ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004.056 **DOI: 10.18413/2518-1092-2021-6-2-0-1**

Нестеренко В.Р.
Маслова М.А.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ BLOCKCHAIN ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: vladimir.nesterenko.workmail@gmail.com, mashechka-81@mail.ru

Аннотация
Применение блокчейна в сетях интернета вещей – новаторский подход, который способен сделать коммуникации между устройствами такой сети распределенными, автономными и безопасными. Блокчейн в данном контексте представляет из себя совокупность криптографически связанных блоков. Транзакции в сети исполняют роль основных носителей информации о состоянии узлов, а также выходной информации самих узлов для автономного функционирования сети. Узлом является “умное” устройство, датчик или же микроконтроллер, который связывает группу датчиков. Блокчейн применятся для обеспечения защищенной передачи и обработки данных устройств в сети интернета вещей. В данной статье рассмотрены основные возможности и вызовы при применении технологии в распределенных сетях.
Ключевые слова: internet of things (интернет вещей); blockchain (блокчейн); peer-to-peer network; proof of authentication (доказательство аутентификации); децентрализованная сеть.
Для цитирования: Нестеренко В.Р., Маслова М.А. Использование технологии blockchain для обеспечения безопасности в распределенном интернете вещей // Научный результат. Информационные технологии. – Т.6, №2, 2021. – С. 3-8. DOI: 10.18413/2518-1092-2021-6-2-0-1

Nesterenko R.V.
Maslova M.A

USING BLOCKCHAIN TECHNOLOGY TO ENSURE SECURITY IN THE DISTRIBUTED INTERNET OF THINGS

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: vladimir.nesterenko.workmail@gmail.com, mashechka-81@mail.ru

Abstract
The use of Blockchain in the Internet of Things networks is an innovative approach that can make communication between devices of such a network distributed, autonomous and secure. The blockchain in this context is a set of cryptographically connected blocks. Transactions in the network act as the main carriers of information about the state of the nodes, as well as the output information of the nodes themselves for the autonomous functioning of the network. A node is a "smart" device, a sensor, or a microcontroller that connects a group of sensors. Blockchain will be used to provide secure data transmission and processing of devices in the Internet of Things network. This article discusses the main opportunities and challenges in the application of technology in distributed networks.
Keywords: internet of things, blockchain, peer-to-peer network, proof of authentication, a decentralized network.
For citation: Nesterenko R.V., Maslova M.A. Using blockchain technology to ensure security in the distributed internet of things // Research result. Information technologies. – T.6, №2, 2021. – P. 3-8. DOI: 10.18413/2518-1092-2021-6-2-0-1

ВВЕДЕНИЕ

С развитием коммуникационных технологий и с повсеместным введением 5G-сетей, технология “Интернет вещей” начала развиваться с экспоненциальной скоростью. Умный дом, умные города, система e-Health, интернет вещей для промышленных предприятий, распределенный интеллект и другие системы – эффективное и привычное для общества средство улучшения многих процессов, например, процессов орошения урожая на основе датчиков и других процессов, которые могут быть автоматизированы. Подобный подход к процессам уменьшает влияние человеческого фактора и способствует повышению эффективности предприятия, где есть все предпосылки для применения технологии IoT.

При всей своей эффективности и распространенности, технология Internet of things (интернет вещей) имеет множество вызовов и проблем, связанных с безопасностью и безопасной конфигурацией устройств Интернета вещей.

Существование огромного количества подобных устройств несет в себе опасность, так как злоумышленник может взять их под контроль и организовывать с помощью устройств интернета вещей ДДОС-атаки и другие манипуляции с трафиком, которые отсылают данные устройства на сервер.

Одним из примеров согласованных атак множества устройств интернета вещей является ботнет. Ботнет – это совокупность взломанных устройств, находящихся под контролем злоумышленника. Mirai – червь и ботнет, образованный взломанными (скомпрометированными) устройствами типа «интернет вещей» (видеопроигрыватели, «умные» веб-камеры, прочее). Данный ботнет взламывает устройства, подбирая пароль к 23 порту (telnet). В централизованных системах интернета вещей иногда достаточно бывает взломать сервер или микроконтроллер, отвечающий за коммуникации между большой группой устройств, чтобы получить возможность контроля всех устройств, коммуницирующих по централизованному протоколу с взломанным сервером [1, 3, 8].

ОСНОВНАЯ ЧАСТЬ

ДЕЦЕНТРАЛИЗОВАННЫЙ ПОДХОД В INTERNET OF THINGS (Интернете вещей). Централизация системы управления интернетом вещей может являться уязвимостью, так как такая архитектура значительно сокращает время, за которое все устройства в такой сети могут быть взяты под контроль злоумышленником.

Выходом служит использование децентрализованного подхода к организации такой сети, где каждое устройство выступает самостоятельным узлом. В случае такой коммуникации, злоумышленнику придется взломать каждое устройство, а не только центральный сервер. Использование протоколов централизованной коммуникации в децентрализованной сети не является достаточно безопасным и эффективным. Использование технологии Блокчейн для организации коммуникации между устройствами в такой сети наиболее оправданное решение, так как информация будет передаваться в виде безопасных, подписанных транзакций, которые должны быть записаны в распределенном реестре каждого узла.

Подобный подход обеспечивает следующие преимущества и свойства взаимодействия устройств в распределенной сети [5, с. 3]:

1) децентрализация;
2) безопасность;
3) идентификация;
4) гибкость сети;
5) автономность работы сети;
6) надежность информации.

Децентрализация предполагает устранение проблем безопасности централизованного подхода к организации интернета вещей, увеличивая погрешность, однако также увеличивая

эффективность такой сети и безопасность. Транзакции между узлами безопасны, подписаны секретным ключом узла отправителя и проверенные узлом получателем, таким образом обеспечивается безопасность и идентификация. В любой момент в сеть может быть подключено любое количество устройств, которые получат актуальную копию распределенного реестра – таким образом обеспечивается гибкость сети. Автономность работы заключается в невозможности приостановить работу всей сети, выведя из строя какой-либо ее компонент, как это может происходить в централизованной сети при выводе из строя сервера. Надежность информации в сети заключается в том, что в блоках распределенного реестра будут находиться только верифицированные майнерами или иным способом транзакции, содержащие выходную информацию устройств [2, 4].

Децентрализация и peer-to-peer организация сети показывают высокий уровень безопасности, надежности, гибкости сети и возможность автономной работы ее частей.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Рассмотрим эффективный консенсус и хранение распределенного реестра. При всех преимуществах децентрализованной сети все еще остаются актуальными следующие вызовы: как хранить распределенный реестр на узле и какой алгоритм консенсуса использовать для эффективной работы сети.

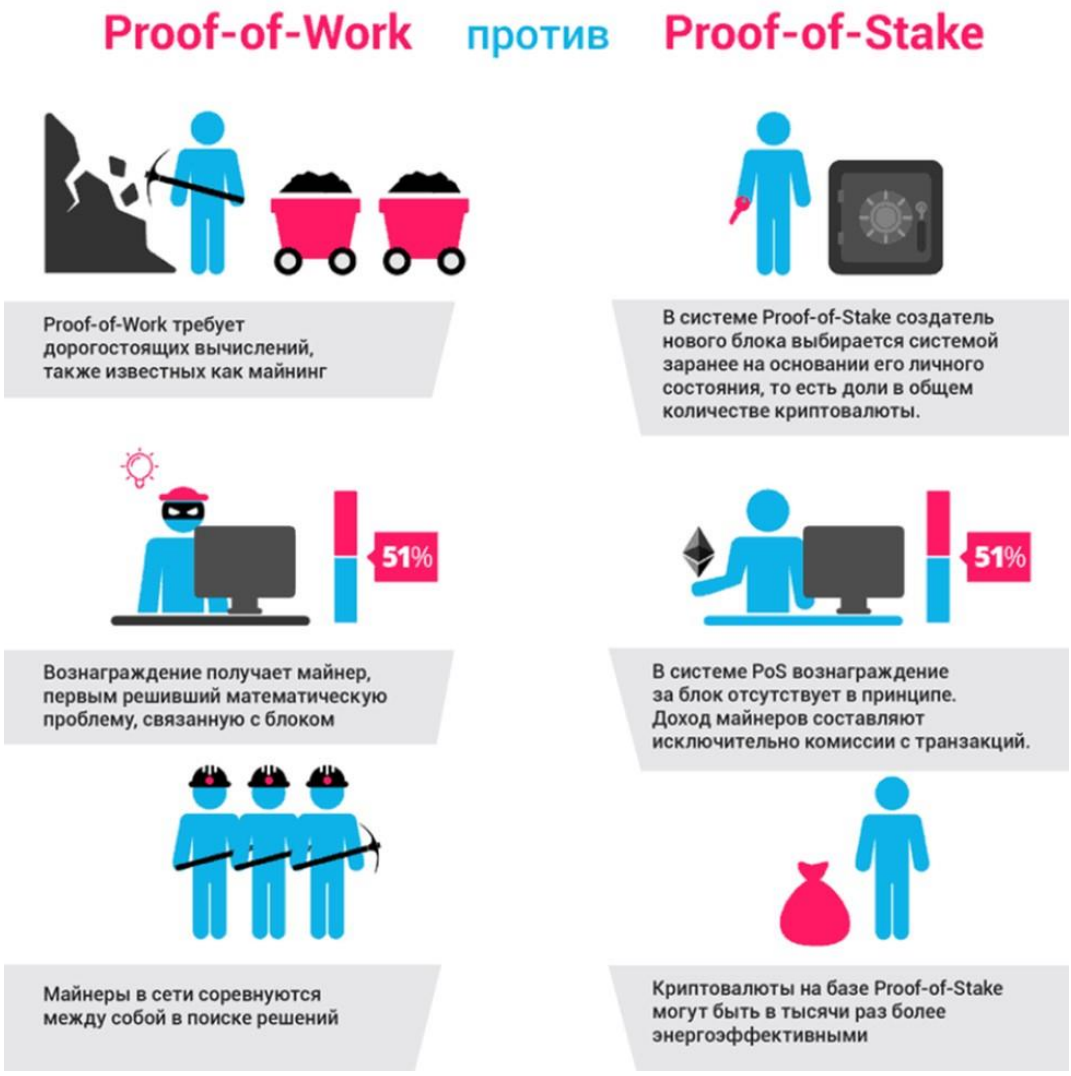

Рис. Доказательство работы и доказательство доли
Fig. Proof-of-work and Proof-of-Stake

Proof-of-work (доказательство работы) – стандартный алгоритм сети Биткоин, который позволяет на основе доказательства каких-то сложных вычислений, доказать проделанную работу для верификации транзакций и криптографического закрытия блока. В огромной сети данный алгоритм консенсуса оказывается очень затратным с точки зрения расходуемой энергии на вычисления для верификации и закрытия блоков.

Сеть интернета вещей должна обеспечивать коммуникацию и принятие решения в режиме реального времени. Данное требование делает доказательство работы неэффективным для решения поставленной задачи. Так как в закрытой сети интернета вещей доказательством работы должны заниматься сами устройства – работа такой сети может быть нарушена из-за высокой нагрузки на устройства, при вычислении доказательства работы.

Майнером считается участник сети, заинтересованный в поддержании работоспособности такой сети за некоторую награду. Возможно организовать распределенную сеть, основанную на доказательстве работы, только сделав интернет вещей открытым для внешних майнеров. В таком случае придется обеспечить достаточно высокую вовлеченность майнеров, чтобы не было задержки в генерации новых блоков и не было дополнительной нагрузки на узлы в сети.

Другим выходом может являться выбор более легковесного алгоритма консенсуса. Например, Proof-of-Stake или доказательство части. Данный алгоритм консенсуса менее требователен к ресурсам, чем доказательство работы (см. рис.1). Однако в соответствии с [7, с. 2], предпочтительным и легковесным алгоритмом консенсуса для распределенного интернета вещей является Proof-of-Authentication (доказательство аутентификации).

Для реализации данного алгоритма необходимо в общей таблице коммуникаций хранить соответствия открытого ключа и MAC-адреса устройства.

Доказательство аутентификации может быть реализовано следующим образом [6, с.9]:

- Выбираются доверенные узлы.
- Недоверенный узел собирает транзакции в блок.
- Недоверенный узел подписывает блок и отправляет всем доверенным узлам.
- Доверенные узлы сопоставляют открытый ключ узла и его MAC-адрес.
- Если все доверенные узлы успешно аутентифицировали узел, отправивший блок, то происходит рассылка этого блока всем узлам сети.
- При получении блока остальные узлы находят хэш заголовка и открывают новый блок с этим хэш-значением в поле “Предыдущий хэш”.

Если доверенный узел не смог аутентифицировать блок и приславший этот блок узел, тогда рейтинг доверия падает на 1. При низком рейтинге доверия происходит переназначение доверенных узлов в сети. Такой алгоритм позволяет очень сильно сократить нагрузку на устройства, а также обеспечить проверку подлинности присланной информации с помощью механизма ЭЦП. Использование приведенного выше алгоритма помимо надежного алгоритма консенсуса также способствует улучшению безопасности хранимых данных.

Хранение распределенного реестра возможно реализовать в облаке, чтобы каждый узел имел возможность доступа к своему участку облака. Таким образом, данные не будут занимать место на самом устройстве.

Также возможно хранить не все, но только самые актуальные блоки с данными на устройствах. Такой способ позволит отказаться от взаимодействия с облаком, а также будет экономить память самих узлов.

ЗАКЛЮЧЕНИЕ

Применение технологии Блокчейн в организации защищенной распределенной сети интернета вещей - очень перспективная и новаторская технология. Данный подход в организации распределенной сети позволяет обеспечить прежде всего автономность работы узлов, высокий уровень безопасности инфраструктуры и элементов интернета вещей, а также идентификацию с помощью ЭЦП. Однако, у применения данной технологии есть некоторые ограничения:

стандартные алгоритмы консенсуса не подходят из-за их привязанности к внешним майнерам или из-за высоких энергозатрат, однако, алгоритм доказательства аутентификации является надежным алгоритмом консенсуса для сети, где майнерами выступают узлы самой сети. Данный алгоритм способен обеспечивать необходимое быстродействие устройств и коммуникацию в реальном времени. Хранение данных возможно реализовать двумя, предложенными в этой статье способами:

1) обеспечить доступ узла к участку облака, где будет храниться копия реестра,
2) хранить только наиболее актуальные блоки в памяти самого узла, обеспечив такому реестру легковесность.

Список литературы

1. Афонькин А.Ю., Ноздрина Н.А. Перспективы развития технологии блокчейн в ближайшем будущем // Научные тенденции: Вопросы точных и технических наук./Сборник научных трудов по материалам XVI международной научной конференции. 2018. С. 20-21.
2. Гончаренко Ю.Ю., Арзамасцев Д.А. Программный модуль для контроля и ведения электронного документооборота на основе технологии блокчейн // Научный результат. Информационные технологии. – Т.5, №3, 2020.
3. Гончаренко Ю. Ю., Паво Ф. Н. Разработка децентрализованного приложения для реализации цифровой идентичности с использованием технологии блокчейн // Вестник УрФО № 3(29) / 2018, С. 23–28.
4. Михаленко Ю.А., Крюкова А.А. Блокчейн как один из элементов цифровизации государства // Вестник Евразийской науки, 2018 №1, https://esj.today/PDF/10ECVN118.pdf
5. Alam, Tanweer. (2019). Blockchain and its Role in the Internet of Things (IoT). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 151-157. 10.32628/CSEIT195137.
6. Deepak Puthal and Saraju P. Mohanty and Venkata P. Yanambaka and Elias Kougianos (2020). PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks
7. Puthal, Deepak & Mohanty, Saraju. (2019). Proof of Authentication: IoT-Friendly Blockchains. IEEE Potentials. 38. 26-29. 10.1109/MPOT.2018.2850541.
8. Горшкова С. Новые технологии на службе интеллектуального права: блокчейн, искусственный интеллект, виртуальная реальность // Сборник научных трудов IX Международного юридического форума (IP форум) // Правовая защита интеллектуальной собственности: проблемы теории и практики Москва, 12–13 февраля 2021 года.

References

1. Afonkin A.Yu., Nozdrina N.A. Prospects for the development of blockchain technology in the near future // Scientific trends: Questions of exact and technical sciences / Collection of scientific papers based on the materials of the XVI International Scientific Conference. 2018. p. 20-21.
2. Goncharenko Yu.Yu., Arzamassev D.A. Program module for monitoring and maintaining electronic document management based on blockchain technology. Research Result. Information Technologies. – Vol. 5, No. 3, 2020
3. Goncharenko Yu.Yu., Pavo F.N. Development of a decentralized application for implementing digital identity using blockchain technology // Bulletin of the Ural Federal District No. 3 (29), 2018, pp. 23-28.
4. Mikhalenko Yu.A., Kryukova A.A. Blockchain as one of the elements of state digitalization // Bulletin of Eurasian Science, 2018 No. 1, https://esj.today/PDF/10ECVN118.pdf
5. Alam, Tanweer. (2019). Blockchain and its Role in the Internet of Things (IoT). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 151-157. 10.32628/CSEIT195137.
6. Deepak Puthal and Saraju P. Mohanty and Venkata P. Yanambaka and Elias Kougianos (2020). PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks
7. Puthal, Deepak & Mohanty, Saraju. (2019). Proof of Authentication: IoT-Friendly Blockchains. IEEE Potentials. 38. 26-29. 10.1109/MPOT.2018.2850541.
8. Gorshkova S. New technologies in the service of intellectual property law: blockchain, artificial intelligence, virtual reality. // Collection of scientific papers of the IX International Legal Forum (IP Forum). // Legal protection of intellectual property: Problems of Theory and Practice Moscow, February 12-13, 2021.

Нестеренко Владимир Романович, студент второго курса магистратуры кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности

Nesterenko Vladimir Romanovich, second-year master's student of the Department Information security, Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, senior lecturer of the Department «Information security», Institute of Radioelectronics and Information security