Табл. 3. Значення затримок передавання пакетів у комп'ютерній мережі (експеримент № 2)

Назва затримки	Назва параметра		
	значення параметра P_{ai}	значення параметра P_{bi}	відносний коефіцієнт зміни K_i
Середня затримка передавання пакетів, *s*	0,0291	0,0254	12,71
Максимальна затримка передавання пакетів, *s*	0,086	0,069	19,77

$$K_i = \frac{P_{a_i} - P_{b_i}}{P_{a_i}} \times 100\%, \ \forall i \in n. \qquad (2)$$

Висновки. З результатів моделювання можна зробити висновки, що впровадження методу Ateb-прогнозування інтенсивності трафіку потоку, запрограмованим на використання інформації щодо зібраних та оброблених значень параметрів трафіку потоку у вузловому обладнанні, створює умови для прогнозування значень цих параметрів для формування рішень адаптивного управління, і цим самим підвищує ефективність використання вузлового обладнання та якість роботи комп'ютерної мережі.

Проведені дослідження показують покращення роботи комп'ютерної мережі за параметрами середньої затримки передавання пакетів на 12-14 %, та максимальної затримки на 14-19 %.

Реалізоване комп'ютерне імітаційне моделювання показує підвищення ефективності роботи комп'ютерної мережі на основі вдосконалення перерозподілу завантаження її вузлового обладнання.

Література

1. Вишневский В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. – М. : Изд-во "Техносфера", 2003. – 512 с.
2. ДСТУ В 3265-95. Зв'язок військовий. Терміни та визначення. – К. : Вид-во УкрНДІССІ, 1995. – 23 с.
3. Дымарский Я.С. Управление сетями связи: принципы, протоколы, прикладные задачи / Я.С. Дымарский., Н.П. Крутякова, Г.Г. Яновский. – М. : Изд-во "ЭкоТрендз", 2003. – 384 с.
4. Cisco VNI Forecast Widget. [Electronic resource]. – Mode of access http://www.cisco.com
5. Dronjuk Ivanna. Asymptotic method of traffic simulation (Distributed Computer and Communication Networks) / Ivanna Dronjuk, Maria Nazarkevych, Olga Fedevych // Communications in Computer and Information Science. Springer. – 2014. – Vol. 279. – Pp. 136-144.
6. The Opte Project. [Electronic resource]. – Mode of access http://www.opte.org/.
7. Nycz M. An analysis of the extracted parts of Opte Internet topology. // Computer Networks / M. Nycz, T. Nycz, T. Czachórski // 22nd International Conference, CN 2015 Brunów, Poland, June 16-19, 2015. Springer International Publishing Switzerland, 2015. – Pp. 371-381.
8. IEEE 802 LAN/MAN Standards Committee. [Electronic resource]. – Mode of access http://www.ieee802.org/.
9. OMNeT++ Community Site. [Electronic resource]. – Mode of access http://www.omnetpp.org
10. Nycz T. A Numerical Comparison of Diffusion and Fluid-Flow Approximations Used in Modelling Transient States of TCP/IP Networks / T. Nycz, M. Nycz, T. Czachórski // Computer Networks // 21st International Conference, CN 2014 Brunów, Poland, June 23-27, 2014. Springer International Publishing Switzerland, 2014. – Pp. 213-222.

Надійшла до редакції 10.11.2016 р.

Федевич О.Ю. **Применение метода Ateb-прогнозирования для уменьшения интенсивности загрузки каналов компьютерных сетей**

Рассмотрено современное состояние роста объемов данных в компьютерных сетях. Проанализированы данные корпорации Cisco. Описана разработанная компьютерная имитационная модель сети с помощью программного обеспечения OMNeT++. Осуществлено имитационное моделирование двух топологий компьютерных сетей, полученных из базы данных проекта The Opte Project. Эффективность предложенного метода Ateb-прогнозирования трафика потока доказана экспериментально. Показано, что благодаря применению метода Ateb-прогнозирования средняя задержка передачи пакетов уменьшилась на 12-14 %, а максимальная задержка уменьшилась на 14-19 %. Эксперименты проиллюстрированы графиками.

Ключевые слова: трафик потока, компьютерная сеть, имитационная модель, OMNeT ++, The Opte Project, Ateb-прогнозирование.

Fedevych O.Yu. **Application of Ateb-prediction Method to Reduce the Downloading Intensity of Network Channels**

This article shows the current state of data volume growth in computer networks. Cisco corporation data were considered and analyzed. Developed computer simulation model of the network through OMNeT++ software was described. Simulation of two topologies of computer networks, obtained from the database of The Opte Project was done. The effectiveness Ateb-prediction method of traffic flows was proved experimentally. It is shown that due to the use of the proposed Ateb-prediction method average delay in the transmission of packets decreased by 12-14 %, and the maximum delay decreased by 14-19 %. The experiments were illustrated by graphs.

Keywords: traffic flow, computer network, simulation model, OMNeT++, The Opte Project, Ateb-prediction.

УДК 004.75

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ

Н.Г. Яцків[1], С.В. Яцків[2]

Досліджено, що технологія Blockchain має значний потенціал застосування у різних сферах діяльності, однак найбільш перспективою сферою застосування цієї технології є Інтернет речей і кіберфізичні системи. Технологія Blockchain пропонує рішення проблеми безпеки і конфіденційності у середовищі Інтернет речей, забезпечуючи новий обчислювальний шар, де дані можуть бути безпечно оброблені та проаналізовані, залишаючись приватним. Розкрито потенційні переваги та виділено проблеми, які потрібно вирішити для ефективного використання цієї технології у середовищі Інтернет речей.

Ключові слова: Інтернет речей, блокчейн, біткойн, хеш-функція, транзакція, безпека.

Вступ. Інтернет речей (Internet of Things, IoT) є наступним етапом еволюції Інтернету на шляху до всеосяжного Інтернету (Internet of Everything, IoE*)*. IoT містить широкий спектр речей, таких як сенсори, виконавчі механізми і послуги, розгорнуті різними організаціями і приватними особами для підтримки різноманітних додатків. Термін "Інтернет речей" (IoT) вперше ввів Кевін Ештон у 1999 р. для опису системи, в якій фізичні об'єкти пов'язані зі сенсорами і мережею Internet **[**1**]**.

Згідно з прогнозами Gartner, у 2020 р. у світі буде 20,8 млрд підключених пристроїв IoT **[**2**]**.

[1] доц. Н.Г. Яцків, канд. техн. наук – Тернопільський національний економічний університет;
[2] студ. С.В. Яцків – Тернопільський національний економічний університет

Потенційними галузями для застосування IoT є сільське господарство, моніторинг навколишнього середовища, моніторинг здоров'я, смарт-виробництво, інтелектуальні міста та ін. [3, 4]. Проте збільшення пристроїв збирання та оброблення даних, підключених до мережі Інтернет, призводить до виникнення проблем, пов'язаних з безпекою даних. Приділення недостатньої уваги проблемі безпеки у середовищі IoT може призвести, наприклад, до атак на секретність і аутентифікацію або атак на відмову в обслуговуванні (DoS) [5].

Мета роботи полягає у визначенні перспективи та потенційних переваг використання технології блокчейн для підвищення ефективності функціонування мережі Інтернет речей.

Перспективи використання технології блокчейн. Blockchain є новою інформаційною технологією, яка набуває розвитку та використання у багатьох галузях. Першим і найбільш відомим прикладом використання технології Blockchain є криптовалюта – Bitcoin [6]. На цей час криптовалюта перетворилась у визнаний платіжний засіб, віртуальну валюту, яку приймають великі та дрібні підприємства, корпорації та сервіси.

На сьогодні ведуть дослідження та здійснюють реалізацію низки проектів з використанням технології Blockchain у таких галузях, як охорона здоров'я, засоби масової інформації, електронне голосування, зберігання файлів, смарт-контракти, страхування, державний сектор (видача паспортів, збір податків, реєстрація земельних ділянок) та ін. [5, 7].

Корпорація IBM досліджує технологію Blockchain і працює над створенням програмного забезпечення, за допомогою якого партнери зможуть укладати цифрові договори, що будуть фіксуватися у глобальній мережі. IBM також реалізує проект під назвою Adept, мета якого відстеження підключених до мережі пристроїв за допомогою технології Blockchain [8, 10].

У роботі [11] запропоновано схему оновлення прошивки вбудованих пристроїв у середовищі IoT на основі технології Blockchain, яка перевіряє версію та правильність прошивки, а також дає змогу завантажувати останню версію прошивки, що, своєю чергою, забезпечить зменшення часу вікна атаки.

У [12] представлено принципи інтеграції технології Blockchain і групи робототехнічних систем (swarm robotics), яка може забезпечити інноваційні рішення та стати ключем до серйозного прогресу у груповій робототехніці, зокрема: 1) можуть бути реалізовані нові моделі безпеки, методи забезпечення конфіденційності даних і способи ідентифікації групи роботів; 2) можуть бути розроблені нові методи прийняття рішень і виконання спільних місій на основі виконання спеціальних операцій у Blockchain, які дають робототехнічним агентам голосувати і досягати угоди; 3) роботи можуть функціонувати в змінюваних умовах без змін в алгоритмі управління.

Завдяки децентралізованій структурі, високій надійності і відмовостійкості, технологія Blockchain може бути використана у системах автоматизованого транспортування, логістики, складських системах, хмарних обчисленнях, а також в Інтернет речей та кіберфізичних системах [13, 14].

Проведений аналіз показав, що технологія Blockchain має значний потенціал і перспективи застосування в різних сферах діяльності, однак найбільш цікавою сферою для цієї технології є Інтернет речей і кіберфізичні системи, які матимуть найбільшу вигоду від цієї технології.

Технологія Blockchain. У 2008 р. автор або група авторів під псевдонімом Satoshi Nakamoto опублікували статтю "Bitcoin: A Peer-to-Peer Electronic Cash System" з описом концепції і принципів роботи платіжної системи у вигляді однорангової мережі [6]. У 2009 р. було представлено протокол криптовалюти Bitcoin та опубліковано код програми-клієнта. Ключова особливість запропонованої концепції полягала в тому, що онлайн платежі між клієнтами здійснюються без центральної фінансової установи, яка виконує роль довіреної структури, з використанням криптографічних методів та публічної розподіленої бази даних, яка складається з ланцюжка блоків (Blockchain) [15].

Blockchain – це розподілена структура даних, яка складається з послідовності блоків, в якій кожний блок містить хеш попереднього блоку, утворюючи, як наслідок, ланцюг блоків (рис. 1). Перший блок у ланцюжку (батьківський блок, genesis block) розглядають як окремий випадок, оскільки в нього відсутній попередній блок. Blockchain працює як розподілена база даних, яка здійснює облік усіх операцій у мережі. Операції мають відзначку часу і зберігаються у блоках, де кожен блок ідентифікується своїм криптографічним хешем. Blockchain повністю зберігається у кожному вузлі мережі. Для роботи Blockchain не потрібно довіри між вузлами мережі, оскільки будь-який вузол може самостійно перевірити, чи збігається його копія бази з копіями, які зберігаються в інших вузлах [16].

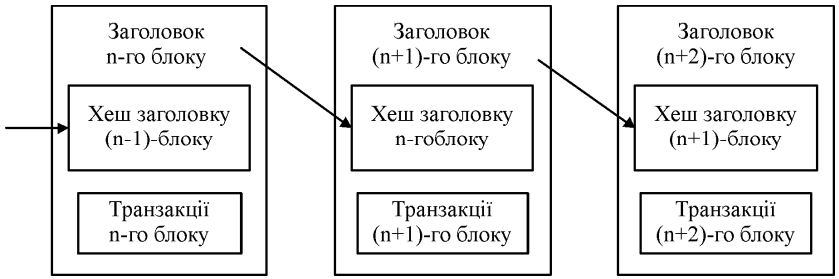

Рис. 1. Спрощена послідовність блоків

Принцип функціонування технології Blockchain розглянемо на прикладі криптовалюти "біткойн". Як хеш-функцію криптовалюта біткойн використовує криптографічну хеш-функцію SHA-256 [15]. Для перевірки цілісності даних у блоці використовується деревоподібне хешування (дерево Меркле), яке представляє особливу структуру даних, що містить інформацію про здійснені транзакції. Для цього з кожної транзакції обчислюється хеш, а потім з кожної пари хешів обчислюється новий хеш пари. Ця процедура повторюється доти, поки не залишиться один хеш. Якщо пара в хешу відсутня, то він переноситься на новий рівень без змін (рис. 2).

Групу транзакцій після перевірки записують у спеціальний блок (див. рис. 2). Блок складається із заголовка та списку транзакцій (Tr A, Tr B, …). Заголовок блоку включає хеш даного блоку, хеш попереднього блоку (Previous

Hash), хеш транзакцій (Merkle Root) та додаткову службову інформацію (Nonce, Timestamp). Відзначка про час (Timestamp) вказує, коли був створений блок, і надає докази того, що дані в блоці існували в певний момент часу.

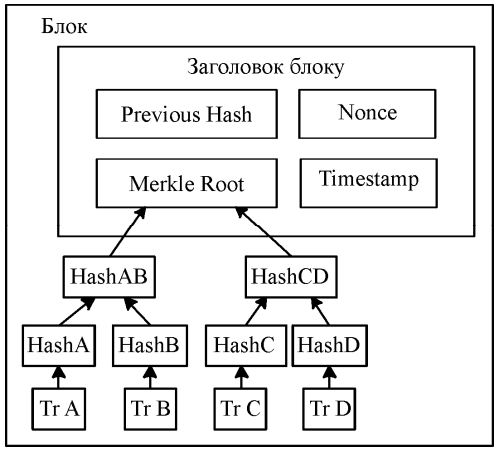

Рис. 2. Структура блоку

Для формування нового блоку вузла потрібні дані: хеш попереднього блоку в ланцюжку; хеш Merkle для операцій, які потрібно помістити у блок; час (Timestamp) та одноразовий код (Nonce), вибраний псевдовипадкових чином.

Для підтвердження коректності блоку потрібно обчислити хеш заголовка нового блоку, який повинен починатися із заданої кількості нулів. Дана задача відома, як доказ правильності роботи (proof-of-work), що базується на двох принципах: 1) зробити підтвердження транзакцій затратними для користувачів мережі у вигляді комп'ютерних обчислень; 2) здійснювати винагороду за допомогу у перевірці транзакцій.

Розв'язання задачі "доказ правильності роботи" полягає в тому, щоб знайти таке число *x*, яке додавши до повідомлення (набір транзакцій) *S*, забезпечить результат хешування, що починається із заданої кількості нулів. Обчислювальну складність задачі "доказ правильності роботи" розглянемо на прикладі. Позначимо через h – фіксовану хеш-функцію, вбудовану в протокол, S – черга незавершених транзакцій. Нехай S = "Internet of Things", одноразовий код x = 0. Обчислюємо хеш-функцію із комбінації ("Internet of Things0"):

h=sha256("Internet of Things0").
h= 'a47a5248711f9bba752137c5d809b0578fc5c038efa15f69d47e4e531a0a6da3'.

Якщо x=40, хеш-функція починається з двох нулів:

h = sha256 ("Internet of Things40").
h = '00dd26369b13e8d81d3e5afedcc2e847aaeaa476e5da8a15c77358761a1623ef'.

Якщо x=47304, хеш-функція починається з чотирьох нулів:

h = sha256 ("Internet of Things 47304").
h = '0000c75f1b2ba0cbc69068dee203907dd4b5ae6fe12aed0261052d25036d174a'.

Отже, складність задачі "доказ правильності роботи" можна змінювати задаючи певну кількість нулів на початку значення кеш-функції. Як видно з прикладу, відносно простим завданням є пошук числа, яке забезпечує 3-4 нулі, і, відповідно, значно складнішим буде знаходження числа, яке забезпечує 10-15 нулів на початку значення кеш-функції.

Новий блок приймається іншими вузлами мережі, якщо значення хешу заголовка дорівнює або менше заданого числа, величина якого періодично змінюється. Коли результат знайдено, сформований блок розсилається іншим вузлам, які його перевіряють. Якщо перевірка пройшла успішно, то блок додається в ланцюжок і наступний блок повинен включати в себе його хеш.

Робота, яку вузли повинні виконати для створення нового блоку, вимагає багато часу та обчислювальних ресурсів. Це знижує ймовірність того, що два блоки будуть зроблені одночасно, але така ситуація все-таки можлива. Коли це відбувається, то створюється розгалуження в Blockchain. У такому випадку вузли можуть почати будувати ланцюг на різних гілках. Щоб запобігти такій ситуації, кожен вузол відстежує всі гілки, але вузли будуть намагатися розширити тільки найдовшу гілку. При цьому, довжина визначається не кількістю блоків, а загальним обсягом роботи, яка затрачена на створення гілки, і визначається кількістю нулів на початку хешу блоку.

Обчислювальна складність перевірки транзакцій допомагає уникнути залежності від кількості вузлів у мережі, які може контролювати зловмисник. Отже, на перевірку впливає тільки загальна обчислювальна потужність вузлів. Отже, для зміни інформації в блоці зловмиснику потрібні значні обчислювальні ресурси, що робить це практично недоцільним.

Оскільки копії Blockchain зберігаються у вузлах розподіленої мережі, це робить технологію Blockchain стійкою до проблем з тимчасовим або постійним відключенням вузлів, пов'язаним із збоями обладнання або зв'язку, а також підключенням нових вузлів.

Переваги технології Blockchain. Переваги технології Blockchain, які забезпечують її ефективне використання у середовищі Інтернет речей **[**6, 11-13, 16, 17**]**:

1) Blockchain є публічною розподіленою базою всіх транзакцій у мережі, яка підтримується одноранговою мережею;
2) мережа Blockchain стійка до збоїв, оскільки вона функціонує без єдиної точки відмови;
3) Blockchain є незмінною і довговічною розподіленою базою і, як тільки транзакції записані в Blockchain, вони не можуть бути змінені або видалені;
4) мережа Blockchain має високий ступінь масштабованості;
5) усі транзакції в мережі Blockchain захищені криптографічними методами;
6) Blockchain дає змогу пристроям IoT здійснювати операції автономно без довіреної сторони.

Вказані переваги технології Blockchain роблять її перспективним інструментом для вирішення проблем у галузі безпеки і конфіденційності в IoT.

Незважаючи на вказані переваги, використання технології Blockchain у середовищі IoT має низку обмежень, які потребують вирішення:

1) створення блоків потребує значних обчислювальних ресурсів, тоді як більшість IoT пристроїв мають обмежені апаратні ресурси;
2) створення блоків займає багато часу, проте для більшості додатків IoT потрібна низька затримка реакції на подію;

3) протоколи Blockchain значно збільшують трафік у мережі, що може бути критичним для мереж IoT із бездротовими каналами зв'язку.

Технологія Blockchain пропонує рішення проблеми безпеки і конфіденційності у середовищі Інтернет речей, забезпечуючи новий обчислювальний шар, де дані можуть бути безпечно оброблені та проаналізовані, залишаючись приватним.

Для ефективного використання технології Blockchain у середовищі IoT має бути розроблена архітектура Blockchain, яка враховувала б зазначені вище обмеження IoT та забезпечувала безпеку і конфіденційність даних.

Висновки. Blockchain є відносно новою концепцією з високим потенціалом, відповідно потребує додаткових досліджень для її ефективного застосування у нових галузях, таких як кіберфізичні системи та Інтернет речей. Інтеграція технології Blockchain в Інтернет речей дасть змогу створити новий обчислювальний сегмент, в якому дані можуть бути безпечно оброблені та проаналізовані, при цьому залишаючись приватним, що забезпечить підвищення безпеки і конфіденційності під час використання пристроїв, підключених до Інтернету.

Література

1. Ashton K. That Internet of Things / K. Ashton // Thing. RFID Journal, 22 July 2009. [Electronic resource]. – Mode of access http://www.rfidjournal.com/articles/view?4986.
2. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. [Electronic resource]. – Mode of access http://www.gartner.com/newsroom/id/3165317.
3. Shancang Li. The internet of things: a survey / Li Shancang, Li Da Xu, and Shanshan Zhao // Information Systems Frontiers 2015, 17.2. – Pp. 243-259.
4. Whitmore Andrew. The Internet of Things – A survey of topics and trends / Whitmore Andrew, Anurag Agarwal, and Li Da Xu // Information Systems Frontiers 17.2, 2015. – Pp. 261-274.
5. Dorri, Ali. Kanhere, and Raja Jurdak / Ali Dorri, S. Salil // Blockchain in internet of things: Challenges and Solutions" *arXiv preprint arXiv:1608.05187*, 2016.
6. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Electronic resource]. – Mode of access https://bitcoin.org/bitcoin.pdf.
7. Christidis Konstantinos, Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. [Electronic resource]. – Mode of access http://ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf? arnumber=7467408.
8. Brody, Paul. Device democracy: Saving the future of the Internet of Things / Paul Brody, Pureswaran Veena // IBM, September, 2014.
9. Panikkar, B.S. ADEPT: An IoT Practitioner Perspective / B.S. Panikkar, S. Nair, P. Brody, & V. Pureswaran, 2014.
10. Veena P. Empowering the Edge-Practical Insights on a Decentralized Internet of Things. Empowering the Edge-Practical Insights on a Decentralized Internet of Things / P. Veena, S. Panikkar, S. Nair, P. Brody // IBM Institute for Business Value, 17 Apr. 2015. [Electronic resource]. – Mode of access http://www-01.ibm.com/common/ssi/cgi-bin/ssialias? infotype=PM&subtype=XB&htmlfid=GBE03662USEN#loaded.
11. Boohyung Lee. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment / Lee Boohyung, Lee Jong-Hyouk. The Journal of Supercomputing, 2016. – Pp. 1-16.
12. Ferrer E.C. The blockchain: a new framework for robotic swarm systems. arXiv preprint arXiv:1608.00695, 2016.
13. Bahga Arshdeep. Blockchain Platform for Industrial Internet of Things / Bahga Arshdeep, Vijay K. Madisetti // Journal of Software Engineering and Applications. – 2016. – № 9. – Pp. 533-546.
14. Мельник А.О. Кіберфізичні системи: проблеми створення та напрями розвитку // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні системи та мережі. – Львів : Вид-во НУ "Львівська політехніка". – 2014. – № 806. – С. 154-161.
15. Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014. – 298 p.

16. Crosby M. Blockchain technology: Beyond bitcoin / M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman // Applied Innovation 2, 2016. – Pp. 6-10.
17. Zhang Y. An IoT electric business model based on the protocol of BitCoin / Y. Zhang, J. Wen // Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on. IEEE, 2015. – Pp. 184-191.

Надійшла до редакції 27.12.2016 р.

Яцкив Н.Г., Яцкив С.В. Перспективы использования технологии блокчейн в сети Интернет вещей

Исследовано, что технология Blockchain имеет значительный потенциал применения в различных сферах деятельности, однако наиболее перспективой областью применения данной технологии является Интернет вещей и киберфизические системы. Технология Blockchain предлагает решение проблемы безопасности и конфиденциальности в среде Интернет вещей, обеспечивая новый вычислительный слой, где данные могут быть безопасно обработаны и проанализированы, оставаясь частным. Раскрыты потенциальные преимущества и выделены проблемы, которые необходимо решить для эффективного использования данной технологии в среде Интернет вещей.

Ключевые слова: Интернет вещей, блокчейн, биткойн, хэш-функция, транзакция, безопасность.

Yatskiv N.G., Yatskiv S.V. Perspectives of the Usage of Blockchain Technology in the Internet of Things

The analysis showed that Blockchain technology has significant potential to be applied in various areas, but the most perspective area of application for this technology is the Internet of Things and cyber-physical system. The Blockchain technology offers a solution for security and privacy problems in the Internet of Things, providing a new computing layer, where data can be safely processed and analyzed while staying private. The potential benefits are revealed and some issues needed to be addressed for the effective use of technology in the Internet of Things are also highlighted. We have found the problems that must be solved for the effective use of the technology in the Internet of Things environment.

Keywords: Internet of Things, Blockchain, Bitcoin, Hash Function, Transaction, Security.