ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТА ОБЧИСЛЮВАЛЬНІ СИСТЕМИ І КОМПЛЕКСИ В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

УДК 004.75

Н.Г. ЯЦКІВ, С.В. ЯЦКІВ
Тернопільський національний економічний університет

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН В МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ

У статті досліджено стан та перспективи використання технології блокчейн в середовищі Інтернет речей. Розкрито потенційні переваги та виділено проблеми, які необхідно вирішити для ефективного використання даної технології в середовищі Інтернет речей.
Ключові слова: Інтернет речей, блокчейн, біткойн, хеш - функція, транзакція, безпека.

N.G. YATSKIV, S.V. YATSKIV
Ternopil National Economic University

PERSPECTIVES OF THE USAGE OF BLOCKCHAIN TECHNOLOGY IN THE INTERNET OF THINGS

Abstract The status and perspectives of the usage of blockchain technology in the Internet of Things are researched in the article. Revealed the potential benefits and found the problems that must be solved for the effective use of technology in the Internet of things environment.
Keywords: Internet of Things, Blockchain, Bitcoin, Hash Function*, Transaction, Security.*

ВСТУП

Інтернет речей (Internet of Things, IoT) є наступним етапом еволюції Інтернету на шляху до всеосяжного Інтернету (Internet of Everything, IoE*)*. IoT включає в себе 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 був введений Кевіном Ештоном в 1999 році для опису системи, в якій фізичні об'єкти пов'язані з сенсорами і мережею Internet [1].

Поява IoT стала можливою завдяки розвитку мікроконтролерів та мережевих технологій, які дозволяють підключати мільярди різних пристроїв без особливих витрат і зусиль на створення додатків, що не залежать від платформи. Згідно з прогнозами Gartner, в 2020 р в світі буде 20,8 млрд. підключених пристроїв IoT [2].

Інформація, зібрана з пристроїв IoT, представляє безпрецедентну можливість для вирішення масштабних завдань з надання послуг та створення нових моделей ведення бізнесу. IoT створює можливість оцифровувати, продавати і постачати фізичні активи так само легко, як і віртуальні товари сьогодні.

З використанням мережі дешевих сенсорів і з'єднаних між собою речей, збір інформації про навколишнє середовище можна реалізувати з високим ступенем деталізації. Наявність детальної і точної інформації дозволить підвищити ефективність і забезпечити додаткові послуги в різних галузях.

Потенційними галузями для застосування IoT є сільське господарство, моніторинг навколишнього середовища, здоров'я, смарт-виробництво, інтелектуальні міста та інші [3, 4]. Проте, збільшення пристроїв збору, обробки та розповсюдження даних, підключених до мережі Інтернет, призводить до виникнення серйозних проблем, пов'язаних з безпекою даних, зокрема з конфіденційністю, анонімністю, стійкістю та зберіганням даних. Деякі з цих ризиків відомі, інші потребують досліджень. Приділення недостатньої уваги проблемі безпеки в середовищі IoT може призвести, наприклад, до атак на секретність і аутентифікацію, цілісність обслуговування або атак відмови в обслуговуванні (DoS) [5].

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

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Blockchains є новою інформаційною технологією, яка знаходить розвиток та використання у багатьох галузях. Першим і найбільш відомим прикладом використання технології блокчейн є криптовалюта - Bitcoin [6]. На даний час криптовалюта перетворилась у визнаний платіжний засіб, віртуальну валюту, яка приймається великими і дрібними підприємствами, корпораціями та сервісами.

В даний час ведуться дослідження та здійснюється реалізація ряду проектів з використанням технології Blockchain в галузі охорони здоров'я, а також у засобах масової інформації, електронного голосування, зберігання файлів, смарт- контрактах, страхуванні, у державному секторі (видача паспортів, збір податків, реєстрація земельних ділянок) та інших [5, 7].

Корпорація IBM одна із перших IT- гігантів зацікавилася технологією Blockchain і створила лабораторію, яка вивчає потенціал та додаткові можливості технології Blockchain з метою реалізації нових проектів та методів ведення бізнесу в сучасних умовах. В даний час корпорація IBM працює над створенням open-source програмного забезпечення, за допомогою якого партнери зможуть укладати цифрові договори, що будуть фіксуватися в глобальній мережі. За минулий рік дослідники з IBM розробили власну версію Blockchain, можливості якої тестуються для зазначеної вище мети. Також IBM провела експеримент, який отримав назву

Adept. Його мета - відстеження підключених до мережі пристроїв за допомогою технології Blockchain [8].

В дослідженнях IBM зазначається, що Blockchain на основі децентралізованого підходу, забезпечить в IoT більшу масштабованість, надійність, конфіденційність і безпеку. Результатом буде «Інтернет децентралізованих, автономних речей» – динамічна група об'єктів, підключених до універсальної цифрової головної книги, яка надає користувачам можливість безпечної ідентифікації і аутентифікації [9]. Архітектура Adept заснована на протоколі TeleHash, програмному забезпеченні для обміну даними BitTorrent та платформі для смарт - контрактів і децентралізованих автономних організацій Ethereum [10].

В роботі [11] запропонована схема оновлення прошивки вбудованих пристроїв в середовищі IoT на основі технології Blockchain, яка надійно перевіряє версію програмно-апаратних засобів, правильність прошивки, а також дозволяє завантажувати останню версію прошивки. Дана схема дозволяє вбудованому пристрою перевірити версію програмно-апаратних засобів та завантажити останню прошивку, якщо це необхідно, що в свою чергу забезпечить зменшення часу вікна атаки. Таким чином, Blockchain допомагає зменшити вплив атак на відомі вразливості програмно-апаратних засобів вбудованих пристроїв.

В [12] представлено принципи інтеграції технології Blockchain і групи робототехнічних систем (swarm robotics), яка може забезпечити інноваційні рішення та стати ключем до серйозного прогресу в 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 в Blockchain, які дають можливість робототехнічним агентам голосувати і досягати угоди; 3) роботи можуть функціонувати в різноманітних змінюваних умовах, якщо за їх роботу відповідають різні регістри Blockchain, що використовують різні параметри без будь-яких змін в алгоритмі управління.

Завдяки децентралізованій структурі і ключових принципах, таких як надійність і відмовостійкість, технологія Blockchain може бути також використана в системах автоматизованого транспортування, логістики, складських системах та хмарних обчисленнях, а також в кіберфізичних системах [13, 14, 15].

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

ТЕХНОЛОГІЯ BLOCKCHAIN

У 2008 році автором або групою авторів під псевдонімом Satoshi Nakamoto була опублікована стаття «Bitcoin: A Peer-to-Peer Electronic Cash System» з описом концепції і принципів роботи платіжної системи у вигляді однорангової мережі [6]. У 2009 році було представлено протокол криптовалюти Bitcoin і 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) [16].

Blockchain - це розподілена структура даних, яка складається з послідовності блоків, в якій кожний блок містить хеш попереднього блоку, утворюючи таким чином ланцюг блоків (рис.1).

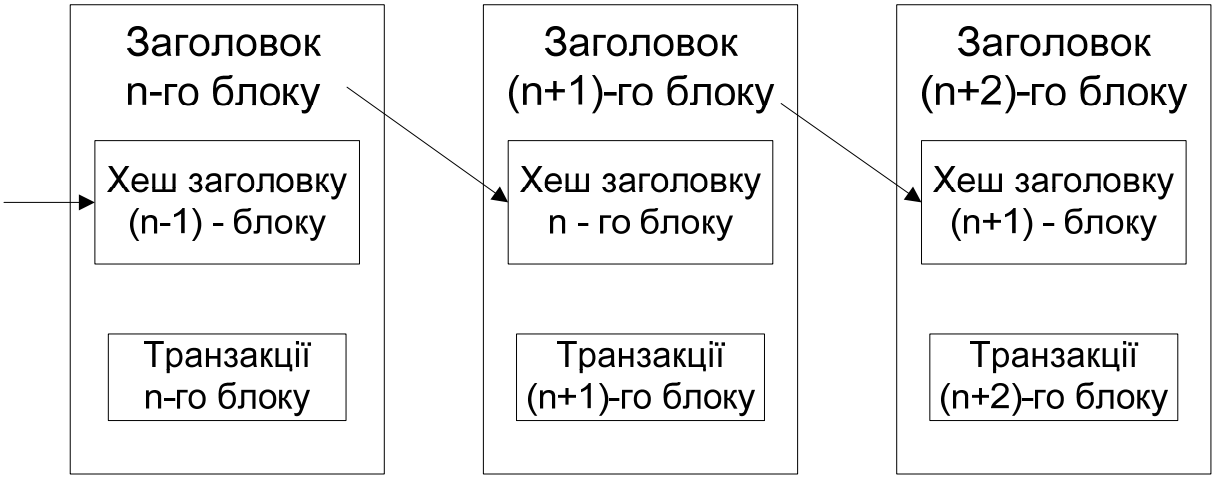

Рис.1. Спрощена послідовність блоків

Перший блок у ланцюжку (батьківський блок, genesis block) розглядається як окремий випадок, так як в нього відсутній попередній блок. Blockchain працює як розподілена база даних, яка здійснює облік усіх операцій в мережі. Операції мають відмітку часу і зберігаються в блоках, де кожен блок ідентифікується своїм криптографічним хешем. Blockchain повністю зберігається у кожному вузлі мережі. Для роботи Blockchain не потрібно довіри між вузлами мережі, так як будь-який вузол може самостійно перевірити, чи збігається його копія бази з копіями, які зберігаються в інших вузлах [17]. Принцип функціонування технології Blockchain розглянемо на прикладі криптовалюти «біткойн». В якості хеш-функції криптовалюта біткойн використовує криптографічну хеш-функцію SHA-256 [16]. Для перевірки цілісності даних в 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 до тих пір, 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 (рис.2). Блок складається із заголовку 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).

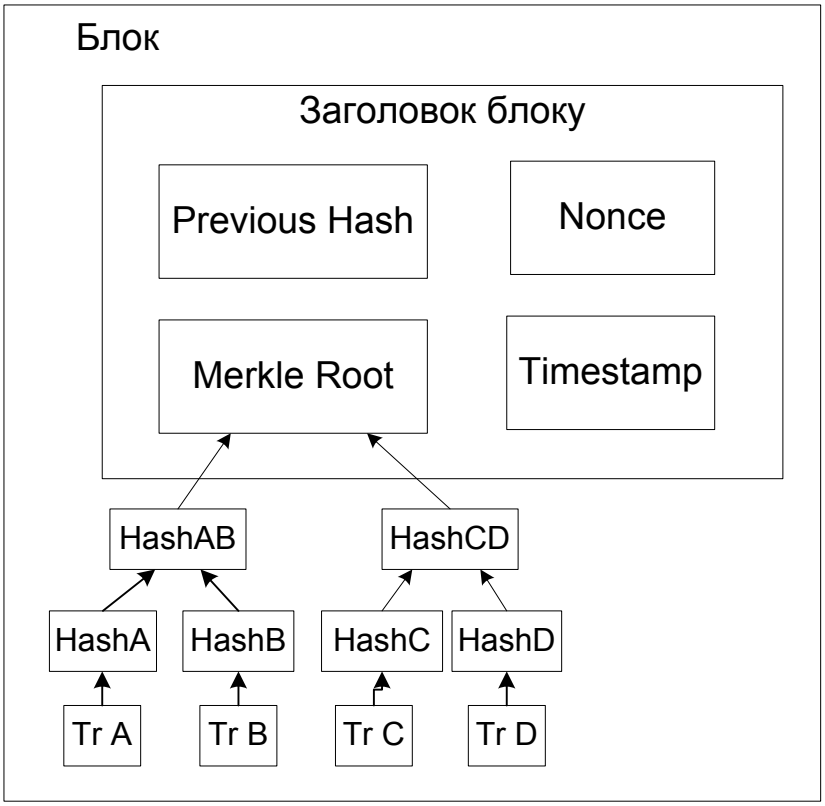

Рис.2. Структура блоку

Відмітка про час (Timestamp) вказує, коли був створений блок, і надає докази того, що дані в блоці існували в певний момент часу.

Для формування нового блоку вузла необхідні наступні дані: хеш попереднього блоку в ланцюжку; хеш Merkle для операцій, які необхідно помістити в блок; час (Timestamp) і одноразовий код (Nonce), вибраний псевдовипадкових чином. Для підтвердження коректності блоку необхідно обчислити хеш заголовку 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.

Вирішення 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'

При x=40 хеш - функція починається з двох нулів:

h = sha256 ("Internet of Things40")

h = '00dd26369b13e8d81d3e5afedcc2e847aaeaa476e5da8a15c77358761a1623ef'

При 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 і 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. В 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. Таким чином, на перевірку впливає тільки загальна обчислювальна потужність вузлів. Отже, для зміни інформації в блоці або створення некоректного блоку зловмиснику для обману необхідні значні обчислювальні ресурси, що робить це практично недоцільним.

Так як 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. Чим більше вузлів знаходиться в мережі, тим надійніше зберігання Blockchain. В Blockchain немає єдиної точки відмови, на відміну від централізованої системи з одним сервером, що забезпечує високу надійність збереження даних.

ПЕРЕВАГИ ТЕХНОЛОГІЇ BLOCKCHAIN

Переваги технології Blockchain, які забезпечують її ефективне використання в середовищі Інтернет речей [6, 11-13, 16-18]:

1) Blockchain є публічною розподіленою базою всіх транзакцій в мережі, яка підтримується децентралізованими вузлами. Blockchain технологія використовує децентралізовану і ненадійну однорангову мережу, де вузли не повинні вимагати довіреного посередника для взаємодії один з одним. Оскільки мережа Blockchain не контролюється центральним сервером і всі угоди перевіряються і підтверджуються консенсусом між вузлами, вузли не повинні довіряти один одному;

2) мережа Blockchain стійка до збоїв, так як вона являє собою децентралізовану мережу рівноправних вузлів без єдиної точки відмови. Сам Blockchain є незмінною і довговічною розподіленою базою і, як тільки транзакції записані в Blockchain, після консенсусу вони не можуть бути змінені або видалені;

3) мережа Blockchain має високий ступінь масштабованості за своєю природою, оскільки вона підтримується мережею рівноправних вузлів. Обчислювальна здатність мережі масштабується при збільшенні кількості приєднаних до мережі вузлів;

4) всі транзакції в мережі Blockchain захищені криптографічними методами. Крім того, прозорий характер публічної розподіленої бази, яка підтримується мережею Blockchain робить її безпечною, і кожен користувач мережі може перевірити правильність всіх операцій;

5) Blockchain дозволяє пристроям IoT взаємодіяти один з одним і робити операції автономно, так як кожен пристрій має свій власний Blockchain рахунок і немає необхідності використання третьої довіреної сторони.

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

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

1) створення блоків вимагає значних обчислювальних ресурсів, в той час як більшість IoT пристроїв мають обмежені апаратні ресурси;

2) створення блоків займає багато часу, проте для більшості додатків IoT необхідна низька затримка реакції на подію;

3) протоколи, які лежать в основі Blockchain, значно збільшують службовий трафік в мережі, який може бути небажаним для мереж IoT з бездротовими каналами зв'язку.

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

Для ефективного використання технології Blockchain в середовищі IoT має бути розроблена архітектура Blockchain, яка б враховувала вищезазначені обмеження IoT та забезпечувала децентралізовану безпеку і конфіденційність даних.

ВИСНОВКИ

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

Література

1. K. Ashton. That 'Internet of Things' Thing. RFID Journal, 22 July 2009. 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,” http://www.gartner.com/newsroom/id/3165317.

3. Li, Shancang, Li Da Xu, and Shanshan Zhao. The internet of things: a survey. Information Systems Frontiers 2015, 17.2, pp. 243-259.

4. Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. "The Internet of Things - A survey of topics and trends." Information Systems Frontiers 17.2, 2015, pp. 261-274.

5. Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "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. https://bitcoin.org/bitcoin.pdf

7. Christidis Konstantinos, Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. http://ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf?arnumber=7467408

8. Brody, Paul, Veena Pureswaran. Device democracy: Saving the future of the Internet of Things. IBM, September, 2014.

9. Panikkar, B. S., Nair, S., Brody, P., & Pureswaran, V. ADEPT: An IoT Practitioner Perspective, 2014.

10. Veena P., Panikkar S., Nair S., Brody P. "Empowering the Edge -Practical Insights on a Decentralized Internet of Things." Empowering the Edge -Practical Insights on a Decentralized Internet of Things. IBM Institute for Business Value, 17 Apr. 2015. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03662USEN#loaded

11. Lee Boohyung, Jong-Hyouk Lee. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. 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, and Vijay K. Madisetti. Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, №9, 2016, pp. 533-546

14. Мельник А.О. Кіберфізичні системи: проблеми створення та напрями розвитку // Вісник Національного університету "Львівська політехніка". Комп’ютерні системи та мережі. - 2014. – № 806. - С. 154-161.

15. Святний В.А., Бровкіна Д.Ю. Сучасні тенденції в автоматизації промислових комплексів. Системні дослідження та інформаційні технології, 2016, № 1. – С.32-39

16. Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014, 298 p.

17. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. Blockchain technology: Beyond bitcoin. Applied Innovation 2, 2016, pp.6-10.

18. Zhang Y., Wen J.. An IoT electric business model based on the protocol of BitCoin. Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on. IEEE, 2015, pp. 184-191.

References

1. K. Ashton. That 'Internet of Things' Thing. RFID Journal, 22 July 2009. 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,” http://www.gartner.com/newsroom/id/3165317.

3. Li, Shancang, Li Da Xu, and Shanshan Zhao. The internet of things: a survey. Information Systems Frontiers 2015, 17.2, pp. 243-259.

4. Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. "The Internet of Things - A survey of topics and trends." *Information Systems Frontiers* 17.2, 2015, pp. 261-274.

5. Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "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. https://bitcoin.org/bitcoin.pdf

7. Christidis Konstantinos, Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. http://ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf?arnumber=7467408

8. Brody, Paul, Veena Pureswaran. Device democracy: Saving the future of the Internet of Things. *IBM, September,* 2014.

9. Panikkar, B. S., Nair, S., Brody, P., & Pureswaran, V. ADEPT: An IoT Practitioner Perspective, 2014.

10. Veena P., Panikkar S., Nair S., Brody P. "Empowering the Edge -Practical Insights on a Decentralized Internet of Things." Empowering the Edge -Practical Insights on a Decentralized Internet of Things. IBM Institute for Business Value, 17 Apr. 2015. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03662USEN#loaded

11. Lee Boohyung, Jong-Hyouk Lee. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *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, and Vijay K. Madisetti. Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, №9, 2016, pp. 533-546

14. Melnyk A.O. Kiberfizychni systemy: problemy stvorennya ta napryamy rozvytku // Visnyk Natsional□noho universytetu "L□vivs□ka politekhnika". Kompyuterni systemy ta merezhi. - 2014. – № 806. -S. 154-161.

15. Svyatnyy V.A., Brovkina D.YU. Suchasni tendentsiyi v avtomatyzatsiyi promyslovykh kompleksiv. Systemni doslidzhennya ta informatsiyni tekhnolohiyi, 2016, № 1. – S.32-39

16. Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014, 298 p.

17. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Applied Innovation* 2, 2016, pp. 6-10.

18. Zhang Y., Wen J.. An IoT electric business model based on the protocol of BitCoin. Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on. IEEE, 2015, pp. 184-191.

Рецензія/Peer review : 23.1.2017 р. Надрукована/Printed :28.2.2017 р.
Стаття рецензована редакційною колегією