УДК 004.056

Использование блокчейн для обеспечения информационной безопасности интернета вещей

Волков Иван Максимович
Российский экономический университет им. Г.В. Плеханова
Студент

Токмакова Наталия Романовна
Российский экономический университет им. Г.В. Плеханова
Студент

Аннотация
Безопасность устройств, составляющих Интернет вещей, становится острым вопросом. Так, появляется необходимость в поиске новых подходов по обеспечению безопасности с точки зрения обеспечения доступности данных на устройствах, их целостности и конфиденциальности, а также возможности корректного обновления программного обеспечения для исправления имеющихся уязвимостей. Блокчейн может стать ответом на многие вопросы безопасности за счет своей архитектуры, обеспечивающей распределенное и неизменяемое хранение зашифрованных данных.
Ключевые слова: Интернет вещей, Блокчейн, Информационная безопасность

Using blockchain to secure the internet of things

Volkov Ivan Maximovich
Russian Plekhanov University of Economics
Student

Tokmakova Nataliya Romanovna
Russian Plekhanov University of Economics
Student

Abstract
The safety of the devices of the Internet of things becomes an acute issue. Thus, there is a need to find new security approaches in terms of ensuring data availability on the devices, their integrity and confidentiality, as well as the possibility to correct vulnerabilities using installation of software updates. The blockchain technology can become a response to many security issues through its architecture that provides distributed and unchanged storage of encrypted data.
Key words: The Internet of Things, Blockchain, Information Security

Введение

Интернет вещей – это вычислительная сеть физических объектов для взаимодействия друг с другом или с внешней средой с применением различных технологий связи и стандартов соединения. Аппаратная архитектура Интернета вещей представляет собой совокупность конечных узлов, которые должны быть оснащены сенсорами, и подключенные к ним агрегирующие устройства (шлюзы), соединенные с удаленными облачными платформами для передачи и последующей обработки данных для представления их в приложениях и сервисах. [4] В такой сети возникает сложная, но критически важная для решения, проблема – обеспечение безопасности данных с точки зрения конфиденциальности, целостности и доступности, а также необходимость в непрерывном обновлении программного обеспечения на устройствах для исправления найденных в процессе эксплуатации уязвимостей.

Одно из возможных решений такой проблемы является технология блокчейн – полностью реплицированная распределенная база данных, которая состоит из непрерывной последовательности цепочки блоков на основе связного списка, содержащей данные и хэш, рассчитанного по хэшу предыдущего блока и данным текущего блока. Таким образом, блокчейн относится к DLT (Distributed Ledger Technology), не имеет централизованного хранилища и работает в реальном времени. Объединение Интернета вещей и блокчейн технологий может разрешить некоторые вопросы безопасности.

Одним из возможных направлений применения блокчейн может быть управление жилищно-коммунальным хозяйством, где в последнее время активно внедряются облачные технологии и устройства Интернета вещей. Использование технологии блокчейн одновременно с использованием облачных технологий и технологией Интернета вещей позволит устранить многие проблемы информационной безопасности информационных сервисов для управления ЖКХ [2, 3].

Обеспечение доступности данных

Как уже было сказано выше, данные со шлюзов отправляются в облачное хранилище для последующей работы с ними. В то же время при увеличении количества устройств будет увеличиваться передаваемый трафик и общий объем данных для хранения. Это ведет к усложнению таких облачных хранилищ для обеспечения бесперебойной работы. Более того, такое хранилище становится узким местом, при отказе которого может возникнуть серьезный простой в ведении бизнеса и финансовым потерям.

Данную проблему решает блокчейн с помощью своей децентрализованной природы. Вместо дорогостоящего централизованного центра обработки данных сеть хранения цепочки блоков дублируется на сотни (или, возможно, тысячи или миллионы) компьютеров и устройств, входящих в сеть. [8] Так предотвращается опасность DDoS-атаки. Большой объем избыточности означает, что данные всегда будут доступны, когда это

необходимо, сокращая время передачи данных, а отказ одного и более серверов не будет иметь критического влияния на деловую активность.

Обеспечение целостности данных

В Интернете вещей транзакции данных происходят между несколькими сетями, принадлежащими и управляемыми несколькими организациями. Запись в цепочку блоков означает, что хранение данных является в высокой степени контролируемым, поскольку данные или физические товары, проходя между контрольными точками в цепочке поставок, записывают данные в блокчейн. Именно такую систему протестировали в «Газпром Нефть» в логистике материально-технических ресурсов. [1]

Более того, записи в блокчейн по своей природе прозрачны - активность может отслеживаться и анализироваться любым, кто имеет право подключаться к сети. Если что-то пойдет не так, например, возникают поломки или утечки данных там, где этого не должно быть, тогда запись в цепочку блоков упростит определение места возникновения такого нарушения, и в идеальном случае система предпримет корректирующие действия без вмешательства человека.

В дополнение, целостность данных поддерживается за счёт их дублирования на разные хранилища. Это создаёт дополнительные слои защиты для обеспечения неизменяемости цепочки блоков.

Естественно, использование блокчейн повышает степень доверия в сети между различными организациями, участвующими в работе Интернета вещей. Устройства будут надежно записывать зашифрованные детали транзакций, которые производят между собой. [7] Без секретных ключей, дающих возможность записи в цепочку блоков, которые в данном случае будут храниться в самих вещах, ни один человек не сможет перезаписать блок с искаженной информацией.

Обеспечение конфиденциальности данных

Блокчейн не только обеспечивает неизменяемость данных, но также может контролировать доступ к ним. Учитывая то, что данные, фигурирующие в Интернете вещей, являются очень личными, необходимо защитить их от получения третьими лицами. Если разрешить доступ к данным только через блокчейн с помощью ассиметричных алгоритмов шифрования, то появится еще один слой безопасности, препятствующий доступу хакеров к данным. [6]

Такая работа блокчейна обеспечивается следующим образом: каждый участник сети имеет доступ к блоку и транзакциям, произведенным в них. В то же время не все имеют доступ к полезному содержимому блоку, который защищён с помощью закрытого ключа.

Сама система защищена от внешнего вмешательства или прочтения. При формировании блока записывается не вся информация, а только та часть, которая необходима для конкретного пользователя, затем вписывается номер предыдущего хэша, и сформированный блок отправляется в цепочку.

При шифровании закрытый ключ знает только владелец цепочки, а для связности данные в зашифрованном виде отправляются следующему по цепи. Если же злоумышленник попытается вскрыть содержимое блока, он не сможет этого сделать незаметно, так как нарушится структура блока и будет заметно, в каком месте и какое устройство пытались взломать. Помимо местоположения попытки взлома, так же будет известно, как именно пытались узнать ту часть информации, ведь расшифровка кода может показать, какими средствами и методами пользовались хакеры. Но если даже кому-либо удастся вскрыть блок незамеченным и получить данные, они будут неполные и недостаточные для формирования связного отчёта для понимания. Другие части информации будут идти в последующих или предыдущих блоках.

Как было сказано выше, любые вредоносные действия можно будет распознать и предотвратить за счет контроля за изменением состояния цепочки блоков. [5] Так, будет возможность заблокировать работу устройства на основе подозрительных действий, например, попытки изменения структуры блокчейна, доступа к зашифрованных данным или иное нетипичное поведение.

Непрерывное обновление безопасности устройств

Ошибки в программном обеспечении неизбежны и создают уязвимости для хакеров. При обнаружении таких ошибок их исправляют специалисты, и, в идеальном случае, обновленное программное обеспечение автоматически рассылается в необходимые места хранения и после – всем пользователям. Так, блокчейн может выступать таким хранилищем обновлений. При регистрации нового обновления можно быть уверенным, что новая версия легитимна, так как доступ к записи будут иметь только производящая организация.

Для реализации такого подхода необходимо в первую очередь настроить устройства на периодическую регистрацию с помощью системы блокчейн с целью получения данных о новом программном обеспечении. При получении информации о наличии обновлений устройство должно получить его и установить. Каждое устройство должно иметь криптографическую идентификацию на основе конфигурации и состоянии устройства, чтобы гарантировать, что производитель взаимодействует и предоставляет доступ к базе данных своему устройству. Таким образом, можно обеспечить непрерывное обновление настроек безопасности.

Идентификация устройства в сети позволяет также решить проблему уязвимости перед DDoS-атакой или взлома за счет защищенного обмена сообщениями между вещами. При взаимодействии внутри сети идентификаторы устройства проверяются, транзакции подписываются и криптографически верифицируются. Если устройство не обладает необходимым доверием, то любые его запросы игнорируются. [10]

Для обеспечения эффективности «общения» между устройством с ограниченным объемом памяти и вычислительной мощности и

распределенной базой данных необходимо использовать или, при отсутствии таковых, разработать легкие протоколы обмена данных. Например, протокол Bitcoin SPV (Simplified Payment Verification) реализует методы проверки того, включены ли необходимые данные в блок без необходимости загрузки такого блока в память. Другой протокол – Ethereum Light Client Protocol – позволяет принимать данные о корректности интересующего блока при загрузке около 1 Кбайт за 2 минуты. Объединение таких идей позволит адаптировать новые протоколы для работы с маломощными устройствами Интернета вещей.

Возможные проблемы использования блокчейн в Интернете вещей

Блокчейн эффективно работает как способ уменьшения издержек транзакций, обеспечения безопасности данных, а также как является достаточно устойчивой системой, защищенной от сбоев и других проблем. В то же время, в данной технологии присутствуют некоторые недостатки. К примеру, сложность масштабирования. Блокчейн не способен поддерживать огромное количество транзакций одновременно. Так, современные платёжные системы способны обрабатывать несколько десятков тысяч операций в секунду, в то время как технологии с криптовалютами всего несколько единиц. С увеличением базы начинаются сложности с откликом системы и внесением данных, так как для формирования новой ячейки записи необходимо подтверждение всех предыдущих узлов. База данных растёт, как правило, с каждым днём.

Существует законодательная проблема привлечения блокчейн в повсеместную жизнь, так как не все страны пока приняли однозначное решение по отношению к новой технологии. Из-за сложности связывания данных и обмена ещё нет уверенности в том, что эту технологию не запретят. Хотя она прозрачна и безопасна.

Ещё одна проблема может появится, когда в частные руки начнут попадать большие вычислительные мощности. Это может произойти с распространением технологий квантовых компьютеров. В теории есть возможность взлома всей базы данных и ее изменения, при условии, что вычислительная мощность злоумышленников будет больше 51% от мощности всей сети.

Заключение

Реализация вышеописанной системы уже началась. Например, ряд организаций (Bosch, Cisco, US Bank, Ledger, IOTA, Qtum, Chain of Things и другие) основали Trusted IoT Alliance [9]. Целью Альянса является создание надежного Интернета вещей, который связывает криптографические идентификаторы с метаданными, чтобы предоставить объектам эквивалент цифровых и портируемых документов, которые могут быть инвентаризированы и управляемы в рамках блокчейн.

Таким образом, блокчейн действительно способен обеспечить доступность, целостность и конфиденциальность данных, циркулирующих в

Интернете вещей, а также настроить непрерывное обновление программного обеспечение устройств с целью исправления найденных после ввода в эксплуатацию уязвимостей. Это обеспечивается посредством распределенной архитектуры хранения зашифрованных данных в структуре связного списка. Каждый блок связан с предыдущим по хэшу.

В то же время, блокчейн не может полностью заменить все имеющиеся технологии из-за слабых мощностей современных компьютеров. Когда технологии смогут обеспечить данную технологию необходимыми мощностями, могут возникнуть новые проблемы с разрешением проблемы взлома зашифрованных данных.

Библиографический список

1. В «Газпром Нефть» испытали блокчейн и Интернет вещей в логистике. // Газпром Нефть URL: http://www.gazprom-neft.ru/press-center/news/1388456/ (дата обращения: 26.05.2018).
2. Попов А.А. Проблемы повышения информационной безопасности облачных информационных сервисов при формировании инновационной ИТ-инфраструктуры организации по управлению многоквартирными домами // Современные проблемы науки и образования. 2013. № 3.
3. Попов А.А. Разработка политики информационной безопасности для управления многоквартирными домами с использованием облачных информационных сервисов // Международный журнал фундаментальных и прикладных исследований. 2016. № 1-4. С. 497-502.
4. Токмакова Н.Р. Операционные системы для работы с Интернетом вещей М.: Молодежный научный вестник, 2017.
5. A Secure Model of IoT with Blockchain. // MIT TEchnology Overview. URL: https://www.technologyreview.com/s/603298/a-secure-model-of-iot-with-blockchain/ (дата обращения: 27.05.2018).
6. Blockchain And The Internet Of Things: 4 Important Benefits Of Combining These Two Mega Trends. // Forbes. URL: https://www.forbes.com/sites/bernardmarr/2018/01/28/blockchain-and-the-internet-of-things-4-important-benefits-of-combining-these-two-mega-trends/ (дата обращения: 27.05.2018).
7. Blockchain for IoT security. // Get Connected Blog. URL: https://blog.nordicsemi.com/getconnected/blockchain-for-iot-security (дата обращения: 25.05.2018).
8. How blockchain can secure the IoT. // Computer Weekly. URL: https://www.computerweekly.com/news/252433944/How-blockchain-can-secure-the-IoT (дата обращения: 25.05.2018).
9. Trusted IoT Alliance. // URL: https://www.trusted-iot.org/ (дата обращения: 27.05.2018).
10. Using Blockchain to Secure the «Internet of Things». // Scientific American. URL: https://www.scientificamerican.com/article/using-blockchain-to-secure-the-internet-of-things/ (дата обращения: 27.05.2018).