

*Меркулов Андрей Вячеславович*¹,
студент магистратуры;
*Ефремов Артём Александрович*²,
доцент, канд. физ.-мат. наук, доцент

МИНИМИЗАЦИЯ РАСХОДУЕМОГО МЕСТА В ХРАНИЛИЩЕ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ БЛОКЧЕЙН

^{1,2} Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого;

¹ Россия, Санкт-Петербург, ООО «Отраслевой центр разработки и внедрения информационных систем» (ООО «ОЦРВ»);

¹ andrew.merkulov2011@yandex.ru, ² artem.efremov@spbstu.ru

Аннотация. Тема этой работы: «Минимизация расходуемого места в хранилище данных при использовании технологии блокчейн». Данная работа посвящена изучению технологии блокчейн и минимизации расходуемого места в хранилище данных при использовании данной технологии. В результате исследования будет разработан Proof of Concept блокчейн, который будет использовать меньше дискового пространства для хранения блоков, чем имеющиеся готовые решения.

Ключевые слова: минимизация, блокчейн, уменьшение дискового пространства, Hyperledger Fabric, Proof of Concept.

*Andrey V. Merkulov*¹,
Master's Student;
*Artem A. Efremov*²,

Candidate of Physical and Mathematical Sciences, Associate Professor

MINIMIZATION OF WASTE SPACE IN THE DATA STORAGE WHEN USING BLOCKCHAIN TECHNOLOGY

^{1,2} Peter the Great St. Petersburg Polytechnic University,
St. Petersburg, Russia;

¹ LLC “Industry Center for the development and implementation of information systems”, St. Petersburg, Russia;

¹ andrew.merkulov2011@yandex.ru, ² artem.efremov@spbstu.ru

Abstract. The topic of this work: “Minimization the space consumed in the data warehouse when using blockchain technology.” This work is devoted to the study of blockchain technology and minimization of the consumed space in the data warehouse when using this technology. As a result of the study, a Proof of Concept blockchain will be developed that will use less disk space to store blocks than existing ready-made solutions.

Keywords: minimization, blockchain, disk space reduction, Hyperledger Fabric, Proof of Concept.

Введение

К основным применениям технологии отнесены трансграничные платежи и расчеты, торговое финансирование и транзакционные расчеты.

По словам аналитиков, компании, использующие технологию блокчейн, уже в первые месяцы пандемии COVID-19 ощутили ее преимущества. Как утверждается, она «помогла предприятиям во многих отраслях промышленности преодолеть трудности, связанные с управлением цепочками поставок, проверкой медицинских данных и отслеживанием страховых требований».

1. Постановка задачи и теоретическая часть

Блокчейн — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока. Изменение любой информации в блоке изменит его хеш-сумму. Чтобы соответствовать правилам построения цепочки, изменения хеш-суммы нужно будет записать в следующий блок, что вызовет изменения уже его собственной хеш-суммы. При этом предыдущие блоки не затрагиваются. Если изменяемый блок последний в цепочке, то внесение изменений может не потребовать существенных усилий. Но если после изменяемого блока уже сформировано продолжение, то изменение может оказаться крайне трудоёмким процессом. Дело в том, что обычно копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.

Hyperledger Fabric — блокчейн платформа, предназначенная для построения бизнес приложений уровня предприятия. Hyperledger Fabric был изначально стартован Digital Assets и IBM.

Hyperledger Fabric создавался корпорацией для корпораций, поэтому в него «пускают по билетам». Участник сети должен получить сертификат и быть идентифицирован. Разным участникам могут быть предоставлены разные права, ограничения и привилегии.

В Fabric есть три основных типа участников блокчейна:

– **Клиенты (client / committing peers)**. Конечные пользователи, которые могут совершать транзакции.

– **Узлы (peers)**. Этот тип управляет транзакциями. К ним также относится специальный тип узлов поручителей (**endorsers**), которые проверяют, удовлетворяет ли транзакция необходимым требованиям.

– **Сервисные узлы (orderers from ordering service)**. Они формируют блоки транзакций и добавляют их в блокчейн. Кроме того, они обрабатывают все конфигурационные транзакции по настройке сети.

В HLF нет токенов, что также крайне важно для корпоративного использования. Ведь предприятие не спрячешь от налоговиков, правоохранителей и прочих чиновников — ему приходится трудиться в правовом поле. А с законодательным урегулированием оборота криптовалют в мире обстановка далеко не самая благоприятная. Где-то их легализовывают, где-то пытаются запрещать, где-то еще думают, как с ними быть. Так что отсутствие токена для корпоративного блокчейна сейчас — очевидный плюс. Снимает много хлопот по подгонке работы сети в каждой конкретной юрисдикции [4].

Зато в HLF есть смарт-контракты, называемые в данной сети чейн-кодами. Для программирования смарт-контрактов в HLF используется язык GO (Golang) и предусмотрена поддержка Java и Javascript. Приятный момент, ведь для написания смарт-контрактов на Ethereum приходится осваивать специальный внутренний язык виртуальной машины Ethereum [9].

Отсутствие токенов не означает невозможность организации обмена активами — HLF позволяет хранить информацию о физическом имуществе и обязательствах. Благодаря этому механизму работает, например, торговая платформа Batavia, помогающая отслеживать и оплачивать транспортировку и поставку партий товаров по всему миру по мере прохождения ими каждого этапа.

Проблема при использовании готовых решений с блокчейн технологией, состоит в том, что большая часть дискового пространства, занимаема данными, записанными в блоки, используется для хранения метаданных, сертификатов и подписей участников.

Постановка задачи: Необходимо проанализировать работу нескольких готовых решений, например Hyperledger Fabric, понять причины использования такого количества метаданных и придумать возможность уменьшить этот объем без потери функционала по проверке неизменности и неотчуждаемости данных.

2. Proof of Concept (PoC) блокчейн

С имеющимися результатами исследования можно разработать Proof of Concept блокчейна, который будет использовать меньше дискового пространства для хранения блоков, чем имеющиеся готовые решения.

Proof of Concept блокчейн — это метод выяснения того, осуществим ли конкретный проект блокчейна в реальной ситуации. Процесс направлен на проверку того, имеет ли первоначальная идея потенциал и будет ли она работать должным образом. Доказательство концепции может быть реализовано как прототип проекта или как минимально жизнеспособный продукт.

Можно выделить три наиболее важные причины, по которым стартапы и предприятия выбирают Proof of Concept блокчейн:

- Тестирование блокчейн-проекта перед запуском в серийное производство.
- Выявление болевых точек, которые могут привести к будущим рискам при реализации проекта.
- Экономия времени и снижение затрат.
- Доказательство концепции не только не позволяет вам инвестировать в потенциально неосуществимые проекты, но также помогает реализовать наилучшую версию вашей идеи с учетом ваших требований и возможностей.

Реализация данного блокчейна подразделяется на 3 шага:

- поиск подходящих секторов применения блокчейна, которые представляют ценность: финансы, страхование, поставки, правительство, медицина, интернет вещей, идентификация, управление активами, платежи;

- фаза планирования продукта блокчейна

Требования к функциям блокчейна;

Измерение ключевых показателей;

Согласование с заинтересованными сторонами;

- исследование технологии

Идентификация протокола блокчейна;

Определение архитектуры управления.

Заключение

Блокчейн PoC эффективно выявляет болевые точки проекта. Однако это также может показать, что проект совершенно неосуществим. При этом можно прийти к выводу, что развитие блокчейна пока нельзя осуществить. Несмотря на результат, проверка концепции блокчейна неизбежна для любой организации, стремящейся внедрить блокчейн.

Список литературы

1. Peters G.W., Efstathios P. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money // Banking Beyond Banks and Money. – Springer, Cham, 2016. – Pp. 239–278.

2. Ekblaw A., et al. A case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data // Proceedings of IEEE Open & Big Data Conference, 2016.

3. Samaniego M., Ralph D. Using blockchain to push software-defined IoT components onto edge hosts // Proceedings of the International Conference on Big Data and Advanced Wireless Technologies. – ACM, 2016.

4. Muneeb A., et al. Blockstack: A global naming and storage system secured by blockchains // USENIX Annual Technical Conference, 2016.

5. Яковлева Е.Ю., Сергеев И.В. Обзор технологии блокчейн в качестве инструмента таможенного администрирования // Молодой ученый. – 2017. – № 20. – С. 301–304. [Электронный ресурс]. – URL: <https://moluch.ru/archive/154/43535/> (дата обращения: 16.10.2018).
6. Zyskind G., Nathan O. Decentralizing privacy: Using blockchain to protect personal data // Security and Privacy Workshops (SPW), 2015.
7. Vorick D., Champine L. Sia: simple decentralized storage // Security and Privacy Workshops (SPW), 2014.
8. Christidis K., Devetsikiotis M. Blockchains and smart contracts for the internet of things // Ieee Access. – 2016 – Vol. 4. – Pp. 2292–2303.
9. Kosba A. et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts // 2016 IEEE symposium on security and privacy (SP). – IEEE, 2016. – С. 839–858.
10. Воронов М.П., Часовских В.П. Blockchain – основные понятия и роль в цифровой экономике // Современные проблемы науки и образования. – 2017. – №. 9–1. – С. 30–35.
11. Соколова Т.Н., Сыксин В.В. Управление децентрализованными системами с помощью технологии blockchain // Информационная безопасность регионов. – 2017. – № 1 (26).