, и ни одно юридическое или физическое лицо не несет ответственности за функционал или данные, хранящиеся таким способом.

Данные сети обладают следующими свойствами:

- использование для изменения данных вероятностного консенсуса в большинстве случаев не гарантирует финальность расчетов с помощью такой сети из-за наличия различных версий набора данных в каждый конкретный момент времени и вероятностного механизма выбора единственной итоговой версии данных [8];
- непредвиденное поведение сети, связанное с внутренней активностью и внесением изменений в технологическую платформу;
- ограничения производительности и масштабируемости сети;
- возможна косвенная связь платформы, используемой сетью, с конкретным юридическим или физическим лицом, отвечающим за разработку и стабилизацию технологии и имеющим влияние на возможность эксплуатации данной платформы;
- возможна реализация механизмов анонимизации участников сети и сокрытия данных/самого факта проведения транзакций с помощью криптографических конструкций.

Закрытые блокчейн-сети с ограниченным числом идентифицированных узлов подразумевают наличие оператора, управляющего конкретной сетью, идентификацию и возможные ограничения для участников сети. Тем не менее, возможна как реализация централизованного механизма принятия решений внутри сети, так и децентрализованное управление сетью. Оператор может представлять интересы одного из участников (вертикальная модель) или реализовать идею совместного управления с помощью консорциума участников. С точки зрения обеспечения конфиденциальности данных в таких сетях возможно разделение прав доступа на конкретные объекты, аналогичное традиционным системам.

Данные сети обладают следующими свойствами:

- возможность гарантировать финальность расчетов с помощью детерминированного консенсуса;
- стабильное предсказуемое поведение сети;
- возможность оптимизации структуры сети в соответствии с требованиями производительности и масштабируемости;
- возможность ограничения доступа к данным с помощью встроенных механизмов;
- зависимость от оператора сети;
- возможна реализация механизмов анонимизации участников сети и сокрытия данных/самого факта проведения транзакций между участниками сети с помощью криптографических конструкций.

Участники финансовой инфраструктуры также описали гибридный вариант с эксплуатацией управляемой закрытой блокчейн-сети, интегрированной во множество открытых блокчейн-сетей [41]. При использовании закрытых блокчейн-сетей также наблюдается почти полное отсутствие "горизонтальных" решений, объединяющих в виде консорциума участников-пользователей с равными правами из нескольких юрисдикций. На рынке доминируют пилотные "вертикальные" проекты, ограниченные юридическими рамками, контролируемые конкретным владельцем и решающие его задачи (в том числе и по монетизации). В противоположность этому, в открытых блокчейн-сетях чаще всего невозможно выявить конкретного владельца технологии, контролирующий орган или сообщество, и это существенно снижает интерес со стороны регулятора и заставляет пересматривать имеющиеся нормы для адаптации к появлению нативных токенов, встроенных в технологию в рамках концепции Web 3.0 [59].

ПРОИЗВОДИТЕЛЬНОСТЬ И МАСШТАБИРУЕМОСТЬ

Данная проблема была сформулирована в форме трилеммы масштабируемости [12, 36].

Блокчейн-решение может удовлетворять не более чем двум из трех свойств:

1. Децентрализованная архитектура (система, способная работать в сценарии, в котором каждый участник имеет доступ только к ресурсам O (c*), то есть к обычной рабочей станции или терминалу).
2. Масштабируемость (определяется как способность обрабатывать транзакции O (n**)> O (c)).
3. Обеспечение конфиденциальности данных (определяется как защита от злоумышленников с использованием ресурсов O (n)).

Первые открытые блокчейн-платформы обладали большими ограничениями производительности, связанными с существенными вычислительными и коммуникационными расходами, которые определялись консенсусом proof-of-work и недетерминированной архитектурой публичной сети. В результате срок ожидания принятия транзакции первыми блокчейн-сетями мог составлять минуты, часы и даже дни в случае разного рода отклонений от нормальной работы. Скорость обработки транзакций постепенно росла от 7 транзакций в секунду в Биткоин и 14 транзакций в секунду в Эфириум до более чем 1000 транзакций в секунду в Stellar, BitShares и Waves, использующих proof-of-stake консенсус [35]. Более поздние реализации публичных блокчейн-платформ применяют механизм шардинга, двухслойные блокчейн-архитектуры и перенос части функционала во внешние по отношению к основной блокчейн-сети блоки и иные способы ускорения, позволяющие рассчитывать на еще большую производительность сети [39, 40].

Закрытые блокчейн-платформы используют детерминированные модели консенсуса (чаще всего базирующиеся на PBFT [37]) и позволяют достичь еще большей производительности — до 20 000 транзакций в секунду [38].

---

* c — размер вычислительных ресурсов (включая непосредственно вычисления, пропускную способность и объем хранимых данных), доступный каждому узлу.

** n — размер экосистемы в обобщенном виде: объем нагрузки сети, объем данных и рыночная капитализация этих данных пропорциональны n.

Некоторые из представителей финансовой инфраструктуры уже предлагают реализацию гибридной модели, которые эксплуатируют более одной блокчейн-платформы в своей работе. Наиболее распространенная версия — использование быстрой приватной блокчейн-платформы с детерминированным консенсусом для работы с открытыми платформами, содержащими нативные токены, тем самым обеспечивая финальность расчетов и нужный уровень конфиденциальности [41].

Таким образом, производительность и масштабируемость рыночных решений позволяет реализовать стоящие перед финансовой инфраструктурой задачи без видимых технических ограничений со скоростью работы более 1000 транзакций в секунду, и дает возможность распространять наиболее успешные проекты с помощью шардинга и гибридных технологий.

СТАНДАРТИЗАЦИЯ ТРЕБОВАНИЙ К БЛОКЧЕЙН-СЕТЯМ

Вопрос стандартизации функциональных и нефункциональных требований к работе с блокчейн-платформами — критически важен для внедрения решений на основе распределенных реестров.

НРД в 2016 году инициировал создание рабочей группы участников финансовой инфраструктуры по работе с блокчейн на базе Международной ассоциации по вопросам обслуживания ценных бумаг (ISSA). Рабочая группа совместно с мировыми экспертами выпустила следующие отчеты:

1. Инфраструктура для криптоактивов с точки зрения финансовой инфраструктуры [42].
2. Технология распределенного реестра — общеотраслевые принципы использования [43].
3. Голосование на общем собрании владельцев ценных бумаг на технологии распределенных реестров. Требования к продукту [44].
4. Таблица использования сообщений ISO20022 при голосованиях на общем собрании владельцев ценных бумаг [45].

Наличие открытого стандарта финансовых сообщений ISO20022 и единой глобальной системы идентификации участников финансового рынка позволяет значительно упростить взаимодействие между традиционными системами и блокчейн [46].

В рамках международной организации по стандартам (ISO) создан комитет, отвечающий за стандартизацию блокчейн и технологии распределенных реестров [47]. Несколько глобальных консорциумов объединяют участников финансового рынка, вендоров решений и представителей иных областей под эгидой создания и внедрения блокчейн-платформ с открытым исходным кодом [48, 49].

Текущий уровень стандартизации показывает, что участникам рынка предстоит большая работа в области снижения стоимости внедрения и поддержки блокчейн-платформ в промышленной эксплуатации. Для этих целей создано достаточное количество глобальных и отраслевых органов и результаты их работы можно ожидать в краткосрочной и среднесрочной перспективе.

УПРАВЛЕНИЕ БЛОКЧЕЙН-СЕТЬЮ

К блокчейн-решениям, используемым в рамках финансовой инфраструктуры, должны применяться требования к непрерывности, надежности и уровню технической поддержки, аналогичные требованиям для традиционных систем. НРД гарантирует реализацию этих требований с помощью выделенного оператора блокчейн-сети (выбранного консорциумом участников сети или инициирующего создание и эксплуатирующего определенную блокчейн-сеть).

Основные задачи оператора:

1. Обеспечение надежности и безопасности платформы.
2. Фиксация и применение единых правил использования, позволяющих признавать юридическую значимость контента платформы, контроль их соблюдения участниками.
3. Технологическое развитие платформы и дополнение функциональных возможностей.
4. Масштабирование.

Требования, предъявляемые к оператору:

1. Нейтральность по отношению к развернутым на платформе бизнес-сервисам и операциям участников.
2. Устойчивость, самодостаточность, далекий горизонт и прозрачная стратегия развития бизнеса.
3. Высокий уровень непрерывности бизнеса, кибербезопасности, корпоративного управления.
4. Финансовая ответственность за ненадлежащее исполнение своих функций.

ТОКЕНИЗАЦИЯ ДЕНЕЖНЫХ СРЕДСТВ

Платежные функции финансовой инфраструктуры целесообразно реализовать непосредственно на блокчейн в виде системы расчетов в режиме реального времени (RTGS) [60] или применения иных моделей расчетов. Этот функционал требует наличия внутри блокчейн денежных средств и, соответственно, классифицирован в рамках рабочей группы ISSA по способу их эмиссии:

СПОСОБ ЭМИССИИ	СТЕПЕНЬ РИСКА, ОТ 1 ДО 5	ЭМИТЕНТЫ	ХРАНИТЕЛИ ЗАЛОГА	ПРИМЕРЫ
Цифровая валюта центрального банка (ЦВЦБ)	1	Центральные банки	Центральные банки	Цифровая валюта в Китае [16], E-Krona в Швеции [13]; Проект Inthanon в Таиланде [14]; Eastern Caribbean Central Bank; Central Bank of Uruguay [15]
Токен, гарантируемый денежными средствами, хранящимися на счетах резервов в центральном банке, и гарантируемый центральным банком	2	Центральные депозитарии и/или объединения коммерческих банков	Центральные банки	Цифровой сингапурский доллар и возможность использования токенов, эмитированных несколькими центральными банками (проект Ubin при участии Банка Англии и Банка Канады) [17]; Проект Stella Европейского Центрального Банка и Банка Японии [18]
Токен, выпущенный для денежных средств, которые хранятся на общем резервном счете центрального банка и не содержат гарантии центрального банка	3	Центральные депозитарии и/или объединения коммерческих банков	Центральные банки	Проект Fnality, финансируемый 14 банками, ранее известный как Utility Settlement Coin (USC) [19]
Токен, выпущенный на основе денежных вкладов в коммерческом банке	4	Коммерческие банки	Коммерческие банки	Signet Coin банка Signature [20]; Проект JPM Coin банка J.P. Morgan [21]
Токен, выпущенный организациями, не обладающими банковской лицензией	5	В основном, трастовые фонды криптовалютных торговых площадок	Коммерческие банки	Gemini Dollar от площадки по обмену криптовалют Gemini [22]; Paxos Standard (PAX) от компании Paxos [23]; Huobi HUSD от площадки по обмену криптовалют Huobi [24] и USD Coin от компаний Circle и Coinbase [24]

Текущая модель распределения рисков внутри финансовой инфраструктуры, а также законодательные ограничения исключают возможность работы с токенами, выпущенными организациями, которые не обладают банковской лицензией или нативными технологическими токенами, и вынуждает участников рынка, использующих данные решения, работать в ограниченном наборе юрисдикций.

Использование токенов, выпущенных на основе денежных вкладов в коммерческом банке, полностью контролируется конкретным юридическим лицом и влечет за собой риски в связи с отсутствием контроля регулятора. Наиболее перспективными в рамках деятельности центральных депозитариев кажутся первые три модели, обладающие наименьшими рисками и контролируемые регулятором.

Удачным примером использования блокчейн является план по реализации цифровой валюты, анонсированный Народным банком Китая. Планируется эмиссия со 100% обеспечением в виде токенизированных наличных. Для использования этого платежного средства не нужно будет открывать банковский счет, но может потребоваться пройти KYC-идентификацию.

С технической точки зрения механизм распределения цифровой валюты будет двухуровневым:

- между центральным банком и коммерческими банками;
- между коммерческими банками и частными лицами и предприятиями.

Декларируются следующие преимущества данной модели:

1. Возможность более точного расчета некоторых показателей, таких как уровень инфляции и другие макроэкономические показатели.
2. Расширение возможностей сбора данных в режиме реального времени, таких как создание, ведение бухгалтерского учета и обращение денег, что обеспечит предоставление полезной информации для лиц, определяющих денежно-кредитную политику.
3. Содействие предотвращению отмывания денег, финансирования терроризма и уклонения от уплаты налогов.
4. Интернационализация использования национальной валюты — юаня.
5. Снижение информационной асимметрии между финансовыми институтами и регулирующими органами.
6. Снижение затрат на выпуск наличной денежной массы (печать и чеканку).

Таким образом, Народный банк Китая потенциально может получить контроль над социально-экономической деятельностью в стране с помощью такой реализации цифровых денег. Также стоит отметить, что предлагаемая схема реализации не может быть прямым конкурентом существующих криптовалют, таких как биткойн или эфир, в силу централизованности эмиссии и отсутствия конфиденциальности при использовании.

ОПЫТ ИСПОЛЬЗОВАНИЯ

Промышленные внедрения блокчейн-сетей в финансовой инфраструктуре не стали популярны в первые годы появления технологии. В 2018 году было опубликовано несколько отчетов, указывающих что:

1. 1% опрошенных ИТ-директоров организаций указали на возможность внедрения блокчейна в процессы своих организаций [10].
2. 8% опрошенных ИТ-директоров организаций планировали активные эксперименты с блокчейном или его изучение [10].
3. Только 4% из 398 известных блокчейн-проектов на предприятиях были полноценно внедрены [11].

С 2015 года в НРД накоплен большой опыт реализации блокчейн-решений для финансовой инфраструктуры:

1. Решение для автоматизации голосования на собраниях владельцев ценных бумаг.
2. Два пилотных выпуска коммерческих облигаций с использованием смарт-контрактов.
3. Пилотное проведение внебиржевой трехсторонней сделки РЕПО.
4. Тестовая сделка по привлечению финансирования путем выпуска токенов на блокчейн.
5. Участие в проекте распределенного цифрового депозитария.
6. Активное участие в международных рабочих группах ISSA, Hyperledger.
7. Консультирование сторонних проектов, работающих с токенизированными активами.

После реализации серии пилотных сделок НРД переходит к промышленному внедрению технологии и участию в создании нормативно-правовой базы для последующего применения в имеющихся и создаваемых бизнес-линиях. В рамках этой деятельности блокчейн-решения рассматриваются с трех точек зрения:

- экономическая эффективность;

- возможность предоставления традиционных сервисов по работе с новыми видами активами;
- возможность предоставления новых сервисов по работе с традиционными видами активов.

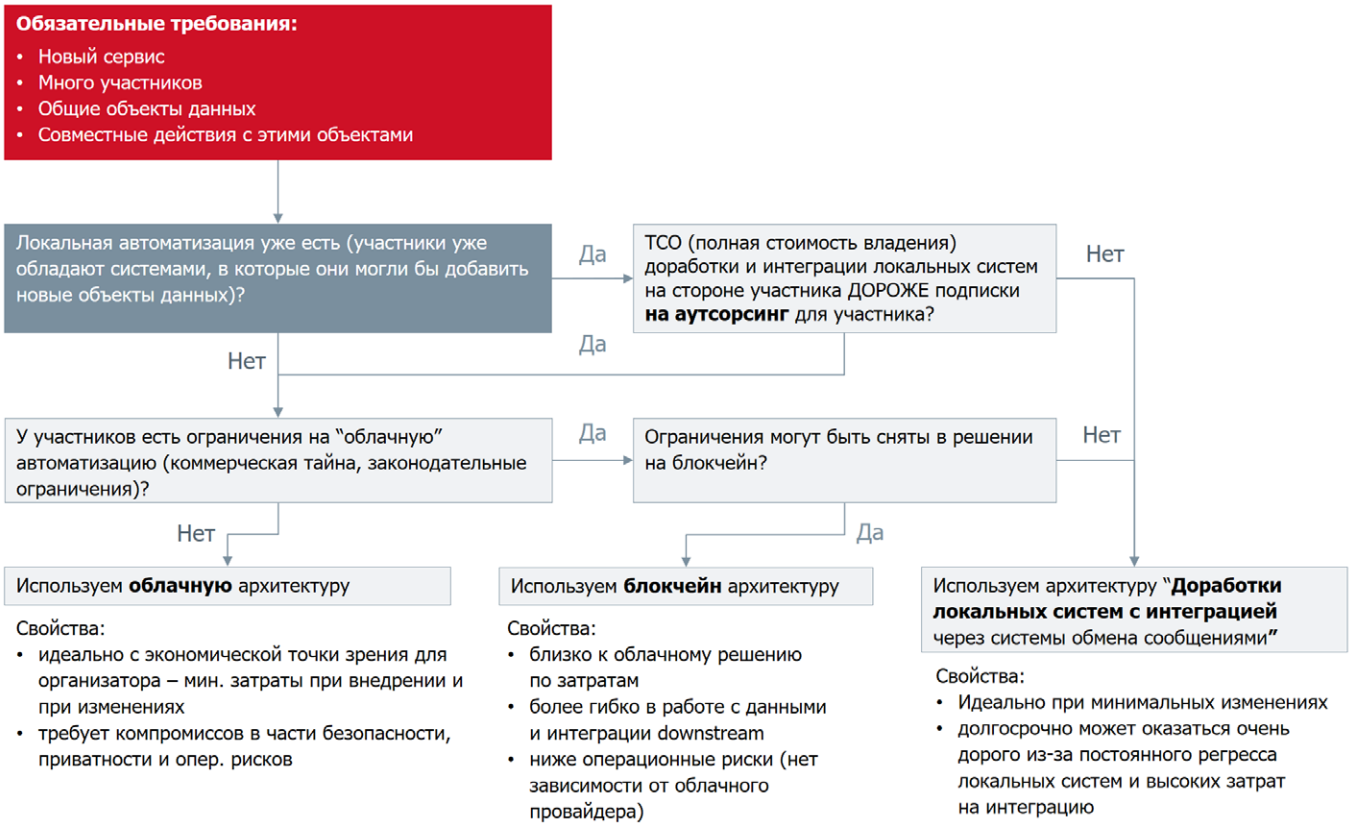
БОЛЕЕ ПОДРОБНО О КАЖДОЙ ИЗ ОЦЕНОК:

Оценка экономической эффективности применения блокчейна

Ключевым фактором при рассмотрении вопроса внедрения новых технологий в бизнесе является существенное снижение затрат организации в сравнении с существующими возможностями реализации процессов. В результате анализа опыта применения блокчейн-решений было выявлено, что существует возможность экономии при использовании данной технологии в сравнении с централизованными или облачными решениями для создания новых систем со множеством участников (вне зависимости от области применения — финансовая инфраструктура или, например, логистика):

- совместное финансирование создания и поддержки системы с распределенной архитектурой;
- сокращение капитальных затрат за счет их распределения между участниками сети и совместного использования компонент системы.

Предлагаемый способ анализа экономической эффективности приведен на диаграмме:



Возможность предоставления традиционных сервисов по работе с новыми видами активов

Существующие сейчас и наиболее популярные технологические решения на базе открытых блокчейн-платформ — нативные токены. Институциональные инвесторы не готовы брать на себя риски, связанные с потерей контроля над такими активами при хранении и торговле, и испытывают потребность в услугах хранения и расчетов со стороны традиционной финансовой инфраструктуры. Регуляторы, в свою очередь, предъявляют определенные требования к идентификации владельцев такого рода активов и контролю расчетов по сделкам с ними с точки зрения AML, в соответствии с глобальными тенденциями контроля над финансовыми потоками во всех юрисдикциях.

Следовательно, существует возможность удовлетворения этого спроса имеющимися финансовыми институтами, согласно требованиям регуляторов и условиями оказания услуг для токенизированных активов, включая выпуск новых токенов, обслуживание имеющихся (включая хранение и расчеты) и предоставление различных сервисов на их базе (аналоги корпоративных действий или иные). Решения для такого рода сервисов могут быть централизованными, децентрализованными и гибридными.

Развитие концепции Web 3.0 или "интернета данных" [62] подразумевает как создание децентрализованной P2P-системы управления следующим поколением интернета, так и создание множества нативных платежных и инвестиционных инструментов с децентрализованным управлением для реализации данной концепции и их интеграцию с "интернетом вещей" [63, 64, 65]. Также по-прежнему актуален сервис микроплатежей, на который была первоначально ориентирована сеть биткойн [8]. Это дает возможность создания сервисов для такого рода активов в долгосрочной перспективе.

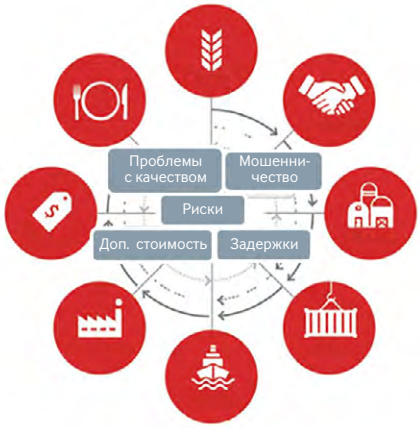
Товарные рынки и блокчейн

Товарные рынки традиционно считаются более консервативными с технологической точки зрения. Тем не менее, использование блокчейн для автоматизации в этой сфере рассматривается как одна из возможностей для упрощения имеющихся на данный момент бизнес-процессов от работы с аккредитивами и использования единого документооборота до расчетов по сделкам и создания производных инструментов непосредственно в распределённом реестре [67]. В случае объединения торговли и управления цепочками поставок в единую экосистему появляются дополнительные преимущества — прозрачность всего процесса работы с товаром, новый уровень борьбы с фальсификациями различного рода и наличие единого источника данных по сделкам и передвижению товара. Примерами таких рынков являются торговля электроэнергией и сельхозпродукцией [67].

Аналогично может быть реализована торговля электроэнергией, не имеющая проблем большой номенклатуры товара или вариативности логистики.

В силу того, что отрасль является одной из старейших и имеет сложившуюся инфраструктуру распределения рисков, наиболее вероятно постепенное проникновение блокчейна в торговлю товарами — от появления P2P-маркетплейсов, выделения конкретных бизнес-процессов в блокчейн (работа с аккредитивами, товарными расписками) к реализации глобальных блокчейн-экосистем, реализующих не только полный цикл внебиржевой и биржевой торговли различными товарными позициями и деривативами, но и интегрированный с распределенным управлением цепочками поставок [68], факторингом [70], страховыми сервисами, локальными налоговыми системами и контролирующими органами [66].

Первые шаги в этом направлении уже реализуются консорциумами международных банковских групп и лидерами международной торговли различными товарами [69], что наглядно доказывает жизнеспособность модели распределения стоимости разработки и внедрения такого рода систем между всеми участниками и необходимость блокчейн-решения преимущественно в случае участия в проекте множества сторон, не обладающих единым набором стандартизированных систем.



НЕВОЗМОЖНОСТЬ ПОДДЕЛКИ
информации — криптографическая защита

ПРОЗРАЧНОСТЬ
за счет единого пространства учета сделок и привязки документов

ЕДИНЫЙ ИСТОЧНИК ДАННЫХ
все участники реестра получают одни данные

Возможность предоставления новых сервисов по работе с традиционными видами активов

В мире существует множество пилотных решений для работы с токенизированными традиционными активами, созданных сторонними компаниями-разработчиками по заказу частных компаний или непосредственно самими компаниями. Тем не менее, большая их часть так и остается на стадии «пилота» и не выходит на стадию промышленной эксплуатации [10,11]. Одна из причин — отсутствие явных преимуществ и подтвержденного спроса на использование данной технологии со стороны бизнеса, государства или регулятора.

Необходимым условием успеха является наличие подтвержденного спроса хотя бы от одной из сторон. Основанием для этого спроса может быть:

- повышение прозрачности сделок;
- невозможность подделки реестра;
- отсутствие необходимости реконсиляции при использовании множества систем;
- упрощение бизнес-процесса за счет единого документооборота, интегрированного с расчетной системой;
- экономия за счет отсутствия необходимости многократного дублирования данных для обеспечения непрерывности бизнеса;
- дополнительное доверие инвестора к распределенной системе управления активами;
- упрощение применения различных моделей расчетов за счет использования умных контрактов;
- создание нового инструмента финансирования для большого числа розничных инвесторов (к которому не приспособлена текущая инфраструктура).

Также необходима проверка следующих факторов:

- Является ли токенизируемый инструмент достаточно ликвидным?
- Требуется ли использование открытой или закрытой блокчейн-сети?
- Кто будет осуществлять эмиссию этого инструмента в блокчейн?
- Каким образом будет осуществляться управление этой блокчейн-сетью?
- Каким образом будут окупаться затраты на создание блокчейн-решения?

В случае подтверждения спроса и наличия определенности с факторами, перечисленными выше, появляется основание для выбора блокчейн в качестве способа реализации бизнес-требований к предоставлению новых сервисов. Само появление блокчейн, также как и появление интернета, может предоставить возможности для реализации новых сервисов, внедрение которых невозможно с применением традиционной архитектуры.

Decentralized Digital Depository

Глобальная распределенная система управления счетами предоставляет следующие преимущества:

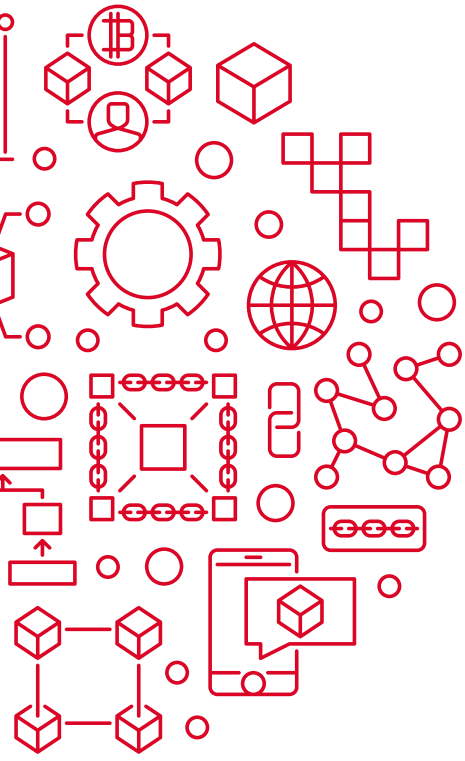
1. Единая глобальная система управления счетами на блокчейне вместо локальных систем в каждом центральном депозитарии или банке.
2. Сам владелец счета (физическое или юридическое лицо) владеет и управляет счетом, а также выбирает банк, предоставляющий ему сервисы для этого счета —- не нужно менять реквизиты при переходе из банка в банк.
   То же самое верно при смене юрисдикции счета.
3. В случае банкротства банка в распределенном реестре остается полный набор данных об остатках в этом банке — владелец может получить доступ к своему счету, пройдя идентификацию у другого участника финансовой инфраструктуры.
4. В случае дефолта финансовой инфраструктуры в конкретной юрисдикции иностранные инвесторы могут получить доступ к управлению активами через другого партнера в другой юрисдикции.

ВЫВОДЫ

Блокчейн, несомненно, одна из перспективных технологий реализации проектов для инфраструктуры финансового рынка, но он остается альтернативным способом работы с данными наряду с централизованными и облачными решениями. Применение технологии распределенных реестров для осуществления функций финансовой инфраструктуры позволяет добиться упрощения процессов по сравнению с использованием нескольких централизованных решений, повышения прозрачности финансового рынка для регулятора, а также обеспечить условия для гибких моделей расчетов непосредственно в блокчейн.

В рамках текущих задач по работе с новыми сервисами и новыми видами активов применение данного решения может быть экономически и логически обосновано по сравнению с иными вариантами реализации. Текущий уровень решений, с точки зрения обеспечения конфиденциальности, требует применения традиционных подходов к работе с данными, достаточного уровня масштабируемости и производительности при работе с распределенными реестрами.

Наличие блокчейн-платформы может упростить внедрение новых моделей расчетов и предоставления на ее базе таких сервисов как, например, факторинг. Наиболее экономически эффективным представляется перенос в блокчейн всего набора бизнес-процессов, связанных с определенным типом актива или сервиса, включение в периметр блокчейна токенизированых денежных средств, а также адаптация финансовой инфраструктуры к работе с новыми типами активов с использованием технологии распределенных реестров.



ЛИТЕРАТУРА

[1] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

[2] US patent 4309569, Ralph Merkle, "Method of providing digital signatures", published Jan 5, 1982, assigned to The Board Of Trustees Of The Leland Stanford Junior University

[3] Merkle R.C. (1988) A Digital Signature Based on a Conventional Encryption Function. In: Pomerance C. (eds) Advances in Cryptology — CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg

[4] Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". Journal of Cryptology. 3 (2): 99–111.

[5] Gartner. Market guide for blockchain consulting and proof-of-concept development services. 2018. https://gtnr.it/2NB9Pp3

[6] Bayer, Dave; Haber, Stuart; Stornetta, W. Scott (March 1992). Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences

[7] "Hashcash - A Denial of Service Counter-Measure" (PDF). hashcash.org. 1 August 2002

[8] Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). bitcoin.org

[9] Project Bletchley Whitepaper Archived 11 January 2017 at the Wayback Machine, Microsoft, 2016-09-19. Retrieved 2016-12-24.

[10] "Hype Killer - Only 1% of Companies Are Using Blockchain, Gartner Reports | Artificial Lawyer". Artificial Lawyer. 4 May 2018. Retrieved 22 May 2018.

[11] https://www.pwc.com/m1/en/services/assurance/documents/accelerating-blockchain.pdf

[12] https://github.com/ethereum/wiki/wiki/Sharding-FAQ

[13] https://www.riksbank.se/en-gb/payments--cash/e-krona/e-krona-reports/e-krona-project-report-2/

[14] https://www.bot.or.th/Thai/PressandSpeeches/Press/News2562/n562e.pdf

[15] https://www.bis.org/publ/bppdf/bispap101.pdf

[16] https://info.binance.com/en/research/marketresearch/CBDC.html?fbclid=IwAR2Y7W5Jw8p0Am1486bwmgwltdJkJV5k-LN8sBg5YHIeP88iBfJ0ovFqnDM

[17] https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf?la=en&hash=F7F232705054CC226297BF396608CA026C3C7139

[18] https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604_1.en.pdf?19a53d7118406fc74c32d7ab2565052d

[19] https://www.fnality.org

[20] https://tassat.com/press-releases/truedigital-launches-revolutionary-real-time-payments-platform-with-signature-bank

[21] https://en.wikipedia.org/wiki/JPM_Coin

[22] https://gemini.com/wp-content/themes/gemini/assets/img/dollar/gemini-dollar-whitepaper.pdf

[23] https://account.paxos.com/whitepaper.pdf

[24] https://loopring.org/resources/pwc-loopring-stablecoin-paper.pdf

[25] https://hackernoon.com/a-huge-list-of-cryptocurrency-thefts-16d6bf246389

[26] https://arxiv.org/pdf/1904.05234.pdf

[27] https://arxiv.org/ftp/arxiv/papers/1801/1801.03294.pdf

[28] https://www.businessinsider.com/bitcoin-price-government-auction-winners-2017-5

[29] https://eprint.iacr.org/2017/238.pdf

[30] https://zcoin.io/zcoins-privacy-technology-compares-competition/

[31] Ronald L. Rivest, Adi Shamir, Yael Tauman. How to leak a secret // Advances in Cryptology — ASIACRYPT 2001 / C. Boyd (ed.). — Berlin, Heidelberg : Springer-Verlag, 2001. — P. 552—565. — (Lecture Notes in Computer Science[en]. Vol. 2248).

[32] https://eprint.iacr.org/2019/508.pdf

[33] https://eprint.iacr.org/2017/1066.pdf

[34] https://zcoin.io/cryptographic-description-of-zerocoin-attack/

[35] Blockchain Quick Reference: A guide to exploring decentralized blockchain application development

By Brenn Hill, Samanyu Chopra, Paul Valencourt https://books.google.ru/books?id=RcJoDwAAQBAJ&pg=PA36&lpg=PA36&dq=cryptokitty+ethereum+performance+references&source=bl&ots=ueYSfKMGld&sig=ACfU3U3v87VnUb83Ney6SOnxBH6C-MfcNw&hl=en&sa=X&ved=2ahUKEwi7wqeQtsvkAhXriIsKHaHWDcY4ChDoATAAegQICBAB#v=onepage&q=cryptokitty%20ethereum%20performance%20references&f=false

[36] https://arxiv.org/abs/1801.04335
[37] http://stsam.irgups.ru/sites/default/files/articles_pdf_files/75-83.pdf
[38] https://arxiv.org/pdf/1901.00910.pdf
[39] https://test.ton.org/ton.pdf
[40] https://www.codementor.io/blog/blockchain-scalability-5rs5ra8eej
[41] http://www.dtcc.com/~/media/Files/Downloads/WhitePapers/Crypto-Asset-Whitepaper-2019.pdf
[42] https://issanet.org/e/pdf/2018-10_ISSA_report_Infrastructure_for_Crypto-Assets.pdf
[43] https://issanet.org/e/pdf/2018-06_ISSA_DLT_report_version_1.0.pdf
[44] https://issanet.org/e/pdf/2017-11_General_Meeting_Proxy_Voting_on_Distributed_Ledger_v2-1.pdf
[45] https://issanet.org/e/pdf/MDR_Part3_ProxyVoting_Maintenance_2014_2015_DLT_aligned.xlsx
[46] http://www.pynx.net/asianregionalpublic2018/files/Session%2011_Alexandre%20Kech_SWIFT.pdf
[47] https://www.iso.org/committee/6266604.html
[48] https://hyperledger.org
[49] https://entethalliance.org
[50] H. Jin, X. Dai, J. Xiao, Towards a novel architecture for enabling interoperability amongst multiple blockchains, in: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), IEEE, pp. 1203–1211.
[51] BTCRelay. a bridge between the Bitcoin blockchain & Ethereum smart contracts, 2018. http://btcrelay.org/.
[52] V. Buterin, Chain interoperability, 2016. https://static1. squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+ Interoperability.pdf
[53] https://www.ingwb.com/media/2667864/assessing-interoperability-solutions-for-distributed-ledgers.pdf
[54] https://cosmos.network/cosmos-whitepaper.pdf
[55] https://blockstream.com/sidechains.pdf
[56] https://arxiv.org/pdf/1908.03999.pdf
[57] https://www.hyperledger.org/projects/quilt
[58] https://polkadot.network/PolkaDotPaper.pdf
[59] Matthew Hodgson (9 October 2016). "A decentralized web would give power back to the people online". TechCrunch. AOL Inc. Retrieved 1 December 2016.
[60] https://www.ecb.europa.eu/paym/intro/governance/shared/pdf/201709_dlt_impact_on_harmonisation_and_integration.pdf
[61] European Business Organization Law Review March 2019, Volume 20, Issue 1, pp 111–137| Cite as Blockchain and Smart Contracting for the Shareholder Community
[62] "Q&A with Tim Berners-Lee, Special Report". businessweek.com. Retrieved 14 April 2018.
[63] http://ceur-ws.org/Vol-2161/paper6.pdf
[64] https://arxiv.org/ftp/arxiv/papers/1801/1801.02027.pdf
[65] Berners-Lee, T.; Hendler, J.; Lassila, O. (2001). "The Semantic Web". Scientific American. 2841 (5): 34. Bibcode:2001SciAm.284e..34B. doi:10.1038/scientificamerican0501-34.
[66] https://www.bcg.com/publications/2018/reality-check-blockchain-commodity-trading.aspx
[67] https://uis.brage.unit.no/uis-xmlui/handle/11250/2563235
[68] https://www.tradelens.com/
[69] https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/about-deloitte/20181002-DLT-v01.pdf
[70] http://ceur-ws.org/Vol-2334/DLTpaper2.pdf

КОНТАКТНАЯ ИНФОРМАЦИЯ

Адрес: Российская Федерация, 105066,
г. Москва, ул. Спартаковская, 12
Телефон: +7 495 234-48-27

E-mail: blockchain@nsd.ru

Сайт: nsd.ru