УДК 004.056

Ю. В. Баришев

АНАЛІЗ СТІЙКОСТІ ТЕХНОЛОГІЇ БЛОКЧЕЙН НА ПРИКЛАДІ РЕАЛІЗАЦІЙ BITCOIN ТА ETHEREUM

Вінницький національний технічний університет;

Анотація

Представлено аналіз технології блокчейн та виконано дослідження криптографічної стійкості її найбільш популярних реалізацій. Визначено вразливі місця реалізацій технології та запропоновано практичні рекомендації щодо усунення визначених недоліків.

Ключові слова: блокчейн, криптовалюта, гешування, мультиколізії, електронно-цифровий підпис, еліптичні криві.

Abstract

The analysis of the blockchain technology is presented and the research of its most popular implementations cryptographic infeasibility is performed. The weak spots of the technology implementations are determined and the practical solutions for revealed drawbacks removal are proposed.

Keywords: blockchain, cryptocurrency, hashing, multicollisions, digital signature, elliptic curves.

Вступ

Поширення технології блокчейн (blockchain) з часів публікації [1] обумовило її впровадження у різні галузі обробки інформації: від криптовалюти до комп'ютерних ігор [2, 3]. Таке активне її використання значною мірою обумовлюється комерційним успіхом проектів Bitcoin та Ethereum [2]. Залучення значних коштів у ринок інформаційних технологій, побудованих з використанням технології блокчейн, обумовлює актуальність проведення дослідження стійкості цієї технології.

Метою даного дослідження є підвищення стійкості технології блокчейн внаслідок вироблення практичних рекомендацій, що будуються на результатах аналізу цієї технології.

Для досягнення мети необхідно розв'язати такі задачі:

- проаналізувати стійкість технології блокчейн;
- визначити методи, що потребують удосконалення;
- розробити практичні рекомендації щодо покращення відомих реалізацій цієї технології.

Результати дослідження

Найбільш відомою роботою з технології блокчейн є робота невідомого вченого, що вийшла під псевдонімом Сатоші Накамото (Satoshi Nakamoto) [1], в якій описується використовувані у проекті криптовалюти Bitcoin технічні рішення. В подальшому дану технологію удосконалювали в наступних роботах, зокрема, найбільш комерційно успішним серед послідовників став проект Ethereum, який, окрім криптовалюти, дозволяв реалізовувати "кмітливі угоди" (smart contracts) між декількома сторонами [4].

Дані реалізації передбачають використання пари ключів для електронного цифрового підпису на основі еліптичних кривих: k_s та k_p – закритий і відкритий ключі відповідно. При цьому передбачено використання відкритого ключа як адреси гаманця і, як наслідок, асоціації із ним певної суми криптовалюти. Відповідно, основною інформацією, що необхідно зберігати, є інформація щодо транзакцій, які відбувалися у системі. У роботі [1] запропоновано використовувати розподілену базу даних для зберігання історії транзакцій. Транзакції t_i та t_{i+1} мають вигляд, схематично зображений на рис. 1.

Отримані транзакції (див рис. 1) об'єднують в блок, для цього їх ітеративно гешують відповідно до конструкції дерева Меркля [1]. Таким чином отриманий корінь дерева використовують як остаточне геш-значення всього повідомлення, яке входить у блок і складається із сукупності транзакцій. Відповідно до роботи [1] на конкретному вузлі мережі не обов'язково зберігати весь блок (для заощадження ресурсів пам'яті вузла) достатньо зберігати корінь дерева та низку гілок, де зберігається транзакція, яка "цікавить" конкретний вузол мережі.

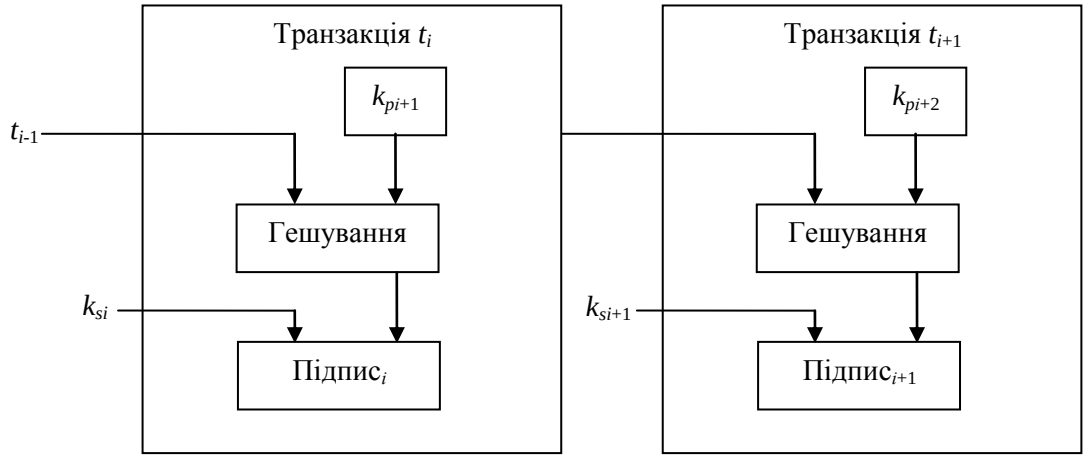

Рис. 1. Зображення транзакції в реалізації Bitcoin

Зрозуміло, що в один момент часу в мережі трапляється неузгодженість між вузлами, яка вирішується шляхом консенсусу за мажоритарним принципом за умови однакової довжини блокчейна [1]. Таким чином, з часом, коли після певного блока "докріпиться" ще низка блоків, він стане наявним у всіх вузлах мережі. Як обґрунтування стійкості такої моделі у роботі наводиться "доказ роботи" (proof of work) – для того, щоб зловмисник між "переконати" мережу у автентичності свого блока, йому необхідно володіти більше, ніж половиною її обчислювальних спроможностей [1].

Внаслідок виконаного аналізу, випливає, що реалізація Bitcoin містить низку вразливостей:

- використовує гешування, побудоване на конструкції, що нестійка до мультиколізій, описаних у роботах [5, 6], а з урахуванням, що не на всіх вузлах мережі зберігається блок повністю становить суттєву загрозу для вже здійснених транзакцій, оскільки це полегшує для зловмисника задачу "доказу роботи";

- використання еліптичних кривих вимагає розв'язання задачі пошуку простих чисел великої розрядності, що є математично складною задачею, а тому на практиці розв'язується за допомогою стохастичних алгоритмів, відповідно попри можливість знаходження чисел, що з ймовірністю, яка наближається до 1, є простими, все ж не досягають 1, а отже існує ймовірність реалізації хибного вибору числа, що, з урахуванням кількості поточного населення Землі та перспектив його зростання, робить ймовірність появи "чорного лебедя" [7] суттєвою;

- перспектива розвитку обчислювальної техніки та поява квантових комп'ютерів, зокрема, не забезпечує стійкість блокчейна протягом довгого періоду часу, що пов'язано із недостатньою довжиною ключів для електронного цифрового підпису;

- концепція "доказу роботи" не є криптографічною і за результатами аналізу даних з [8] є практично досяжною.

Попри те, що реалізація Ethereum покращує стійкість [4], а також, що постійно відбуваються удосконалення технології Bitcoin [9], наразі їх недостатньо, щоб протидіяти виявленим вище загрозам. Особливо це стає актуальним, якщо враховувати прикладне використання технології блокчейн в проаналізованих проектах.

Тому з метою підвищення стійкості технології блокчейн пропонуються такі удосконалення:

- використання конструкцій гешування, що стійкі до атак на основі мультиколізій, зокрема, запропонованих у роботах [10, 11];

- використовувати методи ущільнення для зменшення розміру блоку зам надання можливості вузлам викидати його частини;

- забезпечити можливість збільшення розміру ключа з часом із можливістю захисту вже створених блоків;

- замінити протокол пошуку консенсусу вузлів на криптографічно стійкий.

Оскільки дані пропозиції направлені безпосередньо на усунення виявлених в межах цього дослідження вразливостей, тому їх впровадження дозволить збільшити стійкість блокчейна до них. Варто відзначити, що на відміну від перших двох рішень, останні два потребують провадження додаткових наукових досліджень, оскільки наразі сучасні методи криптографії потребують розвитку для того,

щоб бути здатними розв'язати ці задачі. Зокрема для їх розв'язання перспективним є реалізація моделей псевдонедетрмінованих криптографічних перетворень, представлені в роботі [12], оскільки вони передбачають модульність перетворень, що обумовлює адаптивність та відкритість до рефакторингу програмних засобів, що їх реалізують.

Висновки

Аналіз технології блокчейн продемонстрував перспективність її використання для різноманітних задач. Її ключовою особливістю є можливість розподілення між різними вузлами бази даних, що породжує підвищення стійкості до втручання з боку зловмисників. Водночас аналіз показав, що сучасний стан криптографії не дозволяє реалізувати потенціал цієї технології в повній мірі. Це підтверджується, зокрема, виявленими недоліками в найбільш успішних реалізаціях цієї технології та визначеними шляхами для їх усунення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto [назва з екрану]. – 9 p. – Режим доступу до джерела: https://bitcoin.org/bitcoin.pdf

2. Cryptocurrency Market Capitalizations [назва з екрану]. – Режим доступу до джерела: https://coinmarketcap.com/

3. CryptoKitties [назва з екрану]. – Режим доступу до джерела: https://www.cryptokitties.co/

4. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger / Gavin Wood [назва з екрану]. – 32 p. – Режим доступу до джерела: http://gavwood.com/paper.pdf

5. Hoch J. J. Breaking the ICE – Finding Multicollisions in Iterative Concatenated and Expanded (ICE) Hash Functions / Jonathan J. Hoch, Adi Shamir. – 2006. – 13. – Режим доступу до ресурсу: http://www.wisdom.weizmann.ac.il/~yaakovh/papers/hashpaper_submission.pdf

6. Halunen K. Hash function security. Cryptanalysis of the Very Smooth Hash and multicollisions in generalised iterated hash functions / Kimmo Halunen. – Tampere, Juvenes Print: 2012. – 92 p. – Режим доступу до ресурсу: http://jultika.oulu.fi/files/isbn9789514299667.pdf

7. Талеб Н. Черный лебедь. Под знаком непредсказуемости – 2-е изд., доп. / Нассим Николас Талеб ; Пер. с англ. – Москва: КоЛибри, Азбука, 2015. – 736 с.

8. Ethereum Top 25 Miners by BLOCKS in the last 7 days [назва з екрану]. https://etherscan.io/stat/miner?range=7&blocktype=blocks. – (дата звернення 11.03.2018).

9. Bitcoin Improvement Proposals [назва з екрану]. – Режим доступу до джерела: https://github.com/bitcoin/bips#readme

10. Luzhetsky V The Generalized Construction of pseudonondeterministic hashing / Volodymyr Luzhetsky, Yurii Baryshev // Computing, 2012, Vol. 11, Issue 3, – p. 302-308.

11. Luzhetskyi V. Data-driven pseudonondeterministic hashing constructions / Volodymyr Luzhetskyi, Yurii Baryshev // Problems of Infocommunications Science and Technology (PIC S&T), 2016 – p. 114-116.

12. Баришев Ю. В. Моделі псевдонедетермінованих криптографічних перетворень / Ю. В. Баришев // "Інформаційні технологій та комп'ютерна інженерія"; матеріали статей п'ятої міжнародної науково-практичної конференції, м. Івано-Франківськ, 27-29 травня 2015 року. – Івано-Франківськ: Супрун В. П., 2015. – С.189-191.

Баришев Юрій Володимирович — канд. техн. наук, докторант кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yuriy.baryshev@gmail.com

Baryshev Yurii V. — Cand. Sc. (Eng), Post-doctoral Student of Information Protection Department, Faculty of Information Technologies and Computer Engeneering, Vinnytsia National Technical University, Vinnytsia, email : : yuriy.baryshev@gmail.com