Прототип низкоресурсного блокчейн-протокола для Интернета вещей с HMAC-защитой и edge-валидацией

О. Л. Никифоров*, Б. Г. Мубараков‡

Разработан программный прототип низкоресурсного блокчейн-протокола для Интернета вещей. Конечные устройства формируют сообщения с хешем данных и кодом аутентификации HMAC, а доверенные edge-узлы проверяют сообщения и формируют блоки. Такое разделение переносит ведение реестра на более мощные узлы. При сравнении на одном оборудовании в одинаковых условиях выполнения прототип обработал 5000 событий с пропускной способностью 4980,52 события/с против 306,53 у контрольной модели.

Ключевые слова: Интернет вещей, блокчейн, программный прототип, HMAC, edge-вычисления, дерево Меркла.

1. Введение

Датчики Интернета вещей формируют потоки измерений, для которых важны проверка источника и целостности данных. Ограниченные память, вычислительная мощность и запас энергии затрудняют хранение цепочки блоков и участие устройств в согласовании записей [1].

Разделение функций между устройствами и более мощными узлами используется в архитектуре LSB [2], а применение HMAC в низкоресурсном блокчейне рассматривается в [3]. В данной работе этот подход реализован в прототипе LWB-HMAC-edge для регистрации событий. Цель исследования — объединить аутентификацию сообщений, хранение хешей и пакетное подтверждение блоков, а затем оценить производительность полученной программной реализации.

* *Никифоров Олег Леонидович* — магистрант, Институт вычислительной математики и информационных технологий, Казанский (Приволжский) федеральный университет, e-mail: oleg_02.12.2002@mail.ru.

Nikiforov Oleg Leonidovich — Master's student, Institute of Computational Mathematics and Information Technologies, Kazan Federal University.

‡ *Мубараков Булат Газинурович* — кандидат технических наук, доцент кафедры системного анализа и информационных технологий, Институт вычислительной математики и информационных технологий, Казанский (Приволжский) федеральный университет, e-mail: mubbulat@mail.ru, ORCID: 0000-0002-7628-9870.

Mubarakov Bulat Gazinurovich — Candidate of Technical Sciences, Associate Professor, Department of System Analysis and Information Technologies, Institute of Computational Mathematics and Information Technologies, Kazan Federal University.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

2. Архитектура и принцип работы

Конечное устройство формирует сообщение, а edge-узлы — более мощные компьютеры, например локальные шлюзы, — проверяют его и ведут реестр. Устройство освобождается от хранения цепочки и подтверждения блоков.

Устройство вычисляет хеш данных по алгоритму SHA-256 и передаёт его вместе со своим идентификатором, номером и временем события, длиной данных и кодом аутентификации HMAC. Хеш позволяет впоследствии проверить соответствие исходных данных сохранённой записи. В реестре фиксируется компактное представление события; полные измерения могут храниться отдельно.

Для аутентификации каждому устройству назначается индивидуальный секретный ключ, заранее доступный проверяющим узлам. HMAC защищает поля сообщения от незаметного изменения участником, не знающим ключа. Узел проверяет идентификатор устройства и код аутентификации; успешно проверенные сообщения поступают в очередь формирования блоков. Решение ориентировано на закрытую инфраструктуру с доверенными проверяющими узлами и защищёнными ключами: HMAC подтверждает владение общим секретом, а не служит публичной цифровой подписью.

Сообщения объединяются в блоки по порядку поступления. Каждый блок содержит ссылку на предыдущий, а дерево Меркла объединяет идентификаторы транзакций в общий контрольный хеш. В модели четыре узла проверяют сообщения, а для подтверждения блока требуются три голоса. Пакетная обработка позволяет выполнять подтверждение сразу для группы событий без дополнительного вычислительного поиска.

Через каждые десять блоков сохраняется локальный контрольный хеш состояния цепочки. Голосование моделируется внутри одной программы. Внешняя фиксация контрольных хешей для независимого аудита и проверка распределённой отказоустойчивости предусмотрены на следующем этапе.

3. Экспериментальная оценка

Прототип реализован на Python. Сравнение проводилось на одном и том же оборудовании, в одинаковых условиях выполнения. Оба режима обрабатывали по 5000 событий от 50 моделируемых устройств; размер блока составлял до 32 транзакций. В LWB-HMAC-edge использовались

четыре проверяющих узла. Все компоненты моделировались в одном процессе.

Контрольная модель сохраняла полные данные и использовала Proof-of-Work (PoW) — подтверждение блока посредством вычислительного поиска. Объём и состав записей различались в соответствии с архитектурой каждого режима. Оценивались время обработки всего набора событий и пропускная способность.

Таблица 1: Результаты сравнения программных конфигураций

Показатель	LWB-HMAC-edge	Контрольная модель
Время выполнения, с	1,004	16,312
Пропускная способность, событий/с	4980,52	306,53

В проведённом запуске пропускная способность прототипа оказалась выше в 16,25 раза, а время выполнения сократилось на 93,85%. Подтверждение блоков голосованием исключает такой поиск, а работа с хешами отделяет реестр от хранения полных измерений.

Результаты характеризуют программные конфигурации в целом, без выделения вклада отдельных механизмов. Сетевая задержка и энергопотребление датчиков требуют отдельных аппаратных измерений.

4. Заключение

Разработан прототип, объединяющий HMAC-аутентификацию, хранение хешей данных и пакетное подтверждение блоков. Конечное устройство формирует собственную запись, а ведение реестра выполняют доверенные edge-узлы.

Сравнение на одном оборудовании показало увеличение пропускной способности относительно выбранной контрольной модели. Дальнейшая работа направлена на испытания в распределённой сети и на микроконтроллерах, реализацию смены ключей и защиты от повторной передачи сообщений, а также подключение внешнего аудита состояния реестра.

Список литературы

[1] H.-N. Dai, Z. Zheng, Y. Zhang, “Blockchain for Internet of Things: A Survey”, *IEEE Internet of Things Journal*, **6**:5 (2019), 8076–8094. DOI: 10.1109/JIOT.2019.2920987.

[2] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, “LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy”, arXiv: 1712.02969. DOI: 10.48550/arXiv.1712.02969.

[3] S. Panasenko, “A Lightweight Blockchain for the Internet of Medical Things Using Hash-based Message Authentication Codes”, *2023 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE. DOI: 10.1109/IWCMC58020.2023.10182980, 2023, 1095–1100.

Статья поступила 9 октября 2026 г.

A Prototype Lightweight Blockchain Protocol for the Internet of Things with HMAC Protection and Edge Validation

O. L. Nikiforov, B. G. Mubarakov

A prototype lightweight blockchain protocol for the Internet of Things is developed. End devices generate messages containing a data hash and an HMAC authentication code, while trusted edge nodes verify messages and form blocks. This division transfers ledger maintenance to more capable nodes. In a comparison performed on the same hardware under identical execution conditions, the prototype processed 5000 events at 4980.52 events/s versus 306.53 for the control model.

Keywords: Internet of Things, blockchain, software prototype, HMAC, edge computing, Merkle tree.

References

[1] H.-N. Dai, Z. Zheng, Y. Zhang, “Blockchain for Internet of Things: A Survey”, *IEEE Internet of Things Journal*, **6**:5 (2019), 8076–8094. DOI: 10.1109/JIOT.2019.2920987.

[2] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, “LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy”, arXiv: 1712.02969. DOI: 10.48550/arXiv.1712.02969.

[3] S. Panasenko, “A Lightweight Blockchain for the Internet of Medical Things Using Hash-based Message Authentication Codes”, *2023 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE. DOI: 10.1109/IWCMC58020.2023.10182980, 2023, 1095–1100.

Received on October 9, 2026