ФИНТЕХ
АССОЦИАЦИЯ

ИССЛЕДОВАНИЕ ПРОТОКОЛОВ ВЗАИМОДЕЙСТВИЯ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

АПРЕЛЬ 2020

КЛЮЧЕВЫЕ ВЫВОДЫ ИССЛЕДОВАНИЯ

- Сегодня **рынок блокчейн-платформ фрагментирован**: отсутствуют единые стандарты, которые позволяли бы беспрепятственно обмениваться информацией между различными распределенными реестрами.

- Эксперты в области блокчейна ставят задачу **обеспечить интероперабельность** между различными сетями в условиях отсутствия доверия к согласованности данных в системах обеспечения выполнения безопасности каналов связи.

- Один из ключевых факторов обеспечения интероперабельности – **согласование криптографических алгоритмов**, которые будут использоваться при передаче информации и взаимодействии систем.

- Индустрия еще не разработала стандарты для обеспечения безопасной интероперабельности распределенных реестров. При этом участникам рынка становится очевидной **необходимость стандартизации** подходов к интероперабельности.

- **Участие представителей рынка** в процессах стандартизации подходов, протоколов и концепций поможет решить ряд будущих организационных и технических вопросов.

- Сегодня существуют различные методы обеспечения интероперабельности распределенных реестров. Мы считаем, что описанный ниже **подход «мост» наиболее применим** для использования в блокчейн-решениях для бизнеса.

- **Платформа Мастерчейн** продолжит исследования и свое развитие в сторону использования подхода типа «мост». Этот подход обеспечивает должный уровень безопасности, конфиденциальности и гибкости при взаимодействии с внешними информационными системами и иными распределенными реестрами.

ВВЕДЕНИЕ

Блокчейн перестал быть технологией будущего: уже сегодня распределенные реестры запускаются в промышленную эксплуатацию, а на рынке присутствуют десятки зрелых решений на блокчейне. Вокруг технологии сформировалось устойчивое сообщество блокчейн-специалистов: только на сервисе GitHub в топ-6 крупнейших блокчейн-платформ для бизнеса зарегистрировано более 30 тыс. разработчиков (Chainstack, 2020).

Технология распределенных реестров активно развивается, однако в экспертном сообществе активно обсуждается ряд нерешенных технологических вызовов. Один из них – обеспечение интероперабельности различных блокчейнов. Сегодня, когда использование распределенных реестров предполагает разнообразие и масштабируемость экосистемы, потенциальные преимущества от интероперабельности очевидны:

- Наличие большего числа партнеров в рамках блокчейн-экосистемы может повысить ценность и увеличить отдачу от инвестиций в блокчейн.

- Интероперабельность позволит настраивать и улучшать блокчейн-решения, не позволяя им устаревать.
- Интероперабельность это возможность свободного обмена информацией между различными блокчейн-системами.

Организация интероперабельности выполняется также и для решения технологических задач: обеспечения конфиденциальности, увеличения производительности, безопасности и масштабируемости.

ЦЕЛЬ ИССЛЕДОВАНИЯ – определение практических методов взаимодействия платформ распределенных реестров.

ЗАДАЧИ:

1. Обзор методов взаимодействия распределенных реестров.
2. Анализ протоколов взаимодействия распределенных реестров, а также зарубежной практики.
3. Разработка сервиса взаимодействия распределенных реестров для платформ Мастерчейн и Hyperledger Fabric.

В рамках исследования были проведены интервью с экспертами рынка. Эксперты выразили свое мнение о практических кейсах, препятствиях и перспективах развития функционального взаимодействия платформ распределенных реестров.

1. ПРЕДПОСЫЛКИ ИССЛЕДОВАНИЯ

С момента запуска биткоина и других альткоинов в ИТ-сообществе стал возникать вопрос функционального взаимодействия платформ для обмена криптовалютой между разными сетями распределенных реестров. Функциональная совместимость (далее – интероперабельность) – это способность двух и более компьютерных систем обмениваться и взаимно использовать полученную информацию (IEC 17788:2014(en) Information technology – Cloud computing – Overview and vocabulary, 2019).

В блокчейн-технологиях под функциональной совместимостью понимают протокол, гарантирующий согласованность логических состояний в двух и более независимых распределенных реестрах. При этом возможные сценарии обмена данными между сетями не ограничиваются обменом только криптовалютой, а включают в себя также и решение функциональных задач.

ОСНОВНЫЕ СЦЕНАРИИ ПРИМЕНЕНИЯ ИНТЕРОПЕРАБЕЛЬНОСТИ СЕТЕЙ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

Обмен и передача цифровых активов.
С учетом развития рынка цифровых активов (токенов, криптовалюты) этот сценарий встречается наиболее часто. Процесс обмена и передачи может происходить как с участием доверенной стороны (например, биржи обмена криптовалюты), так и в недоверенной среде с использованием криптографических преобразований для обеспечения безопасности передачи данных. Процесс передачи цифровых активов в недоверенной среде выполняется с использованием смарт-контрактов, которые обеспечивают блокировку токена в одной сети, создание (эмиссию) конвертируемого токена в другой сети, так что блокированный токен становится недоступным для дальнейших операций.

Обеспечение конфиденциальности данных.
В распределенных реестрах с идентифицированными участниками интероперабельность платформ может использоваться для достижения конфиденциальности данных. Так, например, детальные данные по операциям сделки между ограниченным числом участников записываются в отдельный реестр, который хранится только у этих участников.

Масштабируемость и производительность.
Для обеспечения большей скорости распределенный реестр может быть разделен на сегменты (подсети, шарды, сайдчейны). Отдельные операции могут записываться в сегмент сети, при этом результат обработки группы операций записывается в основной реестр.

«Как вы понимаете термин "интероперабельность" в распределенных реестрах?»

Артем Дуванов, директор по инновациям Национального расчетного депозитария (НРД): «С одной стороны, под интероперабельностью мы понимаем техническую возможность кросс-блокчейн-транзакций, т. е. гарантированное совместное обновление или не обновление двух разных блокчейн-сетей. Вторая составляющая интероперабельности – это единые стандарты, возможность высокоуровневых приложений быть независимыми от конкретных блокчейнов и спокойно работать над несколькими сетями».

Функциональное разделение реестров.
Распределенные реестры могут иметь различные смарт-контракты для совершения разных операций. Например, процесс регистрация цифрового актива может быть выполнен в одном реестре, а его продажа и вторичный рынок – в другом.

Проекты, включающие в себя средства интероперабельности:
Virtualchain, Sidechain, Interledger, Cosmos, Polkadot, Overledger, TokenBridge, NEAR Protocol, Wanchain, BTC Relay, Ethereum 2.0, Corda.

2. МЕТОДЫ ИНТЕРОПЕРАБЕЛЬНОСТИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

1. ХЕШ-КОНТРАКТЫ ВРЕМЕННОЙ БЛОКИРОВКИ

Одним из наиболее распространенных способов реализации интероперабельности является атомарный обмен. Он основан на криптографическом протоколе HTLC (Hash Time Locked Contracts) (Hash Time Locked Contracts, 2019). В процессе переноса данных участники обмениваются секретной информацией, которая используется при поверке записи. Примером реализации служит протокол Interledger, поддерживаемый Ripple. Также на основе HTLC построена технология Lightning Network (Lightning Network Documents, 2019), реализация которой выполнена в Мастерчейне для масштабирования количества операций.

Преимущества:
- Универсальное решение для всех приложений.

Недостатки:

- Сервис использует криптографические преобразования (аутентификация, шифрование), требует прохождения сертификации и отдельного ТЗ.
- Неустойчив к цензурированию, когда узлы перестают передавать информацию от одной сети в другую.
- Требует активного участия взаимодействующих сторон.

2. МОСТ НА СТОРОНЕ ДОВЕРЕННОГО УЧАСТНИКА

Если атомарные обмены и протокол Interledger (Interledger Overview, 2019) подразумевают обмен активами, то мосты подразумевают обмен сообщениями, например, вызов функций смарт-контрактов одного распределенного реестра из другого. Подход основан на наличии в системах посредников (оракулов) для передачи информации из одного блокчейна в другой.

Преимущества:

- Небольшие издержки на настройку программного обеспечения участника.
- Достаточно проведения оценки влияния на стороне инфраструктуры доверенной организации.

Недостатки:

- Требует адаптации для каждого кейса в отдельности исходя из особенностей передаваемых форматов данных.
- Требует поддержки на стороне доверенной организации.
- Требует отдельного соглашения между участником и доверенной организацией для каждого кейса в отдельности и включения этой организации в каждый кейс, необходимый для межсетевого взаимодействия.

3. РЕЛЕЙНЫЙ БЛОКЧЕЙН (МАСТЕР-СЕТЬ)

Релейный блокчейн (релейная сеть/мастер-сеть) предполагает создание единой сети из обособленных блокчейн-сетей. При этом согласованность данных блокчейн-сетей, объединенных в релейную сеть, обеспечивается за счет записи их состояний в релейный блокчейн, который лежит в основе такой сети.

Преимущества:

- Все изменения выполняются каждым участником независимо.
- Дополнительная безопасность включенных блокчейнов обеспечивается безопасностью релейной сети.

Недостатки:

- Требует прохождения оценки влияния для каждого участника.
- Решения об инцидентах ИБ не согласованы.

СПОСОБЫ РЕАЛИЗАЦИИ ИНТЕРОПЕРАБЕЛЬНОСТИ ПЛАТФОРМ

АТОМАРНЫЙ ОБМЕН

Реализация атомарного обмена не требует наличия доверенной стороны. При этом условия его выполнения включают ряд требований:

- Пользователи, участвующие в обмене, должны иметь адреса в распределенных реестрах друг друга.
- Платформы не должны в одностороннем порядке ограничивать доступ к сети для участников обмена.

- Платформы должны поддерживать общие криптографические алгоритмы, чтобы создаваемые криптографические доказательства работали в рамках протокола в разных реестрах. Например, если хеш, блокирующий активы в одном реестре, не подойдет к хешу своего прообраза в другом реестре, то это не позволит вывести активы.

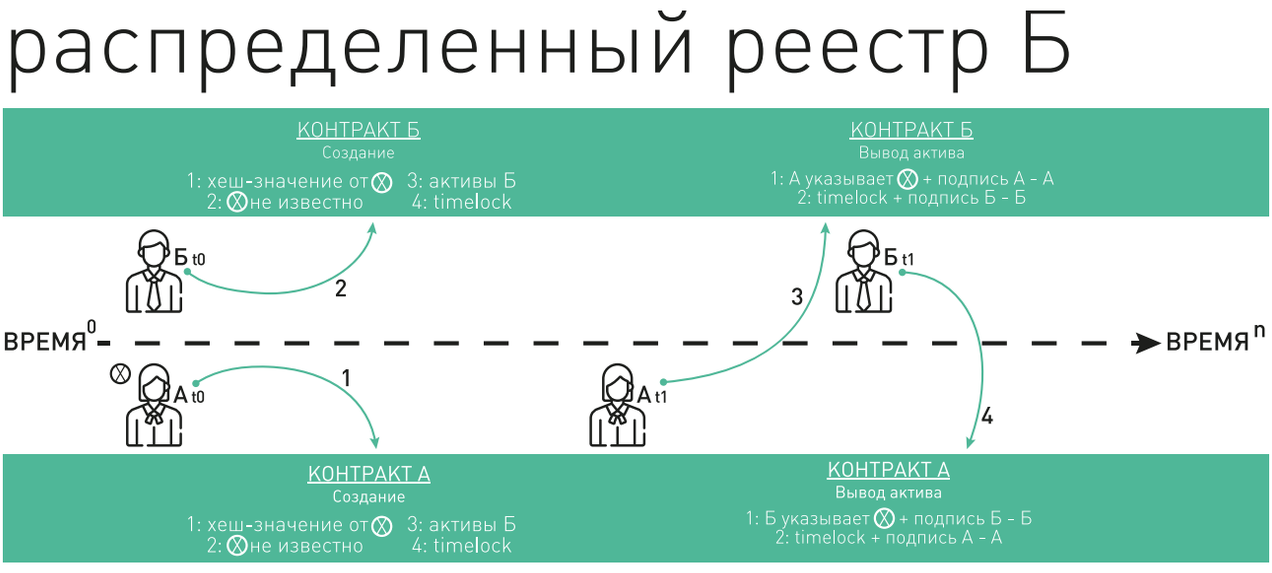


Рис 1. Схема атомарного обмена

ПОШАГОВОЕ ИСПОЛНЕНИЕ:

1. Алиса придумывает *секрет* и берет от него значение криптографической хеш-функции (далее – *хеш-значение*).
2. Алиса размещает в распределенном реестре HTLC-контракт с хеш-значением и блокирует в контракте свои активы для их последующей передачи Борису.
3. Алиса передает экземпляр HTLC-контракта с хеш-значением Борису.
4. Борис проверяет HTLC-контракт, размещает его в своем реестре и блокирует свои активы для последующей передачи Алисе.
5. Чтобы Алиса забрала активы, заблокированные Борисом, она должна раскрыть секрет, хеш-значение от которого она получила на шаге 1.
6. Так как информация хранится публично, Борис видит секрет, который отправила в сеть Алиса, когда забирала свои активы с контракта, размещенного Борисом.
7. Борис использует этот секрет, чтобы забрать активы, которые заблокировала Алиса в своей сети.
8. Так как HTLC-контракт подразумевает еще и блокировку по времени, Алиса не может в течение некоторого времени вывести свои активы.
9. Борис должен до этого времени вывести активы Алисы, иначе Алиса вернет их себе.

МОСТ И НОТАРИАЛЬНАЯ СХЕМА

Подход «мост» позволяет передавать не только активы, но и сообщения, включая вызов метода смарт-контракта в другом реестре.

В профессиональном сообществе «мостом» называется связка из *сервиса-оракула*, который отслеживает транзакции и события, и *системного смарт-контракта*, который генерирует события внутри своего блокчейна и обрабатывает входящие события из других систем.

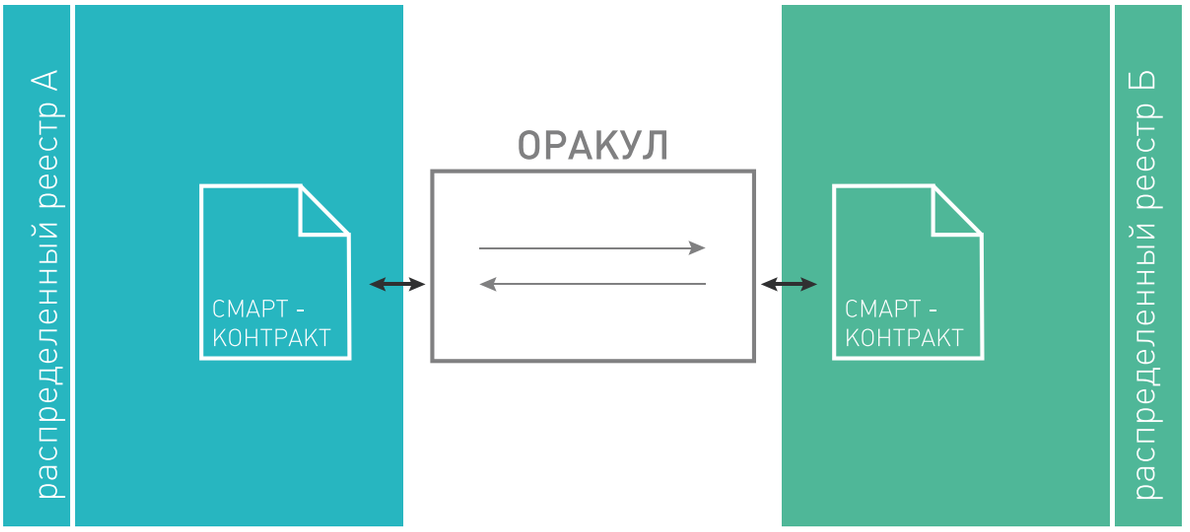


Рис 2. Схема использования моста

Сценарий взаимодействия в сетях на основе Ethereum:

1.В смарт-контракте моста вызывается специальный метод, в который передается:
- адрес вызываемого в другом реестре смарт-контракта,
- сигнатура вызываемого метода,
- передаваемые в этот метод аргументы.

2. Специальный метод генерирует событие, которое содержит информацию, переданную в него на шаге 1.

3. *Оракул* прослушивает смарт-контракт моста на наличие новых событий и при наступлении события вызывает связанную с типом события логику, которая выполняет соответствующий метод в смарт-контракте в другой сети.

Мост одновременно размещается в двух сетях, но также может присутствовать только в одной сети, получая всю необходимую информацию по другим каналам связи. При этом основная функция заключается в криптографический проверки аутентичности передаваемой информации взаимодействующих участников.

Нотариальные схемы являются развитием подхода типа «мост». Главный элемент нотариальных схем – т. н. «нотариусы»: они несут ответственность за передачу сообщений, и чаще всего именно им отведена роль валидаторов в блокчейн-сети. Обязанности нотариусов – проверка того, что событие было сгенерировано в одном распределенном реестре, сбор необходимых подтверждений о событии от других участников нотариальной схемы и передача информации о событии в другой реестр.

РЕЛЕЙНЫЙ БЛОКЧЕЙН, ИЛИ МАСТЕР-СЕТЬ

Релейный блокчейн (мастер-сеть) – это отдельный многоуровневый блокчейн, который связывает обособленные блокчейн-сети в единую структуру. Возможность проверить и передать данные из одного блокчейна в другой через связующий «релейный» блокчейн называется релейной передачей.

Релейный блокчейн наблюдает за состояниями всех связанных в релейную сеть блокчейнов и при необходимости, согласно определенным правилам, может контролировать и управлять активами в этих сетях.

Рис 3. Релейная сеть, или мастер-сеть

В рамках подхода «релейный блокчейн» стоит упомянуть о т. н. *сайдчейне*. Сайдчейн (от англ. sidechain – боковая цепь) – это обособленный блокчейн, который входит в структуру релейной блокчейн-сети. В зависимости от реализации сайдчейны имеют различную степень зависимости от своего «родительского» блокчейна.

Основная цель сайдчейнов – реализация возможности безопасного перемещения некоторых цифровых активов между реестрами для проведения действий над ними.

Предпосылки для использования подхода «сайдчейн»:

- Время подтверждения транзакций. Задержки транзакций в сайдчейне обычно значительно меньше, чем в основном блокчейне.
- Стоимость записи транзакций. В сайдчейне стоимость транзакций может быть значительно ниже, чем в основном блокчейне.
- Расширение функциональных возможностей. Сайдчейн может обладать некоторыми функциональными возможностями, которые могут отсутствовать в основном блокчейне.

В настоящее время релейный блокчейн проходит стадию исследований и не рассматривается далее.

«Какой подход в настоящее время больше всего подходит для достижения интероперабельности блокчейн-сетей?»

Валентин Руль, ведущий разработчик QBT: «Подход "мост" на этом этапе развития индустрии – наиболее универсальный способ достижения интероперабельности блокчейн-сетей. При этом в закрытых корпоративных сетях наличие доверенного посредника не является существенным негативным фактором, и при должной реализации такого подхода безопасность сетей не компрометируется. Релейные сети сулят много преимуществ в будущем, но на данный момент в отрасли нет устоявшегося понимания технологии, поэтому для решения практических задач она пока не подходит».

СРАВНЕНИЕ ПОДХОДОВ

	Атомарный обмен	Построение моста	Релейная цепь
Назначение	Передача активов	Передача сообщений	Передача сообщений
Масштабируемость по количеству участников	Низкая	Средняя	Высокая
Требуется доверенный участник	Нет	Да	Нет
Сложность реализации	Низкая	Средняя	Высокая
Отношения между участниками обмена	Один-к-одному	Один-к-одному	Многие-ко-многим
Способ обеспечения достоверности данных	Криптографические преобразования	Выделенный участник	Доверенная сеть
Примеры реализации	Interledger, Lightning Network	Corda, BTC Relay, TokenBridge, Overledger	Polkadot, Cosmos, Ethereum 2.0, NEAR Protocol, Wanchain, Sidechain

3. ОБЗОР ЗАРУБЕЖНЫХ ПРОЕКТОВ ИНТЕРОПЕРАБЕЛЬНОСТИ

На фоне постоянного развития отрасли и растущей необходимости в налаживании совместимости между различными блокчейн-сетями уже появились различные примеры работы над соответствующими решениями. С одной стороны, наличие таких игроков свидетельствует о развитии рынка, с другой – инициативы довольно конкретные и работают только с определенными платформами.

POLKADOT

Идея Polkadot приписывается Гэвину Вуду, одному из сооснователей Ethereum. Polkadot облегчает не только транзакции, но и обмен данными. Экосистема Polkadot содержит парачейны (parachains – отдельные блокчейны, ставшие частью среды Polkadot) и релейную цепь (relay chain), которая их соединяет. Каждый парачейн может иметь различные характеристики и распространять свои транзакции по всей экосистеме. Все цепочки, которые становятся частью экосистемы Polkadot, должны адаптировать свои механизмы консенсуса к правилам Polkadot, но у них есть свобода развития структуры и функций своего блокчейна.

BLOCKNET

Blocknet – это протокол для совместимости, который обеспечивает связь, взаимодействие и обмен данными между различными публичными и частными блокчейнами, а также доступ к внесетевым данным, API и сервисам через оракулов.

AION
Aion разработан канадской компанией Nuco, специализирующейся на корпоративных блокчейн-решениях. Aion отличается от других разработок тем, что в его консенсусную модель интегрируется ИИ. Многие блокчейн-системы не в состоянии вместить большие объемы данных, и Aion предлагает решить эту проблему с помощью высокопроизводительной виртуальной машины и масштабируемой базы данных.

ARK
Ark ставит своей целью создание масштабируемого и адаптируемого решения для взаимодействия с блокчейном. Компания автоматизировала создание новых блокчейнов в экосистеме. Платформа Ark имеет встроенную поддержку для многих языков программирования, включая Java, Swift, Python и Ruby. Это делает ее доступной для людей, которые предпочитают работать с определенными языками.

WANCHAIN
Wanchain позиционирует себя как первое в мире интерактивное блокчейн-решение с защищенными многопользовательскими вычислениями. В его основе лежит Ethereum, который позволяет развертывать смарт-контракты. Также Wanchain позиционируется как блокчейн-решение для создания распределенных приложений, которые требуют легкого доступа к различным блокчейнам. Конфиденциальность на блокчейне повышается за счет использования одноразовых скрытных адресов и кольцевых подписей (вид электронной подписи, который позволяет одному из участников группы подписать сообщение от имени всей группы, сохранив при этом свою анонимность).

COSMOS
Cosmos в настоящее время является одной из крупнейших инициатив по обеспечению совместимости блокчейн-платформ. Эта экосистема работает по алгоритму консенсуса Tendermint. Независимые блокчейны, называемые зонами, подключаются к сети Cosmos, при этом все зоны связаны с Cosmos Hub и могут взаимодействовать друг с другом.

BLOCKCHAIN INTEROPERABILITY ALLIANCE
Blockchain Interoperability Alliance – это объединение ICON, Aion и Wanchain. Альянс уже начал сотрудничать в области исследования обменных операций и коммуникаций. Разработка общих отраслевых стандартов, а также обмен результатами исследований и архитектурой протоколов остаются на повестке дня на первом месте.

INTERLEDGER
Interledger – это набор открытых протоколов для отправки платежей между различными реестрами. Выпущен компанией Ripple в 2015 году.

LIGHTNING NETWORK
Lightning Network – это децентрализованная система мгновенных микроплатежей (менее нескольких центов – до 0,00000001 биткоина).

CORDA SETTLER
Corda Settler – приложение консорциума R3 с открытым исходным кодом для проведения международных платежей. Первым токеном, поддерживаемым Corda Settler, стал XRP от Ripple.

BTC RELAY
BTC Relay позволяет смарт-контрактам на Ethereum безопасно проверять транзакции биткоинов без посредников: пользователи могут платить биткоинами для использования Ethereum DApps.

TOKENBRIDGE

TokenBridge позволяет обмениваться данными (например, информацией о владении цифровым активом) между двумя цепями в экосистеме Ethereum. В режиме бета-тестирования разработаны три моста между Ethereum Mainnet и другими сетями, построенными на Ethereum: POA, xDai, Eth Classic. Также тестирование проходят мосты Arbitrary Message (для обмена любыми данными между любыми цепями, основанными на Ethereum Virtual Machine) и ETH-BNC (Ethereum to Binance).

OVERLEDGER

Overledger – это операционная система для блокчейна, которая позволяет приложениям подключаться к нескольким технологиям распределенного реестра или блокчейна, тем самым превращаясь в «многоцепочные» приложения (англ. multi-chain applications, mApps). Разработчики могут создавать подписанные транзакции и отправлять их одновременно всем поддерживаемым технологиям распределенного реестра через интерфейс Blockchain Programming Interface (BPI) Overledger.

ETHEREUM 2.0

На июль 2020 года запланирован выход Ethereum 2.0. Для обновления под названием Istanbul (хардфорк состоялся в декабре 2019 года) в числе предложений EIP (Ethereum Improvement Proposals) было вынесено EIP-152. Его суть в том, что внедряется новый контракт с целью создания интероперабельности между виртуальной машиной Ethereum (EVM) и ZCash или другими криптовалютами на базе протокола Equihash.

NEAR PROTOCOL

NEAR – управляемая сообществом разработчиков облачная инфраструктура для развертывания и запуска децентрализованных приложений. Она сочетает в себе функции децентрализованной базы данных с другими функциями бессерверной вычислительной платформы. Токен, который позволяет этой платформе работать, также дает возможность приложениям, построенным поверх нее, легко взаимодействовать друг с другом.

ENTERPRISE ETHEREUM ALLIANCE (EEA)

Альянс EEA запустил в январе 2020 года песочницу EEA TestNet, где форки Ethereum могут быть стандартизированы в соответствии с определенными спецификациями, установленными ранее альянсом, что сделает их совместимыми друг с другом. В настоящее время сотни компаний работают над корпоративными версиями Ethereum, появляются новые игроки, присоединившиеся к альянсу через Hyperledger Besu (Ethereum – участник консорциума Hyperledger), что делает стандартизацию приоритетом.

JASPER-UBIN

В ходе совместного проекта денежно-кредитного управления Сингапура и Банка Канады были объединены распределенные реестры двух государств – Project Ubin и Project Jasper. Пилотный проект доказал возможность успешного обмена токенизированных цифровых валют между разными блокчейн-платформами. В основе лежал подход HTLC. Эксперимент проводился на платформах Quorum (сингапурский Project Ubin) и Corda (канадский Project Jasper). В ходе проекта были переведены 105 сингапурских долларов из местного банка в канадский с валютным курсом 1 сингапурский доллар к 0,95 канадскому доллару. В итоге канадский банк получил 100 сингапурских долларов.

4. ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ НА ПРИМЕРЕ ПЛАТФОРМ МАСТЕРЧЕЙН И HYPERLEDGER FABRIC

Исследуемые подходы, обеспечивающие интероперабельность сетей Мастерчейн и Hyperledger Fabric:

- **атомарный обмен,** HTLC-протокол. Подход выбран из-за простоты программной реализации и концепции обмена активами между идентифицированными участниками в разных сетях.
- **построение моста** между сетями Мастерчейн и Hyperledger Fabric. Подход «мост» выбран из-за возможности передачи произвольных сообщений между сетями, которые можно использовать для вызова функции смарт-контрактов в других реестрах и возврата данных в вызывающий смарт-контракт.

Прикладной целью исследований было изучение этих подходов и определение потенциальных проблем и трудностей реализации интероперабельности между сетями Мастерчейн и Hyperledger Fabric.

Сопутствующей целью было определение и понимание границ применимости технологий Burrow EVM (EVMCC) (Hyperledger Burrow – Hyperledger, 2019) при создании атомарного обмена и моста между сетями. Выбор технологий Burrow EVM и EVMCC был обусловлен их технологической близостью к платформе Мастерчейн.

ОПИСАНИЕ ИСПОЛЬЗУЕМЫХ ТЕХНОЛОГИЙ

Мастерчейн (v1.0) – сертифицированный распределенный реестр, основанный на платформе Ethereum и созданный для проведения юридически значимых транзакций. Разработан Ассоциацией ФинТех совместно с ключевыми участниками российского финансового рынка.

Solidity 0.5.x – язык написания смарт-контракта для EVM и компилятор, который преобразует исходный код в байт-код EVM.

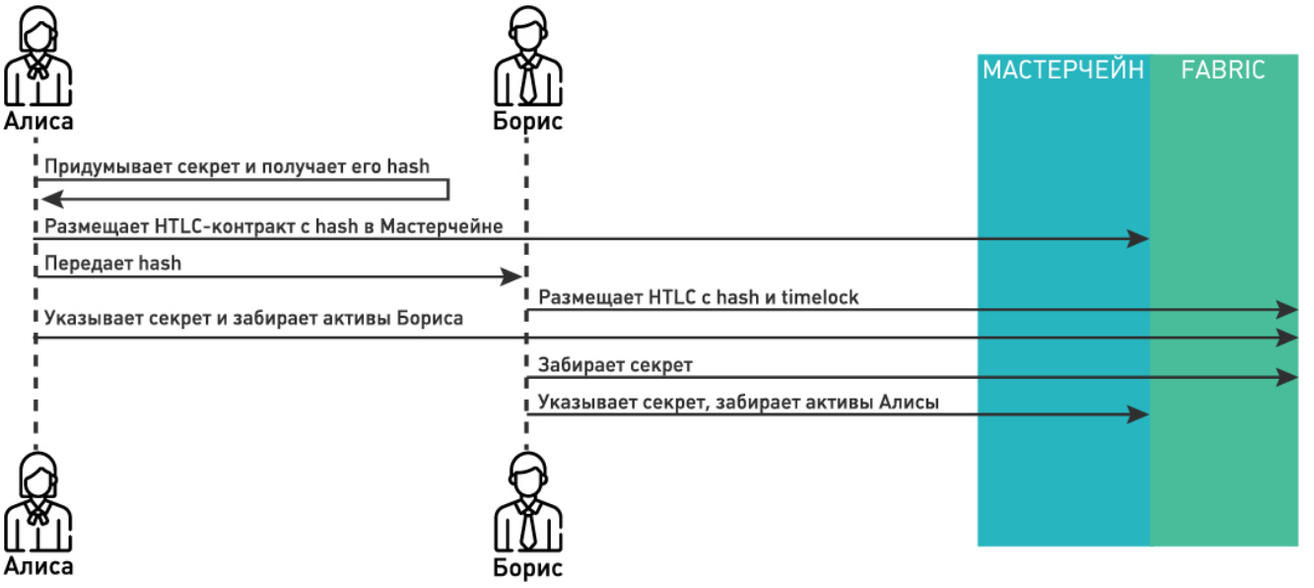
Hyperledger Fabric (v1.4) – фреймворк для создания доверенных корпоративных распределенных реестров с алгоритмом консенсуса (класса CFT) Raft (The Raft Consensus Algorithm, 2019). Далее используется аббревиатура HLF. Типовое использование HLF заключается в создании закрытой сети, в которой организации-участники генерируют и обрабатывают транзакции. За упорядочивание и распространение транзакций отвечает ключевой элемент сети – узлы Ordering Service. Участвующие в бизнес-процессах организации формируют каналы, в которых происходит их взаимодействие. Бизнес-логика взаимодействия осуществляется через предварительно размещенные в канале чейнкоды.

Hyperledger Burrow – проект консорциума Hyperledger, целью которого является реализация спецификации Ethereum под управлением консенсуса Tendermint (Tendermint Docs, 2019).

EVMCC – чейнкод для канала в сети Hyperledger Fabric. Работа чейнкода EVMCC заключается в создании внутри себя окружения Burrow EVM, в котором можно запустить смарт-контракт и вызвать его бизнес-логику. После размещения и инициализации чейнкода в канале к нему можно обращаться как к экземпляру EVM и размещать в нем смарт-контракты.

В нашем исследовании мы размещаем смарт-контракты атомарного обмена (HTLC.sol) и моста (Bridge.sol) в сети Мастерчейн и чейнкоде EVMCC (Hyperledger Fabric).

ПОДХОД «АТОМАРНЫЙ ОБМЕН»



4. Диаграмма последовательности схемы «атомарный обмен»

Атомарный обмен включает в себя смарт-контракты, размещенные в сетях Мастерчейн и Hyperledger Fabric, и дальнейшее выполнение HTLC-протокола с их участием.

Экземпляр основной структуры данных атомарной сделки

```
struct HushTimeLockContract {
        adress payble sender; // адрес отправителя платежа
        adress payble receiver; // адрес получателя платежа
        uint amount; // количество передаваемых активов
        bytes32 hashlock; // хеш-значение от прообраза
        unit timelock; // Врема UNIX в секундах, блокировка во времени
        bool withdrawn; // логическое поле - были ли активы выведены
        bool refunded; // логическое поле - были ли активы возвращены
        bytes32 preimage; // прообраз для hashlock, по умолчанию 0x0
    }
```

РЕАЛИЗАЦИЯ СЦЕНАРИЯ

1. Смарт-контракт HTLC_A.sol размещается в сети Мастерчейн.
2. Алиса загадывает секрет (*preimage*) и берет от него хеш-значение (*hashlock*).
3. Алиса вызывает метод newContract у размещенного в сети Мастерчейн смарт контракта HTLC_A.sol и передает в него параметры (receiver – *получатель_активов*, hashlock, timelock – *время_жизни_контракта*) и создает тем самым новую сделку на количество активов переданных в *msg.value.*

```
function newContract(address payable _receiver, bytes32 _hashlock, uint _timelock) external payable futureTimelock(
    _timelock) returns (bytes32 contractId)
```

4. Борис размещает аналогичный контракт (HTLC_B.sol) в своей сети HLF и указывает свои данные, но hashlock берет у Алисы.
5. Алиса, чтобы перевести активы себе на счет в реестре Бориса (HLF), должна вызвать функцию смарт-контракта HTLC_B *withdraw* и указать *preimage* – после этого активы будут переведены на ее счет, а *preimage* будет записан в реестре HLF.

```
function withdraw(bytes32 _contractId, bytes32 _preimage) external contractExists(_contractId) hashlockMatches(
    contractId,  preimage) withdrawable( contractId) returns (bool)
```

6. После того как *preimage* Алисы будет записан в HLF, Борис может увидеть его и воспользоваться им для перевода активов в реестре Алисы (Мастерчейн), вызвав функцию *withdraw* в HTLC_A.
7. Алиса получила активы в реестре Бориса (HLF), Борис получил активы в реестре Алисы (Мастерчейн). Сделка совершена.

ПОДХОД «ПОСТРОЕНИЕ МОСТА МЕЖДУ СЕТЯМИ»

Реализация подхода типа «мост» заключается в размещении в сетях Мастерчейн и HLF системных смарт-контрактов и создании сервиса-оракула.
Основная задача системных смарт-контрактов заключается в регистрации события вызова прикладного смарт-контракта, расположенного в другом реестре. Зарегистрированное событие является триггером для выполнения логики сервиса-оракула.

```
interface CommonBCBridgeInterface {

   function setValueInAnotherBC(adress anotherBCBontract, bytes4 method, uint256 _inputData) external;
   function getValueInAnotherBC(adress anotherBCBontract, bytes4 method, external returns(unit256 data);

   event RequestForChangeValue(
     address contractSender,
     adress contactReceiver,
     bytes encodedData);
}
```

Сервис-оракул – это программа, которая отслеживает активность системных смарт-контрактов. При возникновении в системных смарт-контрактах событий оракул выполняет связанную с типом события логику. В нашем случае – вызов функций в другом реестре.

Например, при вызове функции системного смарт-контракта *setValueInAnotherBC* регистрируется событие *RequestForChangeValue* (которое содержит передаваемые данные в специальном формате), оракул получает это событие из логов Мастерчейна, проверяет корректность поступившей информации в Hyperledger Fabric (адреса смарт-контрактов, адреса участников, соответствие отправляемых и принимаемых данных, подписи транзакций), после чего вызывает соответствующую функцию прикладного смарт-контракта в запрашиваемом реестре.

Прикладные смарт-контракты – это смарт-контракты, функции которых мы вызываем из других реестров, или контракты, в которых мы вызываем функции других смарт-контрактов в других распределенных реестрах.

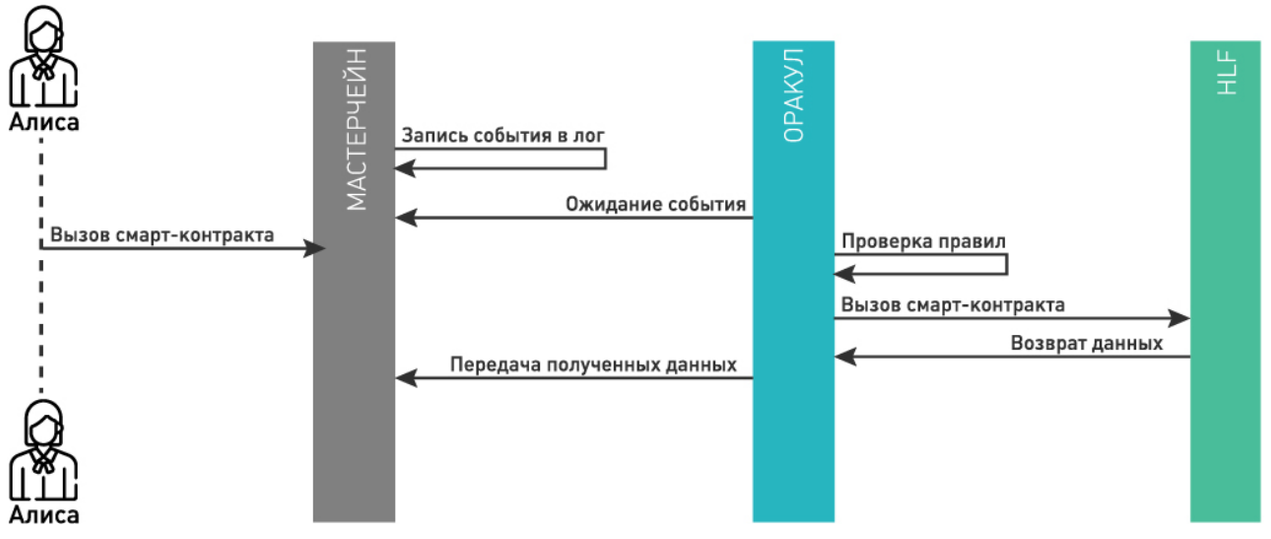


Рис 5. Диаграмма последовательности взаимодействия через мост

1. В реестрах Мастерчейн и HLF размещается системный смарт-контракт Bridge.sol.
2. В реестрах Мастерчейн и HLF размещаются прикладные смарт-контракты TestMasterchain.sol и TestHLF.sol.
3. Алиса (реестр Мастерчейн) хочет вызывать функцию setValue в смарт-контракте TestHLF (реестр HLF) и передать в нее данные.
4. Алисе известен адрес смарт-контракта TestHLF, функцию которого ей нужно вызвать, и ей известна сигнатура вызываемой функции в виде первых 4 байтов.
5. Алиса (Мастерчейн) вызывает в смарт-контракте Bridge.sol функцию setValueInAnotherBC
6. Функция setValueInAnotherBC кодирует поступившую информацию о методе (4 байта сигнатуры) и передаваемых в него данных.
7. Функция setValueInAnotherBC формирует событие, передает в него адрес вызываемого смарт-контракта, закодированные данные и затем записывает событие в логи смарт-контракта Bridge.
8. Оракул подписан на события смарт-контракта Bridge, и при возникновении нового события он определяет адрес и функцию вызываемого смарт-контракта.
9. Оракул вызывает функцию в смарт-контракте в сети HLF и передает в него отправленные Алисой данные.
10. После проверок на корректность и доступ данные записываются в реестр HLF.
11. Оракул возвращает Алисе хеш-транзакции как подтверждение проведенной операции.

ВЫВОДЫ ПО ПРАКТИЧЕСКОЙ ЧАСТИ

АТОМАРНЫЙ ОБМЕН

- Реализация EVMCC для HLF не хранит пользовательские адреса на уровне состояния распределенного реестра, а генерирует их на основе публичных пользовательских ключей сети HLF. Соответственно, нет балансов и встроенной платежной единицы, которая могла бы быть заблокирована контрактом HTLC. В качестве альтернативы можно рассмотреть реализацию токенов на основе протокола ERC-20. Совмещая базовую реализацию HTLC и ERC-20, можно создать комбинированный контракт, который позволяет выполнить перевод токенов из одной сети в другую.
- Из-за несовместимости используемой платформами криптографии в EVMCC невозможно проверить результат хеширования прообраза для разблокировки активов. Эта фундаментальная для HTLC проблема не позволяет реализовать атомарный обмен между сетями Мастерчейн и HLF.

ВЫЗОВ ФУНКЦИЙ ЧЕРЕЗ МОСТ

- При проведении испытаний на стороне EVMCC обнаружено, что транзакции не содержат vrs (ECDSA: (v, r, s), what is v?, 2019), по которым возможно однозначно определить отправителя транзакции, проверив подпись транзакции. Эта особенность мешает строить безопасное взаимодействие между сетями.

ОСОБЕННОСТИ EVMCC/BURROW

- EVMCC – это не отдельный экземпляр Burrow EVM, а представление Burrow EVM в среде Hyperledger Fabric в виде чейнкода, который оказался недостаточно функциональным для реализации выбранных подходов. Например, в EVMCC отсутствуют аккаунты (адреса, балансы, платежные единицы, трансфер платежных единиц), в Burrow не реализованы некоторые предкомпилированные смарт-контракты ([SNatives] Implement mainline Ethereum precompiles, 2019). В HLF Burrow используется криптография, отличная от той, которая используется в Мастерчейне – это накладывает ряд ограничений на реализацию интероперабельности платформ.

5. ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНОЛОГИЧЕСКИХ РЕШЕНИЙ ПО ИНТЕРОПЕРАБЕЛЬНОСТИ

По консолидированному мнению опрошенных экспертов, необходимость в интероперабельности есть, но рынок еще недостаточно осознал ее. Это связано со слабой развитостью рынка блокчейн-решений в целом и отсутствием промышленных сетей, которые можно было бы объединить для создания «сквозных» бизнес-процессов. При этом эксперты сходятся во мнении, что подходы к интероперабельности необходимо исследовать и развивать, так как потребность в функциональной совместимости будет нарастать – это связано с активным развитием технологий распределенных реестров и вводом блокчейн-решений в промышленную эксплуатацию.

Некоторые эксперты считают, что будущее – за консорциумными блокчейн-сетями, которые свяжут в общее информационное пространство организации, объединенные по сфере профессиональной деятельности или сектору экономики. Такие сети будут представлять из себя кластеры с выделенной структурой управления. Функциональное взаимодействие подобных кластеров потенциально может реализовать концепцию Internet-of-Value (Internet of Value Manifesto, 2019).

Ричард Браун, технический директор блокчейн-консорциума R3, предлагает разбить проблему интероперабельности на конкретные составляющие, чтобы эффективнее ее решать (Brown, 2020):

- нужна *интеграция* с существующими системами;
- нужна возможность *инициировать* транзакции на других сетях;
- нужна возможность осуществлять *interchain*-транзакции (между разными реестрами) с решениями на других технологиях;
- нужна возможность проводить *intrachain*-транзакции (с использованием различных вариантов развертывания одной и той же технологии);
- нужно упростить *interchange* – замену одной базовой платформы на другую.

«Требуется ли стандартизация подходов к интероперабельности?»

Павел Болотов, старший архитектор Райффайзенбанка: «Безусловно, требуется. Группы компаний будут создавать свои внутренние блокчейн-кластеры. И здесь остро встанет вопрос взаимодействия систем, основанных на разных технологиях: банки будут сидеть в своем кластере, покупатели и продавцы – в своем, и нужно обеспечить магистральное межкластерное взаимодействие в пределах одной сделки. Здесь, конечно, необходима стандартизация, т. к. кластеры должны работать по конкретным видам сделок, в одном формате, обеспечивать бесшовность взаимодействия».

Также эксперты сходятся во мнении, что функциональная совместимость распределенных реестров, основанных на различных технологиях, придает значительную ценность платформам с функциями интероперабельности. Интероперабельность позволит реализовать новые бизнес-кейсы в консорциумных и частных распределенных реестрах. При этом у экспертов нет единого мнения относительно возможного успеха функционального взаимодействия открытых (публичных) блокчейнов и консорциумных распределенных реестров. Среди причин, по которым возникли сомнения в успехе, – разные функциональные свойства, требования к безопасности и производительности.

Главными препятствиями для развития технологий интероперабельности являются: ключевые расхождения в используемых технологиях (различия в классах консенсусов, криптографическая несовместимость, разные способы обработки транзакций), недостаточность научных и практических исследований технологий подобного рода, отсутствие острой потребности в интероперабельности, дефицит профессиональных стандартов в сфере функционального взаимодействия распределенных реестров.

По мнению экспертов, подходы к интероперабельности необходимо стандартизировать, но процессы стандартизации необходимо выполнять после апробации подходов на реальных кейсах, которые позволят сформировать практические требования.

Стоит отметить, что в данный момент ведутся исследования в международных центрах стандартизации: в International Organization for Standardization, ISO/TC 307 Blockchain and distributed ledger technologies (Международная организация по стандартизации, ИСО/ТК 307 «Блокчейн и технологии распределенного реестра»), в International Telecommunication Union, ITU-T (Международный союз электросвязи, Сектор стандартизации электросвязи – МСЭ-Т). На национальном уровне – в Техническом комитете по стандартизации «Криптографическая защита информации» (ТК 26) и в Техническом комитете по стандартизации «Программно-аппаратные средства технологий распределенного доступа и блокчейн» (ТК 159).

Ждет ли нас в будущем огромное количество блокчейн-платформ? Скорее всего, нет. Уже сейчас есть топ-3 платформы, занимающие значительную долю рынка: Ethereum, Hyperledger и Corda. Если три года назад отрасль находилась в состоянии повышенного внимания к технологии, то к настоящему времени рынок значительно созрел в технологическом плане, и пришло время для следующего шага в развитии технологии – обеспечения взаимодействия между разными платформами. Поэтому будущее – не за большим количеством платформ, а за протоколами для их взаимодействия и стандартизацией.

ЗАКЛЮЧЕНИЕ

Распределенные реестры сталкиваются с непростой задачей: обеспечить интероперабельность между сетями в условиях недостатка доверия к согласованности данных и обеспечения безопасности каналов связи.
В зависимости от требований подходы к интероперабельности имеют разный уровень сложности реализации: от криптографической связи транзакций в различных реестрах до многоуровневых структур с высокой степенью масштабируемости.
При этом у всех подходов прослеживаются общие ограничения.

СОГЛАСОВАНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Основная задача при разработке протоколов функциональной совместимости – согласование криптографических алгоритмов, которые будут использоваться при передаче информации и взаимодействия систем.

Важными факторами при согласовании логических состояний объединяемых реестров являются: противодействие «недобросовестному» поведению, отсутствие единой точки отказа, существующие политики доступа и управления распределенными реестрами.

СТАНДАРТИЗАЦИЯ

Стандарты для обеспечения безопасной интероперабельности распределенных реестров еще не разработаны рынком. При этом рынок понимает, что стандартизация подходов к интероперабельности неизбежна. Решением этих вопросов занимаются в техническом комитете 159 «Программно-аппаратные средства технологий распределенного реестра и блокчейн» рабочие группы «Интеллектуальные контракты» и «Взаимодействие систем распределенных реестров».

Участие представителей рынка в процессах стандартизации подходов, протоколов, концепций обеспечения функциональной совместимости распределенных реестров поможет решить ряд будущих организационных и технических вопросов.

ПРИОРИТЕТНЫЕ ПОДХОДЫ В КОРПОРАТИВНОМ СЕКТОРЕ

Подход «мост» предполагается рассматривать как наиболее применимый для использования в корпоративной среде. Во-первых, этот поход обеспечивает возможности передачи структурированных сообщений. Во-вторых, с учетом идентификации участников может быть выбрана доверенная сторона или нотариат. В-третьих, подход обеспечивает должный уровень конфиденциальности соединяемых распределенных реестров с учетом относительной простоты реализации.

Релейная сеть (мастер-сеть) потенциально позволит объединить распределенные реестры в единую сеть, повысив безопасность включенных в нее распределенных реестров и упростив передачу сообщений между ними посредством использования общих криптографических алгоритмов. Это направление интероперабельности активно исследуется, но на данный момент ни одно из решений в рамках релейной сети не прошло достаточных промышленных испытаний.

ИНТЕРОПЕРАБЕЛЬНОСТЬ МАСТЕРЧЕЙНА

Платформа Мастерчейн продолжит исследования и свое развитие в сторону использования подхода типа «мост». Этот подход обладает необходимыми свойствами, которые обеспечивают должный уровень безопасности, конфиденциальности и гибкости при взаимодействии с внешними информационными системами и иными распределенными реестрами.

СПИСОК ЛИТЕРАТУРЫ

SNatives] Implement mainline Ethereum precompiles. 2019. URL: https://github.com/hyperledger/burrow/issues/1240 (дата обращения: 02.12.2019).

Brown, R. G. The Five Ingredients Of Blockchain Interoperability // Forbes, 2020. URL: https://www.forbes.com/sites/richardgendalbrown/2020/02/13/the-five-ingredients-of-blockchaininteroperability/#7d3e7ce558a1 (дата обращения 13.02.2020).

Buterin, V. Chain Interoperability. 2016. URL: https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf (дата обращения: 14.11.2019).

Byzantine fault tolerance (BFT) and Crash fault tolerance (CFT) // Stack Overflow, 2019. URL: https://stackoverflow.com/questions/56336229/byzantine-fault-tolerancebft-and-crash-fault-tolerance-cft (дата обращения: 11.11.2019).

Chainstack. Enterprise Blockchain Protocols: Evolution Index 2020. URL: https://chainstack.com/wp-content/uploads/2020/01/Enterprise-Blockchain-Protocols-Evolution-Index-2020.pdf (дата обращения: 22.01.2020).

ECDSA: (v, r, s), what is v? // Stack Exchange, 2019. URL: https://bitcoin.stackexchange.com/questions/38351/ecdsa-v-r-s-what-is-v (дата обращения: 09.12.2019).

Hash Time Locked Contracts // Bitcoin Wiki. URL: https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts (дата обращения: 04.12.2019).

Hyperledger Burrow. Hyperledger. 2019. URL: https://www.hyperledger.org/projects/hyperledger-burrow (дата обращения: 12.11.2019).

ISO/IEC 17788:2014 Information technology – Cloud computing – Overview and vocabulary. 2014. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en (дата обращения: 10.12.2019).

Interledger Overview. Interledger. URL: https://interledger.org/overview.html (дата обращения: 10.12.2019).

Internet of Value Manifesto. World Wide Web Consortium (W3C). URL: https://www.w3.org/WebCommerce/IG/wiki/Internet_of_Value_Manifesto (дата обращения: 12.12.2019).

Lightning Network Documents. Lightning Network. URL: https://lightning.network/docs/ (дата обращения: 03.12.2019).

Johnson S., Robinson P., Brainard J. Sidechains and interoperability. 2019. URL: https://arxiv.org/abs/1903.04077 (дата обращения: 15.11.2019).

Tendermint. URL: https://docs.tendermint.com/ (дата обращения: 02.12.2019).

The Raft Consensus Algorithm. URL: https://raft.github.io/ (дата обращения: 03.12.2019).

Siris V., Nikander P., Voulgaris S., Fotiou N., Lagutin D., Polyzos G.C. Interledger Approaches. 2019. URL: https://ieeexplore.ieee.org/document/8755830 (дата обращения: 18.11.2019).

Zamyatin A., Al-Bassam M., Zindros D., Kokoris-Kogias E., Moreno-Sanchez P., Kiayias A., Knottenbelt W.J. SoK: Communication Across Distributed Ledgers. 2019. URL: https://eprint.iacr.org/2019/1128.pdf (дата обращения: 14.11.2019).

АВТОРЫ:

Илья Дружинин
R&D-инженер Ассоциации ФинТех, руководитель рабочей группы «Взаимодействие систем распределенного реестра» ТК 159 «Программно-аппаратные средства технологий распределенного реестра и блокчейн»

Анатолий Конкин
Руководитель направления «Развитие технологии распределенного реестра» Ассоциации ФинТех

Александр Чубурков
Руководитель рабочей группы «Интеллектуальные контракты» ТК 159 «Программно-аппаратные средства технологий распределенного реестра и блокчейн»

Петр Каламбет
Системный инженер

Алексей Трошичев
Архитектор платформы Мастерчейн

АНАЛИТИКИ:

Никита Ломов

Юлия Рязанцева

РЕДАКТОР:

Влада Стеканова

ДИЗАЙНЕР-ВЕРСТАЛЬЩИК:

Александра Щедрина

https://t.me/fintechassociation

https://www.fintechru.org

Адрес электронной почты:
masterchain@fintechru.org

Апрель 2020