Внедрение технологии распределенного реестра в инфраструктуру IoT

А. А. Салагаев, С. А. Молодяков
Санкт-Петербургский политехнический университет Петра Великого
Санкт-Петербург, Россия
gitsartem@gmail.com, samolodyakov@mail.ru

***Аннотация*. Применение приложений IoT к различным аспектам жизни человека в обществе влечет за собой новые проблемы и вызовы. Одной из таких проблем является целостность и безопасность данных внутри IoT-систем. Стремительное развитие блокчейн технологий, основанных на децентрализованных распределенных системах реестров, предоставляют решение, которое можно использовать в IoT. Блокчейн и смарт-контракты обеспечивают безопасность и целостность данных. Однако, внедрение криптографических блокчейн механизмов в IoT системы привносит ряд проблем и вызовов, связанных с масштабируемостью, хранением данных, безопасностью и приватностью данных. В частности производительность блокчейн сети связана с принципами работы механизма консенсуса, с точки зрения конфиденциальности данных, обработки транзакций и масштабируемости сети. В данной работе рассматриваются проблемы интеграции блокчейн технологий в IoT и решение, основанное на построении направленного ацикличного графа, вместо блокчейн сети, которое может стать основой для преодоления этих препятствий.**

Ключевые слова: системы распределенного реестра; блокчейн; интернет вещей; направленный ациклический граф

I. Связанные исследования

С распространением Интернета Вещей (IoT) все больше и больше устройств подключаются к интернету. Например, благодаря прогрессу в IoT и технологиях облачных вычислений, которые послужили гигантским толчком к развитию таких направлений как: Умные Города, Умная Общественная Безопасность (SPS), система автоматизации подготовки и контроля технологических процессов на производственных участках [13]. Сообщается о работах, направленных на решение проблем, связанных с интеграцией систем IoT с использованием механизмов блокчейн и интеллектуальных контрактов. Например, система общественной безопасности [1], интеллектуальная система наблюдения [2, 3], система социального кредита [4, 5, 6], децентрализованный рынок данных [7], космические и авионические системы [8, 9], данные биометрической визуализации [12], идентификация аутентификации и контроль доступа [10, 11]. Все эти исследования подтвердили, что блокчейн и умные контракты способны создать децентрализованный механизм безопасности для систем IoT. Они также показали, что, однако, прямая интеграция существующих технологий блокчейн, ориентированных на криптовалюту, в системы IoT затрудняется рядом проблем, связанных с масштабируемостью, интенсивностью вычислений, емкостью хранения, безопасностью данных и сохранением конфиденциальности.

II. Вызовы, возникающие при интеграции

Так как традиционные блокчейн сети, например как биткойн, были разработаны для сетей содержащих мощные девайсы, компьютеры пользователей и стабильное окружение сети. Следовательно, это не удовлетворяет требованиям IoT, где вычислительные мощности, объёмы хранения и потребления энергии ограничены. Известные вызовы, возникающие при интеграции, представлены ниже.

- Компромисс между масштабируемостью и эффективностью: IoT приложения, такие, например, как умная система наблюдения, генерирует огромное количество транзакций с данными от пользователей и сервисов, где пропускная способность и низкая задержка становятся ключевыми метриками для протоколов IoT.
- Стоимость подтверждения транзакции и ее хранения. Устройства IoT ограничены в вычислительных возможностях и хранение данных на устройстве, а также высокой сложности механизмов консенсуса, основанных на вычислительных криптографических алгоритмах, таких как PoW. Кроме того, блокчейн работает в одноранговой сети, а протокол консенсуса требует частой передачи и обмена данными для обеспечения согласованности записей в распределенном реестре.
- Конфликты между прозрачностью и конфиденциальностью: прозрачность позволяет всем участникам получать доступ к данным блокчейна и проводить аудит транзакций. Однако это вызывает обеспокоенность по поводу вопросов конфиденциальности для некоторых систем IoT, где собранные конфиденциальные данные пользователя должны быть конфиденциальными и доступными только для уполномоченных лиц.
- Безопасность данных IoT и блокчейн сети: устройства IoT уязвимы к сетевым атакам по сравнению с компьютерами и облачными сервисами.

III. Предлагаемое решение

Целью данной работы является описание модели сохранение записей в системе распределенного реестра, которая может работать с устройствами IoT с ограниченными ресурсами.

Для достижения цели требуются три проектных решения:

- Использование DAG [14] для хранения данных записей.
- Использование PoA [15] как проверочную функцию, чтобы позволить узлам добавлять новые записи.
- Обеспечение надёжности системы с помощью набора политик безопасности.

На основе рассмотренных способов реализации распределенного реестра мной предлагается модель, в которой есть допущения, что каждый объект является действительным клиентским узлом или устройством, развёрнутым бизнес-провайдером или участвующими партнёрами, которые авторизованы для доступа к записям графа. Каждый узел в системе проходит через систему идентификации. В частности: каждый объект доверяет менеджеру идентификации, то есть устанавливает цифровой сертификат. Объекты в системе имеют идентификационное имя, и подпись, чтобы связать имя объекта с парой открытого/секретного ключей.

IV. Направленный ациклический граф

DAG – ориентированный граф, в котором отсутствуют направленные циклы, но могут быть «параллельные» пути, выходящие из одного узла и разными путями, приходящие в конечный узел. Происходит запись и блокировка каждой записи в системе, создавая и поддерживая тем самым неизменный и распределенный реестр. Все объекты в системе, включая менеджер идентификации, вместе образуют одноранговую (P2P) сеть. Каждый узел добавляет свои новые записи в граф после согласования с записями других участников и после проверки их действительности.

Консенсус по записи в реестр достигается, если достаточное количество транзакций утвердило эту запись. Количество утверждающих транзакций называется весом ветви в графе. Система сохраняет все записи в направленном ациклическом графе (DAG) вместо единого блокчейна. В DAG вновь сгенерированная запись (вершина) будет помещена рядом с (цепочкой) ($n \geq 2$) существующими записями в DAG, устанавливая утверждения от новой записи к предыдущим. Хвостовые записи – это те записи, которые не утверждены другими записями в DAG.

После завершения этого процесса узел отправляет запись в одноранговую сеть, где другие узлы вписывают новую транзакцию в свои локальные реестры. Система использует набор политик безопасности для обработчиков транзакций, чтобы проверять входящие записи, предотвращая потенциальные угрозы, такие как спам-атака или ситуации, когда транзакция ничего не вносит в систему. Эти политики безопасности гарантируют пороговую схему (k, N) k <N, в которой, если не будет скомпрометировано больше N пиров, система останется защищённой.

V. Консенсус на основе весов ветвей графа

Когда объект утверждает запись, он подтверждает ее действительность и те записи, которые она утвердила прямо или косвенно, до достижения подтверждённых записей. На рис. 1 показан пример такого процесса в случае, когда n = 2.

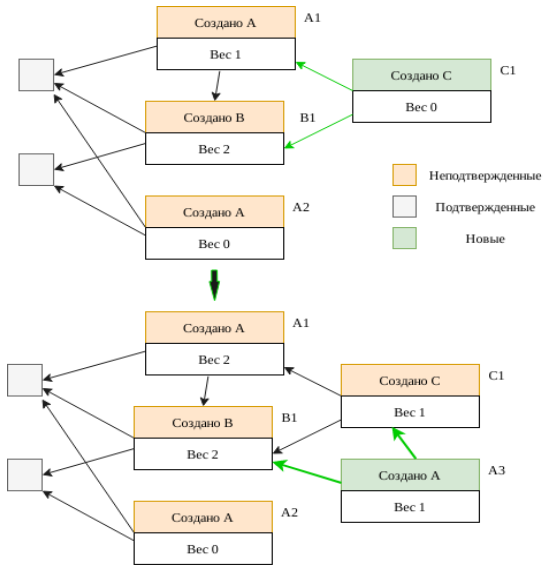

Рис. 1. Пример увеличения веса. Присоединение C1 увеличивает вес A1 и B1 на 1. Затем присоединение A3 увеличивает вес C1 и A1, как прямо так и косвенно, но не у B1, так как вес B1 был уже подтвержден A

- Чтобы быть более конкретным, этот объект должен проверить, что все соответствующие записи удовлетворяют следующим четырём требованиям: Они несут действительные PoA.
- Хвостовые записи не могут утверждать запись, вес которой слишком велик согласно политике вкладов.
- Запись не может одобрить другую запись, сгенерированную той же сущностью с учетом политики блокировки.
- Полезная нагрузка, переносимая в этих записях, удовлетворяет семантике уровня приложения.

Первые три требования определяются моделью, а последнее контролируется уровнем приложения. Система достигает консенсуса за счёт веса транзакций. Вес записи – это число других записей-транзакций, утверждающих ее прямо или косвенно, указывающих на нее. Вновь сгенерированные записи имеют нулевой вес. После объявления и распространения по сети P2P она получает

одобрение, что сопровождается совокупным увеличением её веса. Записи классифицируются по тому, превышает ли их вес пороговое значение, конечная цель записи – набрать достаточно веса, чтобы получить подтверждение. Если это невозможно, однако, она может быть аннулирована после определённого периода подачи заявок. Напротив, подтверждённая запись означает, что система достигла консенсуса в отношении ее достоверности и будет постоянно хранить ее. Примерная схема поведения отображена на рис. 2.

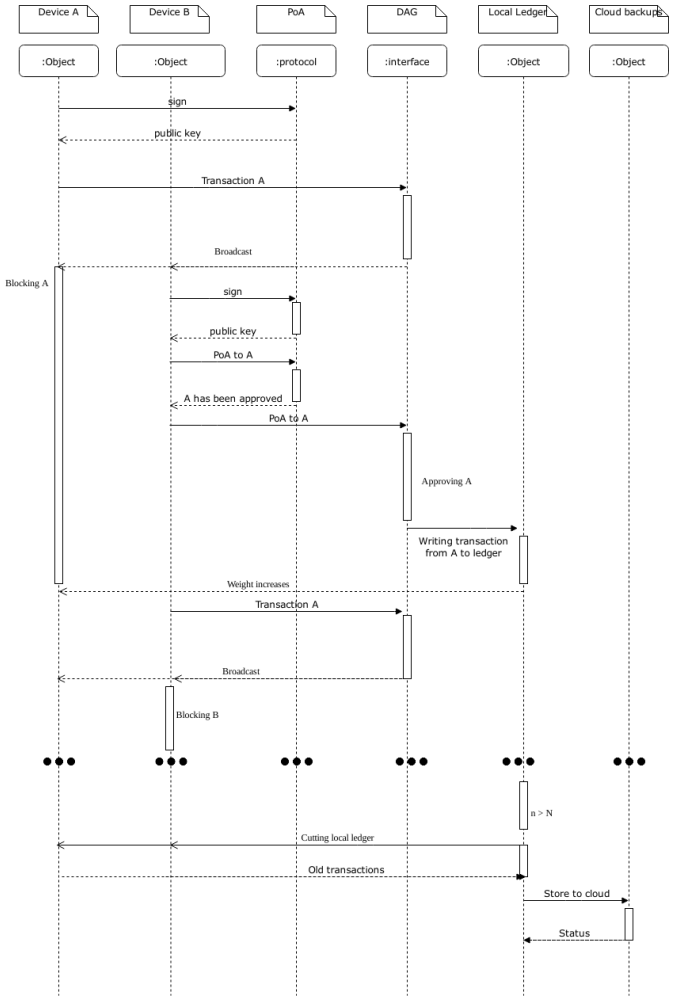

Рис. 2. Пример поведения системы

VI. Заключение

Внедрение технологий распределенных реестров в IoT – непростая задача, и в таких моделях существует множество препятствий. Представлена модель на основе направленного ациклического графа – DAG, набор политик безопасности и алгоритм определения консенсуса PoA для распределенных систем с ограниченными ресурсами. Предлагаемый подход обходит централизованные зависимости, создавая легкое децентрализованное решение. Однако необходимо провести сравнительное изучение различных эталонных решений по обеспечению безопасности в крупных сетях, а также провести оценку сценариев атак и угроз, чтобы утверждать, что предложенный подход удовлетворяет поставленным задачам. В качестве будущего исследования хотелось бы посмотреть на практическую реализацию предложенной системы.

Список литературы

[1] Xu R., Nikouei S.Y., Chen Y., Blasch E., Aved A.: Blendmas: A blockchain-enabled decentralized microservices architecture for smart public safety. In: The 2019 IEEE International Conference on Blockchain (Blockchain-2019), pp. 1–8. IEEE (2019)

[2] Nikouei S.Y., Xu R., Nagothu D., Chen Y., Aved A., Blasch E.: Real-time index authentication for event-oriented surveillance video query using blockchain. In: 2018 IEEE International Smart Cities Conference (ISC2), pp. 1–8. IEEE (2018)

[3] Lin X., Xu R., Chen Y., Lum J.: Enhance generalized exchange economy using blockchain: a time banking case study. the IEEE Blockchain Technical Briefs (2019)

[4] Lin X., Xu R., Chen Y., Lum J.K.: A blockchain-enabled decentralized time banking for a new social value system. In: 2019 IEEE Conference on Communications and Network Security (CNS), pp. 1–5. IEEE (2019)

[5] Xu R., Lin X., Dong Q., Chen Y.: Constructing trustworthy and safe communities on a blockchain-enabled social credits system. In: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 449–453. ACM (2018)

[6] Xu R., Ramachandran G.S., Chen Y., Krishnamachari B.: Blendsm-ddm: Blockchain-enabled secure microservices for decentralized data marketplaces. In: 2019 IEEE International Smart Cities Conference (ISC2). IEEE (2019)

[7] Blasch E., Xu R., Chen Y., Chen G., Shen D.: Blockchain methods for trusted avionics systems. arXiv preprint arXiv:1910.10638 (2019)

[8] Xu R., Chen Y., Blasch E., Chen G.: Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness. Optical Engineering 58, 58–58–16 (2019). DOI 10.1117/1.OE.58.4.041609. URL https://doi.org/10.1117/1.OE.58.4.041609

[9] Xu R., Chen Y., Blasch E., Chen G.: Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1027–1034. IEEE (2018)

[10] Xu R., Chen Y., Blasch E., Chen G.: Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. Computers 7(3), 39 (2018)

[11] Wang W., Hoang D.T., Hu P., Xiong Z., Niyato D., Wang P., Wen Y., Kim D.I.: A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 7, 22328–22370 (2019)

[12] A.D. Dwivedi, P. Morawiecki, and G. Srivastava, “Differential cryptanalysis of round-reduced speck suitable for internet of things devices,” IEEE Access, vol. 7, pp. 16 476–16 486, 2019.

[13] Pavel Drobintsev, Lina Kotlyarova, Nikita Voinov, Alexey Tolstoles, Alexey Maslakov, Irina Khrustaleva Automating preparation of small-scale production for reliable net-centric IoT workshop. CEUR Workshop Proceedings 2019 Actual Problems of System and Software Engineering 75-85

[14] S. Popov, “The tangle,” White paper, 2018. [Online]. Available: https://www.iota.org/research/academic-papers.

[15] D. Puthal and S.P. Mohanty, “Proof of Authentication: IoT-friendly View publication stats Blockchains,” IEEE Potentials, vol. 38, no. 1, 2019.