Практическое применение технологии блокчейн для управления жизненным циклом колесных пар



А.А. Воробьев,
директор ООО «ФИНЭКС Качество», член Комитета по качеству НП «ОПЖТ»



М.П. Парамонов,
руководитель проектов ООО «ФИНЭКС Качество»

Применение технологии блокчейн и реализованных на ней умных контрактов позволяет организовать эффективный, прозрачный и надежный учет железнодорожных изделий на всех стадиях жизненного цикла. Это достигается посредством использования распределенного реестра транзакций, копии которого хранятся на множестве узлов системы, задействования механизма консенсуса, необходимого для внесения изменений (актуализации) в реестр транзакций и применения методов криптографии для защиты от хакерских атак и злонамеренных действий, приводящих к информационным ошибкам.

Зарождение блокчейна

В 2008 году сейчас уже легендарный, но тогда никому еще не известный (остающийся анонимным и до сих пор) Сатоши Накамото опубликовал свою программную статью, в которой изложил концепцию блокчейна (от англ. blockchain – «цепочка блоков»), а уже в 2009 году технология на основе этой концепции была им реализована в качестве платформы криптовалюты – биткоина (Bitcoin).

Многие специалисты считают, что технология блокчейн является вторым после Интернета самым важным изобретением в области информационных технологий.

Постараемся понять, что такого революционного в технологии блокчейн.

До появления блокчейна доминировала так называемая централизованная (серверная) архитектура информационных систем – это когда каждый участник транзакций должен быть связан с центральным узлом системы, на котором осуществляется обработка, хранение и актуализация данных о транзакциях. В этом случае для того, чтобы какому-либо участнику провести транзакцию, необходимо через центральный узел связаться с соответствующим другим участником или участниками. Центральный узел выступает при этом в качестве посредника между участниками транзакции.

Основных недостатков такой централизованной архитектуры три:

1) высокая стоимость обслуживания и повышения производительности центрального узла;
2) подверженность хакерским атакам и информационным ошибкам;
3) возможность выхода из строя всей системы при повреждении центрального узла.

В конце 90-х годов прошлого столетия компанией Nepster (США), специализировавшейся на обмене музыкальными файлами, была реализована так называемая распределенная одноранговая (англ. Pear-to-Pear, P2P) архитектура информационной

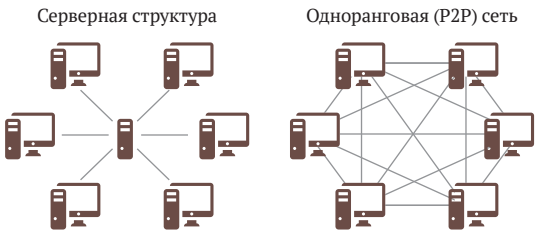


Рис. 1. Централизованная (серверная) и одноранговая архитектуры информационной системы

системы, которая исключала центральный узел, благодаря чему равноправные участники транзакций могли связываться непосредственно друг с другом. На рисунке 1 схематично представлены централизованная (серверная) и одноранговая архитектуры информационной системы.

В блокчейне Сатоши Накамото объединил следующие концепции и технологии, уже существовавшие к тому времени: распределенную одноранговую сеть, технологию связывания отдельных хеш-блоков (от англ. hash[1]) в единую последовательную цепочку, а также механизм доказательства выполненной работы (достижения консенсуса).

Итак, блокчейн позволяет соединенным сетью компьютерам достигать консенсуса по поводу передаваемой информации.

> **Все это время мы обсуждали новые технологии и цифровую экономику. Президент полностью заболел этим. Он прекрасно понимает, что разрыв и значительные темпы роста базируются на цифровой экономике и технологическом лидерстве… В России в данный момент работают над тремя направлениями развития технологии блокчейн: обеспечением «цифровой прослеживаемости товаров», созданием общей платформы на основе блокчейн для идентификации личности и электронной защитой титула собственника… Наше экономическое продвижение вперед и лидерство базируются на возможности технологий. Все, что производит и российский, и мировой интеллект, нами будет применяться.**
>
> **Игорь Шувалов,**
> первый заместитель председателя Правительства РФ,
> панельная сессия ПМЭФ, 2 июня 2017 года

Развитие блокчейна

Базовым элементом блокчейна стал реестр транзакций, представляющий собой необратимую (неизменяемую после добавления) и постоянно добавляемую по результатам консенсуса (специального алгоритма подтверждения выполненной транзакции) цепочку хеш-блоков, распределяемую по всем узлам участников системы.

Реестр транзакций можно представить в виде учетной (бухгалтерской) книги, страницами которой являются отдельные блоки, так же как и страницы в книге пронумерованные и последовательно связанные друг с другом, но только средствами криптографии.

Отличительные особенности блокчейна от иных баз данных заключаются в следующем:

- Весь реестр хранится одновременно у всех участников сети в виде его копий, при этом внести произвольные изменения в реестр ни один из участников сети не может.
- Все транзакции в системе существуют совместно в единой цепочке. Каждый блок, появляющийся в системе, тесно связан с предыдущим. Это исключает возможность внести новые непрошедшие консенсус блоки или взломать сеть в целом.
- Информация в системе шифруется (хешируется) специализированными математическими методами (например, в биткоине применяется криптографический алгоритм SHA-256).
- Прозрачность системы дает возможность каждому ее участнику отследить любую транзакцию, осуществленную в этой системе.

Основных типов сообщений в блокчейне два: это транзакции и блоки, объединяющие транзакции. Транзакции могут инициироваться любыми участниками системы, имеющими необходимый для этого ключ. После того как транзакции инициированы, вступает в действие механизм консенсуса, по результатам которого инициированные транзакции включаются в блоки и после прохождения проверки правильности его формирования добавляются к имеющейся цепочке блоков. Цепочка блоков представляет

[1] Хеширование (англ. hashing) – преобразование массива входных данных произвольной длины в битовую (выходную) строку фиксированной длины, выполняемое определенным алгоритмом. Функция, реализующая алгоритм и выполняющая преобразование, называется хеш-функцией или функцией свертки. Исходные данные называются входным массивом, ключом или сообщением. Результат преобразования (выходные данные) называется хешем, хеш-кодом, хеш-суммой.

Принципы построения блокчейн-технологии

Соединенные компьютеры. Компьютеры объединены в сеть связями по типу «пользователь-пользователь» (peer-to-peer). Каждый компьютер, являющийся частью сети блокчейн, обращается за информацией или за ее подтверждением напрямую к компьютеру другого пользователя сети, а не через централизованный центр.

Достижение соглашения (консенсуса). Достижение соглашения между всеми компьютерами сети возможно благодаря механизмам консенсуса (consensus mechanisms). Это означает следующее: все компьютеры соблюдают незыблемые правила, которые прописаны в программном обеспечении, используемом для доступа к конкретной блокчейн-сети.

Передаваемая информация. То, о чем соглашаются или достигают консенсуса все компьютеры сети, и есть распространяемая информация, или блокчейн. Блокчейн упорядочивает информацию и делает ее более доступной для компьютеров, позволяя группировать огромный объем данных более эффективным образом. Более поздние части информации всегда должны вытекать и соответствовать более ранним, поэтому блокчейн иногда называют неуязвимой системой, справедливость которой поддерживается всеми участниками сети.

собой открытый для всех участников системы и постоянно обновляемый архив данных о всех транзакциях, совершенных в системе.

Каждый блок содержит последовательность из N транзакций и заголовок блока. Заголовок блока включает хеш-значение транзакций блока, а также хеш-сумму на заголовок предыдущего блока. Таким образом, все транзакции в распределенном реестре упорядочены и криптографически (через хеш) связаны между собой. Невозможно изменить данные реестра, не нарушая хеш-ссылки. Хеш-ссылка последнего блока позволяет просмотреть всю цепочку блоков транзакций, созданных ранее, и убедиться в целостности работы системы. На рисунке 2 схематично представлено, как выглядят связанные друг с другом блоки транзакций.

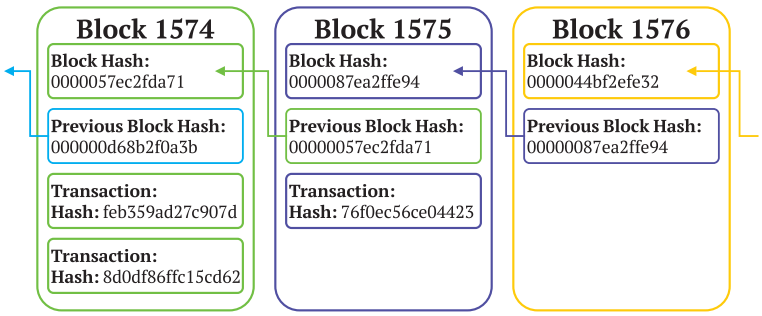


Рис. 2. Связанные друг с другом блоки транзакций

Биткоин, послуживший первым вариантом технологии блокчейн, базируется на публичной распределенной одноранговой сети, в которую может вступать неограниченное число участников, добросовестность которых неизвестна, а значит, степень доверия к ним неопределенна. В связи с этим ключевой задачей, которую надо было решить Сатоши Накамото, выступило обеспечение доверия к системе. В качестве решения им был предложен механизм консенсуса, называемый «Подтверждение выполнения работы» (Proof of Work, PoW). На рисунке 3 представлена схема работы блокчейна с криптовалютой.

Механизм PoW заключается в том, что специальные узлы в сети, называемые майнерами (от англ. mining[2]), работают над вычислением «криптографической головоломки». Это хотя и не сложная задача, решаемая посредством перебора, но она требует серьезных вычислительных мощностей. При этом указанные узлы конкурируют друг с другом. Узел, первым решивший головоломку и получивший подтверждение того, что решение верно (подтверждение выполненной работы), может добавить новый блок транзакций в блокчейн и получить в качестве вознаграждения транш свежедобытой криптовалюты. При этом, если добавление нового блока, то есть решение соответствующей головоломки, требует значительных вычислительных мощностей, проверить правильность решения довольно легко благодаря прозрачности реестра и простоте алгоритма проверки.

Указанный вид консенсуса имеет свои недостатки, на преодоление которых бы-

[2] Майнинг (от англ. mining –«добыча полезных ископаемых») – деятельность по поддержанию распределенной платформы и созданию новых блоков с возможностью получить вознаграждение в форме новых единиц и комиссионных сборов в различных криптовалютах, в частности в биткоинах. Производимые вычисления требуются для обеспечения защиты от повторного расходования одних и тех же единиц, а вознаграждение стимулирует людей расходовать свои вычислительные мощности и поддерживать работу сетей.

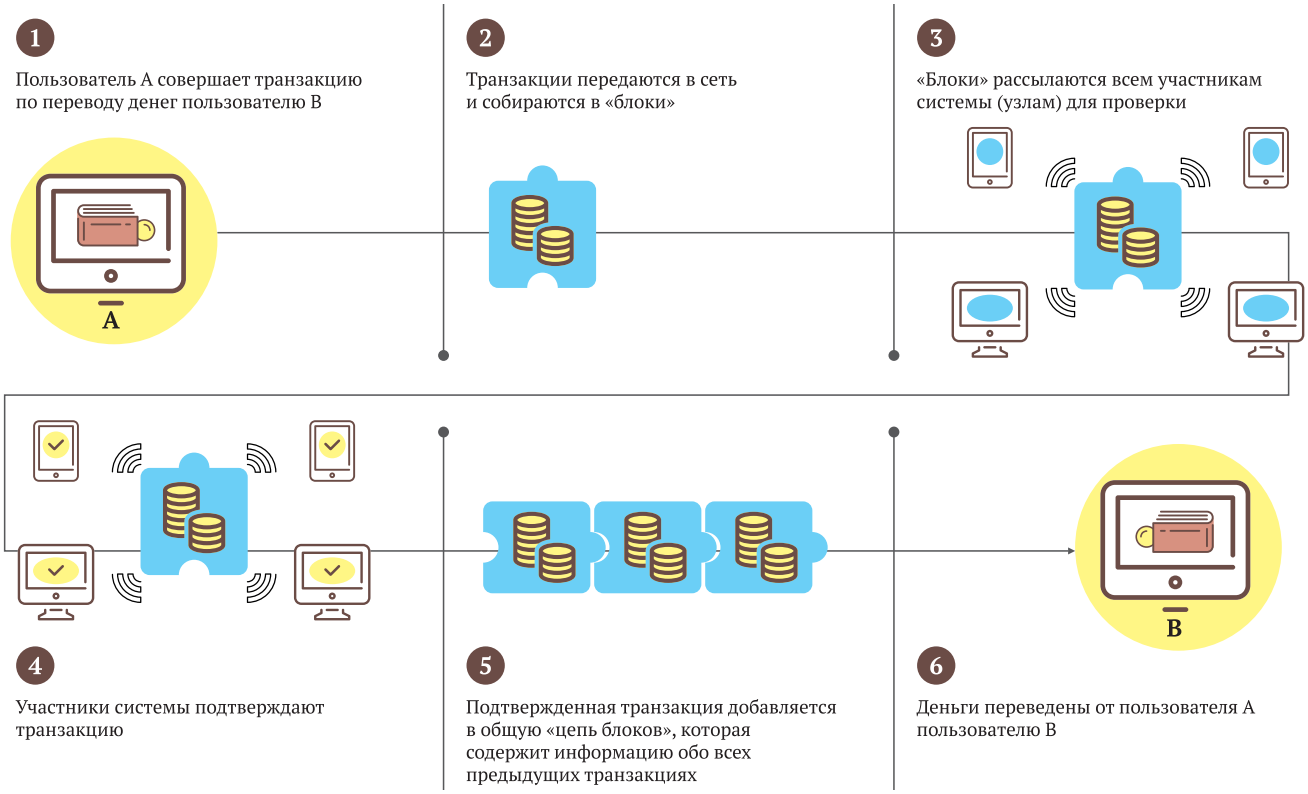


Рис. 3. Схема работы блокчейна с криптовалютой

ли направлены новые виды консенсусов, например «Подтверждение доли» (Proof of Stake), «Арендованное подтверждение доли» (Leased Proof of Stake) и другие, предложенные уже для иных криптовалют, появившихся после биткоина.

После 2012 года многие специалисты задумались о расширении сферы коммерческого применения технологий блокчейна, которые до этого использовались только в качестве платформ для криптовалют. Было очевидно, что блокчейн может также использоваться для хранения любого вида цифровой информации (цифровых активов). И это привело к тому, что блокчейн был добавлен программным кодом, генерирующим «умные контракты» (Smart contract), что позволило найти ему применение в корпоративном сегменте.

Блокчейн: от криптовалют до умных контрактов

«Умные контракты» впервые начали применяться на практике в платформе Ethereum («Эфириум»). Создатель платформы Виталик Бутерин предварительно пришел к выводу, что биткоин плохо подходит в качестве базового протокола под умные контракты, поскольку изначально был спроектирован под другую задачу, и написал в одной из своих программных статей об идее создания такого протокола с нуля.

«Умный контракт» представляет собой программный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн. Основная задача, решаемая «умным контрактом», состоит в полной автоматизации и достоверности исполнения договорных отношений между юридическими и (или) физическими лицами.

На базе «умных контрактов» было сделано множество платформ, на основе которых можно создавать бизнес-приложения под конкретные задачи. Одним из недостатков таких платформ, на наш взгляд, является их открытость (так как большинство

из них базируется на публичных блокчейнах – Bitcoin и Ethereum).

Для целей управления жизненным циклом железнодорожных изделий (в частности, колесных пар) считаем принципиально важным использование такой технологии распределенных реестров, которая дает возможность строить приватные блокчейны, позволяющие группе участников создавать отдельные реестры транзакций, недоступные для других. Мы провели анализ самых распространенных блокчейн-технологий и пришли к выводу, что наиболее подходит для этих целей Hyperlegder Fabric.

Применение Hyperledger Fabric для управления жизненным циклом колесных пар

Hyperledger Fabric представляет собой блокчейн с ограничением прав доступа, имеющий модульную архитектуру и предусматривающий разграничение ролей между узлами, а также настраиваемый консенсус.

О Hyperledger

Hyperledger – блокчейн-консорциум, возглавляемый Linux Foundation, объединяет десятки компаний – мировых лидеров в области финансов, банковского дела, «Интернета вещей», цепочек поставок, производства и технологий. Цель – формирование открытых межотраслевых стандартов для распределенных реестров и технологий с использованием открытого исходного кода. Hyperledger Fabric – один из проектов Hyperledger, являющийся основой для разработки приложений или решений с модульной архитектурой. Летом 2017 года Hyperledger представил код своего распределенного реестра (собственного блокчейна) – Hyperledger Fabric 1.0.[3]

В отличие от публичных блокчейнов без ограничения прав доступа, платформа Hyperledger Fabric предназначена для создания частных (приватных, закрытых) блокчейнов, для чего используется регистрация членов сети Hyperledger Fabric через сервис MSP (Membership Service Provider). Hyperledger Fabric поддерживает работу как сетей, где конфиденциальность (посредством создания каналов) является одним из ключевых эксплуатационных требований, так и сетей, которые сравнительно открыты.

Hyperledger Fabric предлагает разные варианты подключения к сети. Данные реестра могут сохраняться в различных форматах, а механизмы консенсуса могут быть включенными или выключенными (при этом нет потребности в майнинге, что снижает стоимость транзакций). Hyperledger Fabric позволяет выбрать механизм консенсуса, который наилучшим образом учитывал бы отношения, существующие между участниками сети. Hyperledger Fabric поддерживает такие виды консенсусов, как SOLO, Kafka, PBFT, SBFT.

В качестве активов в Hyperledger Fabric могут выступать материальные (товары, недвижимость, оборудование) и нематериальные (контракты и интеллектуальная собственность) активы. Hyperledger Fabric обеспечивает возможность изменять состояние активов с помощью транзакций Chaincode. Активы представлены в Hyperledger Fabric как наборы пар «ключ-значение», при этом изменения состояния активов записываются как транзакции в реестре.

Благодаря возможности координировать операции с колесными парами через единый общий реестр, технология блокчейн способствует сокращению времени, стоимости и риска, связанных с информацией о колесных парах и ее обработкой, одновременно улучшая доверие и прозрачность.

Процесс хранения транзакций в распределенном реестре гарантирует, что записи по операциям с колесными парами будут обновляться только при одобрении транзакций соответствующими участниками жизненного цикла колесных пар.

[3] Узнать больше: https://www.hyperledger.org/

Структура и принципы работы блокчейна колесных пар

Блокчейн колесных пар, на наш взгляд, должен включать следующие ключевые конструктивные характеристики.

Активы (колесные пары)

Активы в виде колесных пар с уникальными идентификаторами представляются как набор пар «ключ-значение» с фиксацией состояния и возможностью его изменения с помощью транзакций путем выполнения цепочных кодов (Chaincode). Активы могут быть представлены в двоичной форме или форме JSON.

Смарт-контракты

Смарт-контракты Hyperledger Fabric программируются в так называемом цепочном коде (Chaincode) и вызываются приложением – внешним по отношению к блокчейну – при взаимодействии клиентского приложения с распределенным реестром.

Chaincode, по сути, является программным обеспечением, определяющим активы (колесные пары) и инструкции (смарт-контракты) для выполнения транзакций, изменяющих состояние активов. С помощью Chaincode осуществляется последовательное обновление информации и выполняется целый ряд функций распределенного реестра (транзакции, запросы, контроль доступа и т. д.). Chaincode может быть реализован на нескольких языках программирования, в том числе популярном Java.

Chaincode обеспечивает соблюдение правил для чтения или изменения информации в базе данных состояний колесных пар. Функции Chaincode инициируются предложением транзакции со стороны клиента, вызываемым соответствующим клиентским приложением. Выполнение Chaincode приводит к набору записей, которые могут быть отправлены в сеть и применены к реестру для всех одноранговых узлов – участников блокчейна колесных пар.

Распределенный реестр колесных пар

Распределенный реестр колесных пар представляет собой проверенную историю всех успешных изменений состояния колесной пары (действительных транзакций) и неудачных попыткок изменить состояние колесной пары (недействительных транзакций), возникающих во время всего жизненного цикла колесной пары.

Распределенный реестр колесных пар создается службой заказа (особый вид узла) как полностью упорядоченный хеш-код блоков (действительных или недействительных) транзакций. Цепочка хешей определяет полный порядок блоков в реестре, при этом каждый блок содержит массив полностью упорядоченных транзакций. В целом это обеспечивает общий порядок всех произведенных транзакций (операций с колесными парами).

Таким образом, мы получаем неизменяемую, упорядоченную и устойчивую к несанкционированному использованию базу, содержащую в закодированном виде всю историю транзакций (операций с колесными парами) и их текущих состояний. Изменение состояния является результатом вызова транзакции, инициированного участвующими сторонами жизненного цикла колесных пар.

Реестр транзакций в Hyperledger Fabric включает два компонента: базу данных состояний и журнал транзакций. База данных состояний описывает состояние реестра в определенный момент времени. Журнал транзакций записывает все транзакции, которые привели к текущему значению базы состояний. Журнал транзакций является неизменяемым, в нем фиксируются значения ключей до и после транзакции, что позволяет восстановить историю обновлений состояний реестра. В большинстве случаев Chaincode взаимодействует только с базой данных состояний, но не с журналом транзакций.

Идентификация

Все участники блокчейна колесных пар имеют идентификаторы. Служба идентификации членства управляет указанными идентификаторами и проверяет подлинность всех участников в сети. Посредством открытого ключа генерируются криптогра-

фические сертификаты, которые привязаны к участникам, сетевым компонентам и клиентским приложениям.

Каждый пользователь приложения должен быть зарегистрирован и зачислен в центр сертификации блокчейна колесных пар, после чего он получает необходимый криптографический ключ (открытый ключ), который используется для аутентификации в сети. Благодаря идентификации участники знают, что все транзакции могут быть обнаружены и прослежены уполномоченными регуляторами и аудиторами.

Конфиденциальность

Hyperledger Fabric предоставляет широкие возможности обеспечения конфиденциальности данных. Во-первых, общая сеть может быть разделена на каналы[4], где каждый канал представляет собой подмножество участников, которым разрешено видеть данные, развернутые только на этом канале.

Во-вторых, в пределах канала можно ограничить входные данные набором подтверждающих узлов (валидаторов), используя настройки видимости. Настройка видимости определит, включены ли входные и выходные данные в отправленную транзакцию, а не только выходные данные.

В-третьих, имеется возможность хешировать или шифровать данные перед вызовом Chaincode. В случае если данные шифруются, необходимо предоставить средства для обмена ключами дешифрования. В-четвертых, можно ограничить доступ к данным определением ролей для участников путем создания контроля доступа в логике цепочки. В-пятых, данные в режиме ожидания могут быть защищены с помощью шифрования на одноранговом узле, а данные в пути – шифрованием посредством протокола TLS (англ. Transport Layer Security).

Каналы

Hyperledger Fabric предусматривает возможность создания каналов, позволяя группе участников вести отдельный реестр транзакций, не доступный для других участников. Это особенно важно для сетей, где некоторые участники могут быть конкурентами, а следовательно, не хотят, чтобы их транзакции, например предложения специальной цены своим контрагентам, были известны каждому участнику сети. В случае если два участника образуют между собой канал, то только у этих участников – и никаких других – имеются в наличии копии реестров транзакций, осуществленных по этому каналу.

Узлы блокчейна

В блокчейне существует три типа узлов:

1. Клиент (отправитель) – участник, который отправляет фактический запрос транзакции подтверждающим узлам (валидаторам) и транслирует транзакционные предложения в службу заказа.

Клиент представляет собой приложение, действующее от имени конечного пользователя. Для связи с блокчейном он должен быть подключен к одноранговому узлу. Клиенты создают и вызывают транзакции.

Клиенты взаимодействуют как с одноранговыми узлами других участников, так и со службой заказа.

2. Одноранговый узел – узел, который совершает транзакции, получает упорядоченные обновления состояний колесных пар в виде блоков из службы заказа и поддерживает состояние и копию реестра.

Реестр колесных пар хранится на всех одноранговых узлах (нодах, англ. node), в качестве которых могут выступать серверы организаций – участников жизненного цикла колесной пары. Это позволяет любому участнику воспроизвести историю всех транзакций и получить информацию об актуальном состоянии колесной пары в любой момент времени.

[4] Канал является частной «подсетью», обеспечивающей связь между двумя или более членами сети с целью проведения конфиденциальных сделок. Канал определяется членами, привязанными одноранговыми узлами, общим реестром и клиентскими приложениями. Транзакция выполняется по каналу, где каждая сторона транзакции должна быть аутентифицирована и уполномочена совершать их по этому каналу. Каждый участник, присоединенный к каналу, имеет свою собственную идентификацию, предоставленную MSP. Все данные, включая транзакцию, информацию об участнике и канале, являются невидимыми и недоступными для любых участников сети, которым не предоставлен доступ к этому каналу.

Одноранговые узлы также могут выполнять специальную функцию одобряющего (подтверждающего) узла или валидатора. Указанная функция осуществляется по отношению к определенному Chaincode и заключается в одобрении транзакции до ее совершения. Каждый Chaincode может устанавливать политику одобрения, которая может ссылаться на набор одобряющих одноранговых узлов. Политика одобрения определяет необходимые и достаточные условия для действительного подтверждения транзакции (как правило, это набор подписей участников).

3. Узел службы заказа – узел, на котором запущена служба заказа, реализующая гарантию доставки транзакции.

Служба заказа предоставляет общий канал связи для клиентов и одноранговых узлов, предлагая услугу по передаче сообщений, содержащих транзакции. Клиенты подключаются к каналу и могут транслировать сообщения на канал, которые затем передаются всем одноранговым узлам. Канал передает одни и те же сообщения всем подключенным одноранговым узлам и выводит их в одном логическом порядке. Переданное сообщение является транзакцией, претендующей на включение в блок транзакций.

Служба заказа может быть реализована по-разному – от централизованной службы до распределенных протоколов, устойчивых к возможным сбоям сети и узлов.

Политика одобрения

Политика одобрения (одобряющая логика) является набором условий для одобрения транзакции. У одноранговых узлов есть предварительно определенный набор политик одобрения, на которые ссылается транзакция, устанавливающая определенный Chaincode. По сути, политика одобрения – это уникальный подход к консенсусу, исключающий необходимость майнинга и обеспечивающий гибкость и масштабируемость, необходимые для участников жизненного цикла колесных пар.

Транзакция объявляется действительной только в том случае, если была согласована в соответствии с политикой одобрения. Вызов транзакции вначале должен получить подтверждение, которое удовлетворяет политике одобрения – в ином случае эта транзакция не будет выполнена. Это происходит путем взаимодействия между отправляющим клиентом и одноранговыми узлами (валидаторами), осуществляющими одобрение.

Например, у валидаторов могут быть заданы «доли» или «вес», общая сумма которых равна 100, а политика одобрения может требовать действительных подписей из набора, в котором имеется большая часть голосов (то есть группа с комбинированной ставкой строго более 50).

Транзакционный поток

1. Инициация (предложение) транзакции.

Для вызова транзакции клиент отправляет сообщение в набор одобряющих одноранговых узлов (валидаторов) в соответствии с политикой одобрения. Например, транзакция может быть отправлена всем валидаторам либо некоторым из них. Необходимо также учитывать, что некоторые валидаторы могут быть в автономном режиме, а одобрить транзакцию могут только доступные валидаторы.

Клиентское приложение, поддерживаемое SDK (англ. Software Development Kit) и использующее один из доступных API (англ. Application Programming Interface), генерирует предложение транзакции. Предложение представляет собой запрос на вызов функции Chaincode, для того чтобы данные могли быть считаны и (или) записаны в реестр (то есть производится запись новых пар ключевых значений для колесной пары). SDK упаковывает предложение транзакции в необходимый формат и использует криптографические учетные данные пользователя для создания уникальной подписи этого предложения транзакции. На рисунке 4 представлена схема инициации (предложения) транзакции.



Рис. 4. Схема инициации (предложения) транзакции

2. Одобрение транзакции

Одобряющие узлы проверяют, что, во-первых, предложение транзакции сформировано корректно; во-вторых, оно не было отправлено в прошлом (защита от повторной записи); в-третьих, подпись клиента действительна и, в-четвертых, клиент имеет право осуществлять выполнение предлагаемой операции с колесной парой.

Одобряющие узлы принимают входные данные предложения транзакции в качестве параметров для вызываемой функции Chaincode. Затем Chaincode выполняется в базе данных текущего состояния для получения результатов транзакции, включая значение ответа, набор чтения и набор записи. В этот момент в реестр не вносятся никакие обновления. Набор этих значений, наряду с подписью одобряющего узла, передается обратно как «ответ на предложение» в SDK, который обрабатывает данные и предоставляет их для использования клиентским приложением. На рисунке 5 представлена схема одобрения транзакции.

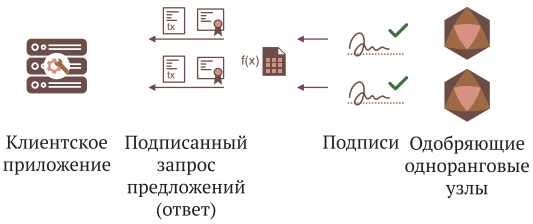


Рис. 5. Схема одобрения транзакции

В соответствии с одобряющей логикой транзакция может быть одобрена или нет, после чего клиенту отправляется соответствующее сообщение.

3. Проверка ответов на предложение транзакции

Клиент ждет, пока не получит достаточное количество сообщений и их подписей, чтобы заключить, что предложение о транзакции одобрено. Этот процесс может включать в себя один или несколько раундов взаимодействия с валидаторами. Точное число зависит от политики одобрения. В случае если политика одобрения выполнена, транзакция одобряется. Сбор подписанных сообщений от одобряющих одноранговых узлов, которыми устанавливается, что транзакция одобрена, называется подтверждением. Если клиенту не удается получить подтверждения предложенной транзакции, он отказывается от этой транзакции с возможностью повторить попытку позже.

Приложение клиента проверяет подписи валидаторов и сравнивает ответы на предложенную транзакцию в целях подтверждения, что они одинаковые. В случае если клиентское приложение намерено передать транзакцию службе заказа для обновления реестра колесных пар, приложение перед отправкой определяет, была ли выполнена указанная политика одобрения.

В случае одобрения служба заказа предоставляет транзакцию всем одноранговым узлам. Служба заказа обеспечивает, чтобы все одноранговые узлы имели одно и то же состояние колесных пар. Это гарантируется получением всеми одноранговыми узлами идентичной последовательности событий, которые зафиксируют одну и ту же последовательность транзакций и, таким образом, обновят свое состояние.

4. Клиент собирает подтверждения в транзакцию

Приложение «транслирует» предложение транзакции и ответы в «сообщении транзакции» службе заказа (рис. 6). Транзакция будет содержать наборы для чтения (записи), подтверждающие подписи узлов и идентификатор канала. Службе заказа не требуется проверять весь контент транзакции – она просто получает транзакции со всех каналов в сети, упорядочивает их хронологически и формирует блоки транзакций.

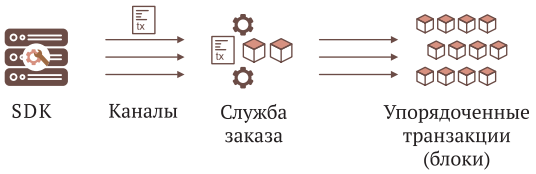


Рис. 6. Схема формирования блоков транзакций

5. Фиксация подтвержденной транзакции

Блоки транзакций доставляются всем узлам – участникам блокчейна колесных пар (рис. 7). Транзакции в блоке проверяются на предмет соответствия политики одобрения и обеспечения того, чтобы не было несанкционированных изменений в

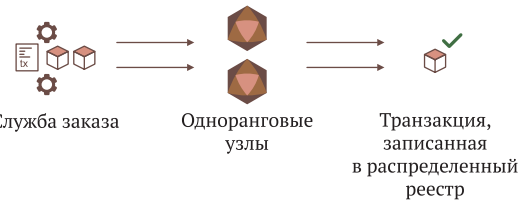


Рис. 7. Служба заказа транслирует блоки транзакций всем узлам

состоянии реестра. Транзакции в блоке будут отмечены как действительные или недействительные.

6. Обновление распределенного реестра

Каждый узел добавляет блок в цепочку канала, и каждая одобренная транзакция записывается в текущей базе данных состояний колесных пар. При этом генерируется событие для уведомления клиентского приложения о том, что транзакция была присоединена к блокчейну колесных пар, а также сообщение о том, была ли транзакция подтверждена или признана недействительной.

Заключение

В настоящей публикации мы представили краткий обзор технологии блокчейн и возможные варианты ее применения для управления жизненным циклом железнодорожной техники, в том числе колесных пар грузовых вагонов. Уверены, что технология блокчейн и ее реализация на платформе Hyperledger Fabric поможет решить задачи идентификации и прослеживаемости подвижного состава, узлов и компонентов, а также исключит использование контрафактных изделий и комплектующих.

Дальнейшим шагом будет создание автоматизированных систем управления жизненным циклом железнодорожной техники на основе технологии блокчейн. В настоящее время ведется разработка технических требований к таким системам, в частности для мониторинга эксплуатации колесных пар грузовых вагонов (при участии ПКБ ЦВ ОАО «РЖД» и АО «ОМК») и тормозного оборудования грузовых и пассажирских вагонов (при участии Ассоциации «АСТО» и ОАО «МТЗ ТРАНСМАШ»).

Запуск в эксплуатацию таких систем позволит фиксировать (документировать с записью в неизменяемый распределенный реестр) все события, происходящие с оборудованием подвижного состава в эксплуатации и при производстве обслуживания и ремонтов. Такое решение обеспечит не только надежную защиту необходимых корпоративных данных, но и приведет к повышению прозрачности, надежности и экономической эффективности транзакций с узлами и компонентами железнодорожного подвижного состава. Тем самым будет создана единая доверительная информационная среда всех участников жизненного цикла: производителей подвижного состава, ремонтных, эксплуатационных компаний и надзорных органов.

Список использованной литературы

1. Дрешер Д. Основы блокчейна. – М. : ДМК, 2018. – 311 с.
2. Википедия: Хеширование. URL: https://ru.wikipedia.org/wiki/. (Дата обращения: 15.01.2018).
3. Тестова А. «Алгоритмы консенсуса»: Подтверждение доли и доказательство работы. URL: https://habrahabr.ru/company/bitfury/blog/327468/. (Дата обращения: 15.01.2018).
4. Manav Gupta. Blockchain for dummies. IBM Limited Edition, 2017. – 51 p.
5. Блокчейн. URL: www.tadviser.ru/index.php/Blockchain. (Дата обращения: 15.01.2018).
6. Википедия: Майнинг. URL: https://ru.wikipedia.org/wiki/. (Дата обращения: 15.01.2018).
7. Kostarev G. Review of blockchain consensus. URL: https://blog.wavesplatform.com/review-of-blockchain-consensus-mechanisms-f575afae38f2 (Дата обращения: 15.01.2018).
8. Википедия: Смарт-контракт. URL: https://ru.wikipedia.org/wiki/. (Дата обращения: 15.01.2018).
9. Key concepts of Hyperledger Fabric. URL: http://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html. (Дата обращения: 15.01.2018).

О подготовке технических требований на разработку Единой автоматизированной базы данных колесных пар с использованием технологии блокчейн

В настоящее время на площадке НП «ОПЖТ» планируется создание единой автоматизированной базы данных колесных пар и организации автоматизированного учета элементов и пробега колесных пар грузовых вагонов в соответствии с решением Протокола совещания под председательством президента НП «ОПЖТ» В.А. Гапановича от 18.07.2017 № 4/17.

В соответствии с Протоколом от 27.11.2017 совместного заседания комитетов НП «ОПЖТ» по грузовому подвижному составу, по координации производителей в металлургическом комплексе и по нормативно-техническому обеспечению и стандартизации ПКБ ЦВ ОАО «РЖД» разрабатывает технические требования на разработку Единой автоматизированной базы данных колесных пар, обеспечивающей идентификацию составляющих основных элементов и самой колесной пары с использованием пассивных радиочастотных меток с данными (RFID метки), защищенными по технологии блокчейн.

Использование технологии блокчейн с применением RFID-меток позволит производителям колес и буксовых узлов кассетного типа получать объективные данные с высокой достоверностью о надежности их работы на протяжении всего жизненного цикла.

Для компаний – операторов подвижного состава технология блокчейн предоставит возможность оперативного обмена, приобретения и перемещения колесных пар грузовых вагонов.

Блокчейн колесных пар позволит сохранять информацию о производстве колесных пар и их элементов, вести учет пробега и всех операций с колесной парой на протяжении всего срока ее службы. Также будут реализованы механизмы контроля над перемещением, хранением и учетом колесных пар, обращаемых на территории СНГ и сопредельных государств.

На основе технологии блокчейн можно построить гибридную систему мониторинга колесных пар, включающую следующие элементы:

1. «Традиционная» централизованная (серверная) СУБД предназначена для хранения технического паспорта колесной пары (включает и паспорта ее элементов).

2. Блокчейн колесных пар предназначен для записи и отслеживания через умные контракты изменений состояния колесной пары с фиксацией всех событий, происходящих с ней в течение жизненного цикла, то есть от момента ее изготовления (первое формирование) до момента исключения в металлолом:

- формирование (первое и последующие);
- пересылка (транспортировка);
- хранение;
- постановка под вагон;
- изъятие из-под вагона;
- производство плановых и внеплановых видов ремонта;
- участие в экстремальных событиях (крушения, аварии, сходы);
- исключение из инвентаря.

Благодаря технологии блокчейн каждая транзакция (операция с колесной парой) будет связана с журналом транзакций, реестром состояний и с техническим паспортом, хранимым и актуализируемым в СУБД.

А.А. Казаков,
заместитель директора ПКБ ЦВ ОАО «РЖД»