УДК 004.738

ЗАЩИТА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ (IOT) С ПОМОЩЬЮ БЛОКЧЕЙН-ФРЕЙМВОРКА HYPERLEDGER FABRIC

Гаранин Н.А., Белов Ю.С.

ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана», филиал, Калуга, e-mail: fn1-kf@mail.ru

Данная статья посвящена вопросу защиты IoT и оценки блокчейн-фреймворка Hyperledger Fabric. Интернет вещей (IoT) стал неотъемлемой частью жизни человека. С ростом популярности данной технологии возрастает её уязвимость и риск эксплуатации. Проблемы безопасности привели к возникновению дополнительных проблем, таких как совместимость и вычислительная мощность устройств интернета вещей. Для решения вопросов безопасности используется технология блокчейн, из-за ее безопасного дизайна и децентрализации. В качестве решения безопасности IoT рассмотрен фреймворк Hyperledger, а также основные компоненты, обеспечивающие работу Hyperledger Fabric. В этом исследовании проводится оценка структур Blockchain и Hyperledger, защищающих устройства интернета вещей. Основное внимание уделяется рассмотрению структуры взаимодействия данного фреймворка с интернетом вещей и безопасностью в целом. Транзакционные отношения между участниками сети должны оставаться конфиденциальными и невидимыми для всех. Это стало возможным благодаря функции «каналы» в структуре Hyperledger. Hyperledger является разрешенным блокчейном, который имеет конфиденциальность и целостность, встроенные в дизайн. Данная технология организует полную изоляцию транзакций и личных данных. При совместном использовании хэшей в качестве доказательств транзакций личные данные могут быть переданы участникам «коллекции» или конкретной организации на основе конфиденциальности данных.

Ключевые слова: блокчейн, интернет вещей, Hyperledger Fabric, безопасность

INTERNET OF THINGS (IOT) DEVICE PROTECTION USING THE HYPERLEDGER FABRIC BLOCKCHAIN FRAMEWORK

Garanin N.A., Belov Yu.S.

Bauman Moscow State Technical University, Kaluga branch, Kaluga, e-mail: fn1-kf@mail.ru

This article is devoted to the issue of IoT protection and evaluation of the Hyperledger Fabric blockchain framework. The Internet of Things (IoT) has become an integral part of human life. With the growing popularity of this technology, its vulnerability and the risk of exploitation increases. Security issues have led to additional issues, such as compatibility and computing power of Internet of Things devices. Blockchain technology is used to solve security issues, because of its secure design and decentralization. As an IoT security solution, the Hyperledger framework is considered, as well as the main components that ensure the operation of Hyperledger Fabric. This study evaluates the Blockchain and Hyperledger structures that protect IoT devices. The main attention is paid to the structure of the interaction of this framework with the Internet of Things and security in general. Transactional relationships between network participants should remain confidential and invisible to everyone. This was made possible thanks to the «channels» function in the Hyperledger structure. Hyperledger, is an authorized blockchain that has privacy and integrity built into the design. This technology organizes the complete isolation of transactions and personal data. When hashes are shared as proof of transactions, personal data can be transferred to the participants of the «collection» or a specific organization based on data confidentiality.

Keywords: blockchain, Internet of Things, Hyperledger Fabric, security

Интернет вещей (IoT) относится к широкому спектру интеллектуальных объектов, объединенных в одну большую сеть и связанных интернетом. Данные объекты состоят из датчиков и микроконтроллеров, которые собирают и обрабатывают информацию из окружающей среды и обеспечивают работу их функций с помощью встроенного программного обеспечения. Объектами интернета вещей можно считать носимые устройства, умный дом, умный город, системы здравоохранения, транспорт, промышленность. Из-за роста охвата интернета вещей возникает проблема взаимосвязанности устройств и, как следствие, образуются проблемы с безопасностью и защитой конфиденциальности. Ученые прогнозируют, что в 2025 г. в IoT будет включать более 40 млрд устройств, которые будут генерировать более 75 млрд зеттабайт данных.

Цель исследования: рассмотреть способы решения вопросов безопасности для объектов интернета вещей, взаимодействующих со структурами Blockchain и Hyperledger Fabric.

Описание модели. Объекты интернета вещей разделены на пятислойную пирамиду, как показано на рис. 1. Устройства пятого уровня содержат небольшой объем памяти, ограниченные вычислительные мощности и, следовательно, более подвержены риску кибер-атак и взломов [1].

В пирамиде интернета вещей на верхнем уровне находятся облачные серверы, это централизованные системные контроллеры, принадлежащие третьим сторонам, таким как Microsoft, Amazon, IBM. Структура IoT

в основном зависит от архитектуры централизованного облачного сервера, от способа хранения данных, аутентификации, связи и любых других дополнительных услуг. Использование централизованных решений интернета вещей сопряжено с проблемами безопасности и доверия, поскольку пользователи должны доверять надлежащей обработке данных и исключению публичного доступа к данным.

Уязвимости в системе безопасности объектов интернета вещей при совместном использовании могут привести к сбоям. Примером такого сбоя может послужить случай, произошедший в феврале 2020 г. Была произведена распределенная атака типа «Отказ в обслуживании» (DDoS) против критически важного коммерческого публичного облака, Amazon Web Services, в результате которой были отключены множество сервисов. Эти типы атак становятся все более частыми, и их трудно исправить, так как трудно определить, какая из систем неисправна, в некоторых случаях злоумышленники используют каналы связи или пароли по умолчанию.

Достижения в области информационно-коммуникационных технологий способствовали эволюции традиционной компьютерной индустрии в интеллектуальную индустрию, основанную на принятии решений на основе данных [2]. Во время этого сдвига парадигмы интернет вещей (IoT) играет важную роль в подключении физической промышленной среды к киберпространству вычислительных систем, в результате чего формируется Киберфизическая система (CPS). IoT может поддерживать широкий спектр промышленных приложений, таких как производство, логистика, пищевая промышленность и коммунальные услуги. IoT нацелен на повышение эффективности работы и производительности производства, сокращение времени простоя оборудования и повышение качества продукции. В частности, IoT обладает следующими особенностями:

1) децентрализация систем IoT;
2) разнообразие устройств и систем IoT;
3) неоднородность данных IoT;
4) сложность сети.

Рис. 1. Пятислойная пирамида

Все они приводят к проблемам, включая неоднородность системы интернета вещей, плохую совместимость, ограниченность ресурсов устройств интернета вещей, уязвимость конфиденциальности и безопасности.

Существующие проблемы в IoT могут быть решены с помощью децентрализованных архитектур, которым присущи безопасность и конфиденциальность. К таким архитектурам можно отнести Blockchain и Hyperledger [3]. При их применении к устройствам интернета вещей может обеспечиться повышение конфиденциальности и целостности по сравнению с нынешними подходами.

Технология Blockchain. Блокчейн – это децентрализованный распределенный и прозрачный глобальный реестр записанных данных, защищенный от несанкционированного доступа, позволяющий хранить любые цифровые активы. Данные цепочки стали популярными в 2008 г. в связи с появлением биткоина и криптовалют [4]. В современных блокчейн-технологиях, таких как Ethereum, они используют смарт-контракты, которые представляют собой программируемый код, который может выполняться без участия третьих сторон.

Благодаря децентрализации блокчейны могут обеспечить выполнение транзакции и проверку в распределенной системе, которой не проверяются друг другом, без вмешательства доверенной третьей стороны. В отличие от существующих систем управления транзакциями, в которых централизованное управление должно проверять транзакции, блокчейны могут обеспечивать децентрализованную проверку транзакций, тем самым значительно экономя затраты и снижая узкое место в производительности центрального агентства. Более того, каждая транзакция, сохраненная в блокчейнах, по сути, неизменна, поскольку каждый узел в сети хранит все зафиксированные транзакции в блокчейне.

В блоки записывают данные и дублируют их по распределенной сети, новые записи транзакций добавляются в конец коллекции, каждая запись данных сохраняется в виде блока, который связан со следующим набором данных, создающим блокчейн. Цепочки блоков поддерживаются и проверяются участниками сети, называемой узлами.

Распределение блокчейн-регистров по узлам обеспечивает прозрачность, поскольку используется одна и та же информационная цепочка по всей сети. Участвующие узлы в сети выполняют проверку достоверности добавленных блоков в сети, принимая и отклоняя записи, используя методы проверки набора, известные как механизмы консенсуса. Механизмы консенсуса – это криптографические алгоритмы, используемые для обеспечения правильного упорядочения транзакций в блоках.

Блокчейн использует одноранговую сеть (P2P) в качестве своей сетевой архитектуры, которая удовлетворяет цели децентрализации цепочки данных. В P2P-сети участники могут обмениваться информацией и общаться без необходимости какого-либо центрального управления. Участникам блокчейна выделяются ключи, которые генерируются криптографически, в отличие от систем учетных данных для входа в централизованных архитектурах [5]. Функция криптографии предоставляет адрес блокчейна и код закрытого ключа, которые специфичны только для этого пользователя, обеспечивая пользователям анонимность, поскольку ни один код ключа не похож, и трудно связать адрес с участником.

Каждый блок содержит заголовок блока, в котором уникальный хэш, называемый корнем, идентифицирует текущий блок, хэш для предыдущего блока и список транзакций с новыми транзакциями также находится в блоке. Блоки будут содержать одинаковое количество транзакций в структуре данных. Однако у разных пользователей будут разные транзакции. Для удобства идентификации разным блокам при создании выдается временная метка, которая обычно отличается. Блок зарождения – это первый блок в цепи, все предыдущие блоки которого связаны с предыдущими. В некоторых случаях существуют блоки, которые могут ссылаться на одного и того же предшественника, если они созданы примерно в одно и то же время, это называется разветвлением, как показано на рис. 2.

Фреймворк Hyperledger. Hyperledger – это проект с открытым исходным кодом, созданный для работы с технологией блокчейн, который предоставляет несколько отличных платформ для работы с межотраслевыми реестрами [6]. IBM и другие компании поддерживают проект Hyperledger. На 2021 г. Hyperledger объединяет шесть различных распределенных реестров.

Активные на данные момент:

– Hyperledger Fabric – технология распределенного регистра корпоративного уровня с поддержкой конфиденциальности.

– Hyperledger Besu – Ethereum на базе Java.

– Hyperledger Sawtooth – основной участник – Intel, работающий над настройкой протоколов.

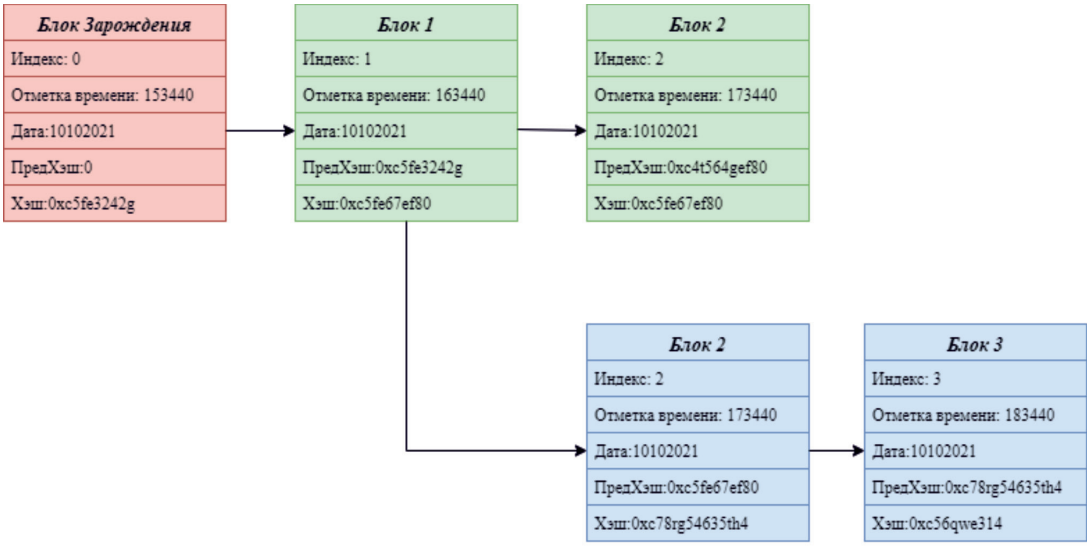

Рис. 2. Иллюстрация простой блокчейн-цепочки

В планах:

– HyperledgerBurrow–смарт-контрактов.

– Hyperledger Indy – инструмент и библиотека для запуска независимых идентификаций в распределенных реестрах.

– Hyperledger Iroha – ориентирован на мобильные приложения и имеет ту же кодовую базу, что и Fabric.

Hyperledger также предоставляет список инструментов и библиотек, которые можно использовать с различными платформами. Основными инструментами в проекте Hyperledger, которые представляют интерес для работы с IoT, а в частности с блокчейн, являются:

– Hyperledger Cello – этот инструмент помогает обеспечить проверку производительности развернутого блокчейна с помощью набора сценариев.

– Hyperledger Caliper – этот инструмент помогает развертывать решения в блокчейн-системах, что приводит к сокращению объема работы за счет предоставления автоматизированных способов создания, завершения и управления цепочками блоков.

– Hyperledger Explorer – с помощью этого инструмента можно вызывать, развертывать и запрашивать блоки.

Блокчейн Hyperledger Fabric. Данная технология объединяет набор узлов в организации, которые создают сеть, взаимодействующую с внешними приложениями. Организации рассматриваются как участники, которые являются частью блокчейн-сети. Каждая организация идентифицируется по идентификатору Membership Service Provider (MSP), который управляет тем, как новым членам могут выдаваться цифровые подписи и проверяться [5]. Организации могут быть разных масштабов. Однако эти предприятия должны быть организациями, не являющимися заказчиками в сети блокчейна. Организация транзакций в сети Hyperledger fabric представлена на рис. 3.

Узлы в сети управляются поставщиком услуг (MSP) [7], который действует как менеджер идентификации, предоставляя действительные цифровые подписи. Узлы в сети блокчейн можно разделить на три группы:

– *Клиенты* – веб-приложения, мобильные приложения, наборы для разработки программного обеспечения, которые взаимодействуют с сетью, отправляя запросы на выполнение транзакций и запрашивая порядок транзакций. Однако цепной код работает за пределами блокчейн-цепочки, взаимодействуя с узлами, а также с децентрализованным, распределенным, глобальным реестром.

– *Одноранговые узлы* – они ведут реестр блокчейна и выполняют цепной код. Существует два типа одноранговых узлов привязки и одноранговых узлов поддержки. Одноранговые узлы поддержки обрабатывают утверждение транзакций в соответствии с запросами. Узлы привязки определяются при создании сети, и они обеспечивают связь между различными организациями в сети, обмениваясь данными между соответствующими предприятиями.

– *Заказчик* – создает логический порядок транзакций, упаковывая их в блоки, а затем передавая в общую сеть. Заказчики отличаются от одноранговых узлов и существуют как совокупность узлов, которые заказывают транзакции по принципу FIFO «первым пришел – первым вышел».

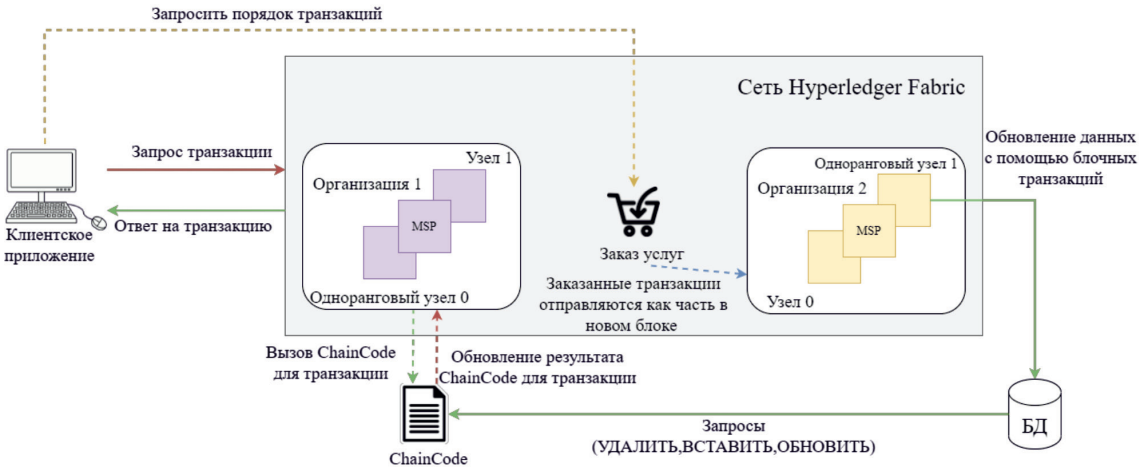

Рис. 3. Организация транзакций в сети Hyperledger fabric

Узлы в сети могут взаимодействовать друг с другом с помощью каналов, это частный и безопасный способ, который гарантирует, что узлы могут отправлять сообщения и блоки без вмешательства извне. В одной сети может быть несколько каналов между различными организациями и одноранговыми узлами для повышения конфиденциальности, добавление к каналу осуществляется с помощью MSP.

Блокчейн при применении к устройствам IoT может обеспечить повышение конфиденциальности и целостности по сравнению с нынешними подходами. Hyperledger Fabric, являющаяся разрешенным блокчейном, по своей сути имеет конфиденциальность и целостность, включающие дизайн [8]. Данная технология может быть интегрирована с различными устройствами интернета вещей.

Заключение

Таким образом, Hyperledger Fabric – это частный блокчейн, который предлагает решения для безопасного управления доступом и ведения реестра для объектов IoT. Структура Hyperledger по своей конструкции использует протоколы шифрования, политики доступа и криптографических функций, которые защищают от вредоносных атак. С помощью этого средства могут быть реализованы механизмы контроля доступа, а также может быть обеспечена конфиденциальность пользователей, поскольку центр сертификации использует открытый и закрытый ключи, защищающие личность пользователя.

Таким образом, можно сделать вывод о том, что представленные технологии достаточно эффективны для решения вопросов безопасности в IoT.

Список литературы

1. Ганкин Н.М., Михейлис Д.А. Hyperledger – инструментарий разработки отраслевых блокчейнов // Juvenis scientia. 2018. № 4. С. 17–19.

2. Вишняков В.А. Организация интернет-маркетинга с использованием интеллектуальных и блокчейн-технологий // Системный анализ и прикладная информатика. 2020. № 1. С. 18–23.

3. Ray P.P. A survey on Internet of Things architectures. Journal of King Saud University – Computer and Information Sciences. 2018. Vol. 30. No. 3. P. 291–319.

4. Ali M.S., Vecchio M., Pincheira M., Dolui K., Antonelli F., and M.H. Rehmani, Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 2. P. 1676–1717.

5. Lade P., Ghosh R., Srinivasan S. Manufacturing Analytics and Industrial Internet of Things. IEEE Intelligent Systems. 2017. Vol. 32. No. 3. P. 74–79.

6. Kang J., Yu R., Huang X., Wu M., Maharjan S., Xie S., Zhang Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal. 2019. Vol. 6. No. 3. P. 4660–4670.

7. Dai Y., Xu D., Maharjan S., Qiao G., and Zhang Y. Artificial Intelligence Empowered Edge Computing and Caching for Internet of Vehicles. IEEE Wireless Communications Magazine. 2019. Vol. 26. No. 3. P. 12–18.

8. Dorri A., Kanhere S.S., Jurdak R. MOF-BC: A memory optimized and flexible blockchain for large scale networks. Future Generation Computer Systems. 2019. Vol. 92. P. 357–373.