ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИИ В ИНТЕРНЕТЕ ВЕЩЕЙ

Мадияр Сейдуллаев
Ташкентский университет информационных технологий
им. Мухаммад аль-Хорезми
Ташкент, Узбекистан

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 блокчейн-технологии в интернете вещей.

Ключевые слова: Интернет вещей, блокчейн, криптография.

1 Введение

Когда Интернет вещей (IoT) становится все более популярным, защита пользовательских данных становится все более важной. В прошлом сообщалось о многих проблемах безопасности, и защита этих систем IoT кажется сложной задачей. Из-за особенностей устройств IoT их безопасность может быть скомпрометирована. Такие факторы, как энергоэффективность, ограниченное пространство для оборудования и чипов, усложняют методы обеспечения безопасности в IoT. Кроме того, огромный спрос на новые продукты затрудняет контроль безопасности IoT. Быстрая эволюция IoT усложняет стандартизацию систем безопасности среди поставщиков. Несмотря на трудности, поставщики могут соблюдать рамки и стандарты безопасности, чтобы снизить риск успешного получения злоумышленником несанкционированного доступа к их системам IoT. К сожалению, угроза сохраняется, и любая система IoT по-прежнему подвергается многим видам атак. [1]

Вместо традиционной системы IoT можно интегрировать блокчейн, чтобы получить различные преимущества в плане безопасности. Хотя обсуждаются преимущества и недостатки IoT с блокчейнами, нет реальной оценки того,

является ли это жизнеспособным способом смягчения угроз безопасности для IoT. В этой статье преимущества использования блокчейнов будут оцениваться в сравнении с потребностями безопасности в IoT. Для этого необходимо выявить угрозы IoT. Необходимо провести обзор недавних угроз безопасности, чтобы понять угрозу и определить, какие меры безопасности имеют наивысший приоритет.

Устройство IoT может быть устройством любого типа, оснащенным одним или несколькими датчиками и возможностью подключения к Интернету. Этими устройствами обычно можно управлять с удаленного устройства, такого как смартфон. Некоторыми примерами устройств IoT, используемых дома (продукты для умного дома), являются лампочки, выключатели и дверные звонки. Устройства IoT обычно используют протоколы связи, такие как Bluetooth и Zigbee. Bluetooth и Zigbee — это технологии беспроводной связи. [2] Чтобы подключиться к Интернету, устройства обычно подключаются к концентратору, который впоследствии подключается к сети с помощью WiFi. Обычно устройство IoT собирает или поддерживает некоторые типы данных. Для этого многие IoT-устройства хранят данные в облачном хранилище. Некоторым устройствам придется ограничить аппаратное обеспечение, такое как встроенная память и хранилище. Это может сделать управление облачной памятью необходимостью. [3].

Интернет вещей предназначен для обеспечения взаимосвязи между устройствами. [2] Одним из самых популярных протоколов радиосвязи является ZigBee. ZigBee подходит для IoT из-за его высокой надежности, низкого энергопотребления и сложности. ZigBee следует стандарту работы IEEE 802.15.4. Устройства Zigbee могут работать как координаторы маршрутизаторов и терминальное оборудование. Различные логические роли определяют, как устройству разрешено обмениваться данными в сети ZigBee. Протокол ZigBee основан на четырехуровневом стеке. Стек имеет физический уровень, уровень доступа к среде, сетевой уровень и прикладной уровень. Уровни управляют различными задачами, чтобы поддерживать полную коммуникационную функциональность в устройстве. Устройства адресуют трафик с помощью MAC-адресов, а топология сети поддерживается на сетевом уровне. [4]

ZigBee имеет некоторые базовые функции безопасности. Он использует 128-битное шифрование AES и код целостности сообщения. Он также имеет базовый контроль доступа и защиту от повторного воспроизведения. Для устройств ZigBee доступны различные режимы безопасности. В режиме по умолчанию ни одна из функций безопасности не включена. Шифрование AES требует набора ключей, которыми можно делиться по-разному. Они могут быть,

например, предварительно разделены или могут передаваться внутри сетевых групп. Если ключ скомпрометирован, вся сеть находится под угрозой. [4]

Для взаимодействия с микроконтроллерами IoT обычно используются такие протоколы, как UART или SPI. Протоколы являются быстрыми и простыми для связи интегральных схем. Эти протоколы не имеют встроенной защиты. [5] Устройства IoT обычно имеют контакты для связи UART на чипе. Точно так же на микросхеме могут присутствовать выводы JTAG, которые используются для отладки и тестирования микросхемы. [6] Реализации систем IoT традиционно следуют централизованной архитектуре, где для полноценной работы необходим сервер. Уровень внедрения IoT с блокчейнами низок из-за ограниченных знаний о его преимуществах. [7]

2. Основная часть

Технологии блокчейна позволяют осуществлять транзакции между двумя одноранговыми узлами без необходимости в доверенной третьей стороне. Когда два узла соглашаются на транзакцию, она вместе с другими транзакциями группируется в блоки. Блоки транзакций проверяются сетью блокчейн. Действительные блоки добавляются в цепочку действительных блоков. В большинстве блокчейнов каждый участвующий узел в сети будет иметь копия этой цепочки. Чтобы добавить блок в цепочку, узлы согласовали метод, и все они следуют этому методу для проверки транзакций. В блокчейне Биткойн и Эфириум пиры должны решить криптографическую головоломку, похожую на взлом хеш-суммы. Узел, предлагающий решение, получает определенный крипто-токен в зависимости от типа блокчейна. Этот тип механизма консенсуса называется доказательством работы. [8] Это оригинальный механизм, и в более поздних блокчейнах обычно применяется доказательство доли. [9]

Первой работающей системой, построенной на основе полностью децентрализованной системы, был Биткойн. Биткойн — хороший пример концепции создания децентрализации. Ключами для достижения этого являются консенсус, бухгалтерская книга и криптография. Интернет традиционно состоял из централизованных и распределенных систем. В центральной системе все вычисления выполняются в одной точке отказа. Вычисления могут быть распределены, чтобы выполняться в отдельных местах с промежуточной связью, создавая распределенную систему. Подобно децентрализованной системе, распределенная система не выйдет из строя, если один узел в сети выйдет из строя. Децентрализованная система работает иначе, чем традиционная система. Он использует механизм консенсуса для принятия решений вместо того, чтобы назначать обязанности узлам [10].

Биткойн — первая работающая распределенная система электронных денег. В 2008 году была выпущена статья «Биткойн: одноранговая электронная кассовая система». Он предложил способ создания цифровой валюты без необходимости в банке. Транзакции будут проходить напрямую из точки А в точку Б без участия третьих лиц. Система использует криптографию с открытым и закрытым ключом для создания незащищенных транзакций для передачи защищенных ценностей. Транзакции проверяются системой с использованием цепочки блоков и механизма консенсуса Proof-of-Work [10].

В сети Биткойн транзакции подписываются закрытыми ключами, чтобы доказать, что он является владельцем своего публичного адреса. Владелец закрытого ключа может подписывать данные, применяя криптографический алгоритм с закрытым ключом. Затем все остальные могут подтвердить, что владелец закрытого ключа действительно является владельцем, отменив подпись с помощью открытого ключа. Криптосистема работает и в обратном порядке: при шифровании данных с помощью открытого ключа только владелец соответствующего закрытого ключа может расшифровать данные. Публичный адрес действует как адрес биткойн-кошелька пользователя. Сжатая версия открытого ключа, называемая биткойн-адресом, может быть передана кому угодно и использоваться другими для отправки средств на этот кошелек. Соответствующий закрытый ключ впоследствии может быть использован для разблокировки активов, отправленных на этот биткойн-адрес. [10, 11]

Закрытые ключи, используемые Биткойном, представляют собой 256 битов случайности. Затем публичный адрес рассчитывается на основе закрытого ключа с использованием алгоритма цифровой подписи кривой Эклиптики. Открытый ключ хешируется, и ему предшествуют два нуля, чтобы сформировать биткойн-адрес. [10, 11]

Транзакции представляют собой перевод цифровой валюты с одного адреса на другой. Все транзакции в блокчейне хранятся в публичном реестре. Каждый узел в сети имеет копию одной и той же книги. Наряду с некоторыми другими флагами и полями транзакции состоят из списков входов и выходов. Входные данные — это неизрасходованные транзакции на общедоступный адрес. Выходы — это адреса получателей токенов. Владельцы транзакций включают свою цифровую подпись, чтобы другие могли подтвердить свою личность. Любой узел в сети блокчейна может подтвердить личность владельца, не зная закрытого ключа [10].

Транзакции формируются в блоки транзакций. Каждый узел в сети содержит одни и те же блоки транзакций. Узлы могут проверить это, вычислив корень Меркла блоков. Корень merkle представляет собой дерево подписей и

действует как снимок блока. Сравнение корня Меркла более эффективно с точки зрения ресурсов по сравнению с использованием всего блока [10].

Каждый блок инициируется с вознаграждением, поступающим издателю блока. Это значение представляет собой сумму всех комиссий за транзакции плюс значение, которое периодически уменьшается вдвое. Первоначально это значение составляло 50 биткойнов. Сеть использует алгоритм консенсуса, что означает, что если большая часть сети злоупотребляет этим консенсусом, сеть скомпрометирована. В нескомпрометированной сети Биткойн консенсус является доказательством работы, означающим, что узел, которому разрешено публиковать следующий блок, должен решить криптографическую проблему. В Биткойне проблема заключается в том, чтобы придумать хеш, который меньше «целевого хэша». Целевой хэш — это просто настраиваемый хеш, который определяет сложность криптографической задачи. Целевой хеш корректируется каждые 2016 блоков и зависит от вычислительной мощности, которая в настоящее время находится в сети. Чем больше майнеров, тем выше сложность [10].

Хеш, который генерируют майнеры, — это хэши некоторых конкретных данных. Этими конкретными данными являются версия программного обеспечения майнера, корень Меркла ранее добытого хэша, корень Меркла текущего блока, отметка времени, текущая цель сети Биткойн и объявление. Объявление — это то, что майнер продолжает корректировать, чтобы получить действительный хэш. Когда майнер придумывает решение, все остальные майнеры могут подтвердить это, просто протестировав решение и проверив полученный хэш, в противном случае опубликованный блок считается недействительным, и майнеры могут продолжить поиск действительного решения [10].

Проблема с системами блокчейна заключается в том, что несколько одноранговых узлов могут предлагать разные решения. Решение этой проблемы называется правилом самой длинной цепи. Правило самой длинной цепочки гласит, что самая длинная цепочка проверенных блоков — это обычная цепочка. Любые другие предложенные цепочки считаются недействительными. Это вводит уязвимость блокчейнов. Если злоумышленник контролирует большую часть вычислительной мощности в сети, он может тайно создать более длинную цепочку на узлах злоумышленника, а затем заменить конвекционную цепочку. Это позволяет проводить атаки с двойным расходом. Однако получить контроль над большей частью вычислительной мощности в сети недешево и не просто. Особенно когда блокчейн набирает популярность, сложность атаки возрастает. Несмотря на стоимость проведения атаки, она прибыльна. [12] Правило самой

длинной цепи применяется во многих различных типах алгоритмов консенсуса [10]. 2.3.2 Эволюция блокчейнов Сеть Ethereum — это еще один блокчейн с некоторыми отличиями от биткойнов. Ethereum представляет смарт-контракты, которые могут выполнять код на узлах сети. Ethereum также использует доказательство работы, но блоки имеют неограниченный размер. Среднее время транзакций Ethereum значительно меньше по сравнению с биткойнами, но все же значительно выше, чем у традиционных централизованных систем. Смарт-контракты обеспечивают большую гибкость, чем в сети Биткойн. Используя смарт-контракт, разработчики могут реализовывать внутренние программы, работающие на блокчейне. Эти программы могут быть сопряжены с минимальной интерфейсной системой. Этот тип приложения называется децентрализованным приложением или «DAPP». [10, 13]

Как уже упоминалось, децентрализованное приложение обычно имеет свои серверные функции, доступные в блокчейне. Это делает логику программы общедоступной для пользователей. При выполнении транзакции, связанной с программой, логический поток выполняется сетью блокчейн. Программы обычно ограничены в ресурсах и имеют ограниченный объем вычислительной мощности, памяти и гибкости [38].

Блокчейны могут поддерживать прозрачную сеть без необходимости в третьей стороне благодаря своим алгоритмам консенсуса. У каждого блокчейна есть свой собственный метод создания консенсуса в сети. Консенсус необходим, чтобы иметь возможность доверять пирам, которые могут попытаться внести недопустимые изменения в реестр. Как упоминалось ранее, биткойн использует доказательство работы, которое требует очень много энергии [14].

Было разработано несколько новых алгоритмов и механизмов консенсуса для решения различных проблем с консенсусом Биткойн. Биткойн неэффективен с точки зрения энергии и требует много энергии для использования. Когда транзакция выполняется, для ее проверки требуется мощность. Популярным предлагаемым методом преодоления этого является доказательство доли, когда вместо этого узел публикации выбирается на основе богатства. Богатство в этом случае — это количество цифровых активов, которые владелец «поставил». При размещении токенов шансы быть выбранным в качестве публикующего узла увеличиваются. Существует множество других алгоритмов консенсуса, таких как proof-of-space и proof-of-history [10].

Традиционные сети блокчейна хранят общедоступные реестры всех транзакций в виде копий на всех узлах. Реестр работает как общедоступная база данных, которая никому не принадлежит. В общедоступных и частных блокчейнах реестр надежно управляет реестром с помощью криптографии.

Реестры содержат блоки транзакций, а некоторые реестры могут даже хранить другие типы данных, например, состояния программ, работающих в блокчейне [14].

3. Блокчейн и Интернет вещей

Блокчейн может заменить централизованные аспекты систем IoT. Всякий раз, когда возникает необходимость передачи данных из одной точки в другую, можно использовать смарт-контракт. Например, когда необходимо настроить устройство IoT. Пользователь может напрямую взаимодействовать с блокчейном через приложение для смартфона. Блокчейн напрямую взаимодействует с сетью IoT.

Что касается хранения данных, объем данных, которые можно хранить в блокчейне, ограничен, поэтому может потребоваться облачное хранилище в зависимости от типа устройства IoT и его функций. Гибридные методы могут использоваться для хранения данных с преимуществами безопасности от блокчейна. Также возможно полное децентрализованное облачное хранилище. При необходимости хранить большие файлы это может быть неуместно, а реализации облачных хранилищ могут быть ограничены масштабируемостью.

Логика приложения традиционной централизованной системы IoT будет находиться на сервере. Когда устройства IoT взаимодействуют с этим сервером, создается сценарий единой точки отказа. Если эта точка выйдет из строя или будет скомпрометирована, это повлияет на все устройства IoT. В децентрализованной системе IoT логика приложения будет заключаться в смарт-контрактах, выполняемых одноранговыми узлами в сети. В таком случае проблема единой точки отказа устраняется, и если один узел выходит из строя, это не повлияет на устройства IoT.

Безопасность сети IoT с блокчейном устранит векторы атак, направленных на серверы приложений. Это также обеспечит конфиденциальность и целостность операций передачи данных, таких как управление устройствами и передача файлов. Шифрование с открытым ключом будет использоваться для всех транзакций, позволяя расшифровку только для действительного узла-получателя. Доступность службы блокчейна также улучшена за пределами системы единой точки отказа.

Несмотря на множество преимуществ интеграции технологий блокчейна в систему IoT, есть, конечно, и недостатки. В настоящее время существуют высокие накладные расходы, неэффективность использования энергии, ограничения хранения и проблемы с конфиденциальностью. В данной статье направлено на сравнение этих недостатков с преимуществами IoT с блокчейнами. Угрозы безопасности обычной системы оцениваются, чтобы включить в это сравнение несколько аспектов безопасности.

4. Выводы

Технология блокчейна может повысить безопасность и производительность IoT сетей, обеспечив при этом неизменность данных, децентрализацию и возможность использовать смарт-контракты. Однако конвергенция этих технологий влечет за собой определенные проблемы, такие как ограниченные ресурсы Интернета вещей, слабое шифрование, проблемы масштабируемости и протоколов коммуникации, ориентированных одновременно на IoT-устройства и блокчейн-сети.

Использованная литература

1. Sanggyu Shin and Yoichi Seto. Development of iot security exercise contents for cyber security exercise system. In 2020 13th International Conference on Human System Interaction (HSI), pages 1–6, 2020. doi: 10.1109/HSI49210. 2020.9142678.
2. Sachchidanand Singh and Nirmala Singh. Internet of things (iot): Security challenges, business opportunities reference architecture for e-commerce. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pages 1577–1581, 2015. doi: 10.1109/ICGCIoT.2015.7380718
3. Aditya Gupta. The IoT Hacker’s Handbook: A Practical Guide to Hacking the Internet of Things. Apress L. P, 2019.
4. Bo Fan. Analysis on the security architecture of zigbee based on ieee 802.15.4. In 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), pages 241–246, 2017. doi: 10.1109/ISADS.2017.23.
5. Rizka Reza Pahlevi, Aji Gautama Putrada S., and Maman Abdurohman. Fast uart and spi protocol for scalable iot platform. In 2018 6th International Conference on Information and Communication Technology (ICoICT), pages 239–244, 2018. doi: 10.1109/ICoICT.2018.8528745
6. Dongfang Li, Wei Shen, and Zhihao Wang. A noval method of security verification for jtag protection function. In 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), pages 487–492, 2019. doi: 10.1109/QRS-C.2019.00093.
7. Satyabrata Aich, Sabyasachi Chakraborty, Mangal Sain, Hye-in Lee, and HeeCheol Kim. A review on benefits of iot integrated blockchain based supply chain management implementations across different sectors with case study. In 2019 21st International Conference on Advanced Communication Technology (ICACT), pages 138–141, 2019. doi: 10.23919/ICACT.2019.8701910.

8. Puneet Kumar Kaushal, Amandeep Bagga, and Rajeev Sobti. Evolution of bitcoin and security risk in bitcoin wallets. In 2017 International Conference on Computer, Communications and Electronics (Comptelix), pages 172–177, 2017. doi: 10.1109/COMPTELIX.2017.8003959.
9. Cong T. Nguyen, Dinh Thai Hoang, Diep N. Nguyen, Dusit Niyato, Huynh Tuong Nguyen, and Eryk Dutkiewicz. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. IEEE Access, 7:85727–85745, 2019. doi: 10.1109/ACCESS.2019.2925010.
10. Daniel Cawrey and Lorne Lantz. Mastering Blockchain. O‘Reilly Media, Inc,2020. ISBN 492054690;9781492054696;
11. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf
12. N Akhmedov, H Khujamatov, A Lazarev, M Seidullayev (2021, November). Application of LPWAN technologies for the implementation of iot projects in the Republic of Uzbekistan. In 2021 International Conference on Information Science and Communications Technologies (ICISCT).IEEE
13. Chibuzor Udokwu, Aleksandr Kormiltsyn, Kondwani Thangalimodzi, and Alex Norta. The state of the art for blockchain-enabled smart- contract applications in the organization. 11 2018. doi: 10.1109/ISPRAS.2018.00029.
14. Tiana Laurence. Blockchain for dummies. Wiley, Newark, 2nd edition, 2019. ISBN 1119555019;9781119555018;.