OPTIMIZATION OF THE INFORMATION SYSTEM OF THE CORPORATE NETWORK

The main approaches to the algorithm of optimization of the information security system of the corporate network are considered. The transition from the multicriterion optimization problem to the one-criterion is proposed. With the formulation of the concept of system security optimization problem is to provide the maximum level of security (as a function of the value of information, protects and probability of breaking) with the limitations of the value of the system of protection and impact onproductivity of the system.

Key words: *optimization, criterion, system, information protection, threat, security level.*

Одержано 31.01.2019

УДК 681.3:519.72:003.26:004.056
DOI: 10.32626/2308-5916.2019-19.62-68

А. М. Кудін*, **, д-р техн. наук,
Л. В. Ковальчук*, д-р техн. наук,
Б. А. Коваленко***

*Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ,
**Національний банк України, м. Київ,
***ООО «GlobalLogic Ukraine», м. Київ

ТЕОРЕТИЧНІ ЗАСАДИ ТА ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ: ІМПЛЕМЕНТАЦІЯ НОВИХ ПРОТОКОЛІВ КОНСЕНСУСУ ТА КРАУДСОРСІНГ ОБЧИСЛЕНЬ

Наведено аналіз існуючих блокчейн-технологій, їх алгоритмів консенсусу та стійкості до відомих атак підміни блоку. Наведені основні ідеї та варіанти практичних реалізацій нового протоколу консенсусу «Proof-of-accuracy», розробленого авторами. Наведено проект блокчейн-системи, яка надає послуги обчислень в режимі краудсорсінгу.

Ключові слова: *блокчейн, протоколи консенсусу, атаки подміни блоку, краудсорсінг.*

Вступ. Сталою сучасною тенденцією розвитку IT-технологій є зростання частки децентралізованих систем зберігання та обробки даних, що визначає актуальність дослідження блокчейн-технології. Важливою складовою технології є протоколи узгодження. В роботі вирішено задачу вдосконалення протоколів узгодження в розподілених системах за рахунок застосування принципово нових схем залу-

чення майнерів до генерації нового блоку. Наведено опис нового варіанту протоколу консенсусу «proof-of-accuracy (PoAcc)», основні ідеї і положення якого вперше були описані в роботі [1]. Наведено результати строго математичного обґрунтування вибору параметрів протоколу, при яких можна забезпечити його стійкість до різних атак на блокчейн (зокрема, атаки, яка в криптовалютних блокчейнах називається атакою «подвійної витрати монети» (double spend attack) [2–5]). Аналог такої атаки будемо називати атакою підміни блоку, що в точності відображає її сутність. Авторами також пропонуються ідеї побудови схем застосування блокчейн-технології для здійснення обчислень.

Ідеї нових протоколів консенсусу. За основу ідеї побудови нового протоколу пропонується взяти найкращі ідеї від протоколів типу «доказу роботи» та «доказу частки володіння», зокрема від протоколів типу «доказу роботи» — ідею змагання між майнерами за якнайшвидше вирішення складної обчислювальної задачі, від протоколів типу «доказу частки володіння» — залежність виграшу майнеру в змаганні за право генерації наступного блоку від наявної у майнера інформації, необхідної для генерації блоку (далі — «вихідної інформації»). Ця інформація пов’язана із деяким цінним ресурсом реального світу, довільне накопичення якого є непростою задачею. Для обчислення рейтингу учасника протоколу в змаганні за генерацію нового блоку важливим є не тільки певні обчислювальні ресурси для вирішення задачі, але і вихідна інформація, яка дозволяє вирішити обчислювальну задачу з певною точністю. Для неможливості згенерувати довільну кількість цінних ресурсів для учасника протоколу, до початку протоколу застосовується такі обмеження: по-перше, регулюється чисельність учасників, які можуть прийняти участь в протоколі; по-друге, окремі дані рейтингу учасників формуються тільки на поточний сеанс протоколу (як сеансові ключі в схемі Діффі–Геллмана), по-третє, винагорода за участь у генерації нового блоку не прямо пов’язана із цінним ресурсом, який застосовується при обчисленні рейтингу учасника. Визначається наступний підхід до побудови протоколу узгодження: пропонується змінити обчислення алгоритму додавання нового блоку в блокчейн при застосуванні протоколу угоди «proof-of-works» таким чином, щоб необхідна для роботи алгоритму вихідна інформація була задані неповно і неточно. Значення, яке обчислюється алгоритмом і яке може бути перевірено іншими учасниками протоколу, визначається з точністю, що задається деяким порогом. Вихідна інформація розташовуються на декількох ресурсах за доступ до яких конкурують учасники протоколу угоди. Цінним ресурсом може бути IP-адреса абонента. Теоретичною основою протоколу пропонується вибрати загальну теорію оптимальних алгоритмів [6], яка пов'язує існування і складність алгоритмів з

точністю задання вхідних даних. Розглянемо один з практичних реалізацій протоколу «доказу точності».

Варіант протоколу консенсусу «proof-of-accuracy». Наведемо покроковий опис протоколу, який реалізує зазначені вище ідеї.

1. Етап ініціалізації.

A. Беруть участь усі активні на даний час вузли мережі зі своїми IP-адресами n вузлів — $IP_1, \ldots, IP_n$.

B. Всі учасники протоколу генерують сумісно випадкове число m за допомогою схеми Діффі–Геллмана для групи абонентів [7]. Випадкове число m є невідомим для всіх учасників протоколу до кроку E.

C. За допомогою s — того вектора ініціації IV_s, поточне значення якого зберігається в блокчейні, кожен учасник протоколу генерує випадкове число R_{si} (різне для кожного учасника). Начальне значення вектора ініціалізації IV_0 формується при ініціалізації блокчейну за допомогою генерації випадкового 256-бітного числа.

D. Кожен учасник мережі обчислює геш-код $H\left(IV_s, IP_i, R_{si}\right)$, $i = \overline{1,n}$. Ці геш-коди будуть коефіцієнтами многочленів степеня k. Всього можна побудувати A_n^k таких многочленів, враховуючи різні перестановки коефіцієнтів. Вибір значення k здійснюється з урахуванням середньої кількості кроків до знаходження всіх значень поліному $\frac{k}{n}$, ймовірностей доступності вузлів мережі, можливостей атак на мережу та імовірності розгалуження. Всі коефіцієнти розміщуються у блокчейні.

E. Обираємо за протоколом «гри в покер» [8] m учасників II етапу. Вибір значення m здійснюється із врахуванням виконання приблизної рівності $\frac{m}{n} \approx 1$. Учасники етапу маркуються як «активні» учасники. Інші учасники («наглядачі») випадково обирають з блокчейну один з поліномів, побудованих на попередньому кроці.

F. За допомогою протоколу захищених багатосторонніх обчислень [9] «наглядачами» значення $y_1, ..., y_k$ обраного поліному в деяких точках $x_1, ..., x_k$ (наприклад, у точках 1, 2, …, k), після чого обрані значення випадково розподіляються між всіма вузлами мережі з використанням (k, m) — порогового протоколу розподілу секрету (деякі вузли мережи не будуть містити жодного значення, але в кожному вузлі не більше одного значення).

2. Етап збору. m активних учасників протоколу збирають по всім вузлам мережі k значень поліному. Перший, хто зібрав всі значення вважається переможцем та формує наступний блок транзакцій. Для зменшення ймовірності виникнення «розгалужень» можна використовувати складність задачі відновлення коефіцієнтів поліному. Величину імовірності виникнення розгалужень можна регулювати за допомогою складності задачі відновлення коефіцієнтів поліному.

3. Етап верифікації. Використовуються протокол з доведення знань секрету «наглядачам» [9].

4. Етап ре-ініціалізації. Генеруємо наступне значення вектора ініціалізації вектора ініціації IV_{s+1} для захисту від атак повтору шляхом обчислення геш-коду за алгоритмом SHA256 від конкатенації сумісно згенерованого випадкового число m' за допомогою схеми Діффі–Геллмана для групи абонентів та збільшеного на одиницю попереднього значення, а саме: $IV_{s+1} = SHA256\,((IV_s + 1) \,||\, m')$.

Оцінка стійкості протоколу консенсусу до атак. Знайдемо точні аналітичні вирази, які пов'язують, з одного боку, імовірність атаки з підміною блоку, а з іншого — параметри мережі, такі як час синхронізації, інтенсивність генерації блоків та частку гешрейту зловмисника.

Введемо позначення. HMs — множина чесних майнерів, MMs — множина зловмисників, T_H та T_H' (T_M та T_M') — випадкові величини часу, які HMs (MMs) витрачають на створення одного блоку та створення і розповсюдження блоку по всім вузлам мережі. За умов експоненційного розподілу цих величин [5], $\alpha = \alpha_H + \alpha_M$ — загальна інтенсивність генерації блоків у мережі, $D_H\,(D_M)$ — верхні межі часу розповсюдження блоків між чесними майнерами (зловмисниками), $p_H\,(p_M = 1 - p_H)$ — ймовірність того, що HMs згенерують наступний блок раніше, ніж MMs. Ми будемо вважати, що $\Delta D = D_M - D_H > 0$. За заданих параметрам мережі ΔD та α межою безпеки (security threshold) для протоколу консенсусу PoAcc є найменше значення p_0, таке що при умові $p_M \geq p_0$ ймовірність успіху атаки підміни блоку дорівнює 1, незважаючи на кількість блоків підтвердження. Доведена наступна теорема.

Теорема 1. За заданих параметрам мережі ΔD та α межа безпеки p_0 може бути знайдена як рішення рівняння $2(1 - p_0) = e^{\alpha p_0 \Delta D}$.

У таблиці наведено значення границі безпеки протоколу при різних параметрах мережі.

Таблиця

Значення границі безпеки протоколу PoAcc при різних параметрах мережі

α \ D_H	$D_H = 2$	$D_H = 5$	$D_H = 10$	$D_H = 20$	$D_H = 60$
$1/600$	0.49917	0.49792	0.49585	0.49174	0.47564
$1/60$	0.49174	0.47961	0.460146	0.42408	0.31492
$1/6$	0.42408	0.33757	0.24626	0.15678	0.06283

Блокчейн обчислювальна система, що надає послуги за принципом краудсорсінгу. Якщо порівнювати обчислювальні потужності найвідомішої з блокчейн платформ Bitcoin (5×10^{19} гешів за секунду) з потужністю сучасних суперкомп'ютерів, то перший з них, Тянхе-2, може обчислювати приблизно $2{,}6 \times 10^{12}$ гешів на секунду, що на 7 порядків менше кількості обчислених гешів мережею Bitcoin, причому у блокчейн мережах вона витрачається даремно. Ідея даної концепції — використання обчислювальних можливостей мережі блокчейн для виконання практичних (наукових або інженерних) обчислень у режимі краудсорсінгу, що дозволяє побудувати відносно дешеву розподілену гнучку та масштабовану систему виконання складних обчислень, без використання додаткової інфраструктури. Запропонована схема є блокчейн мережею, вузли якої можуть пропонувати свої обчислювальні ресурси і отримувати винагороду за виконані обчислення. При цьому архітектура системи надає гарантії проведення чесних обчислень та отримання очікуваної суми винагороди. Кожен вузол мережі може виконувати одну з ролей. Замовник — подає заявку на обчислення певного складного алгоритму з вхідними даними. За отримання результату виплачує винагороду. Виконавець — виконує один із розміщених у блокчейні алгоритмів, за це отримує винагороду від замовника. Майстер-вузол — обирається відповідно до алгоритму консенсусу блокчейну, його задачею є перевірка множини транзакцій та підтвердження чергового блоку. Кожен з вузлів також має однакову бібліотеку з множиною допустимих алгоритмів, що можуть відправлятися на краудсорс Замовником / обчислюватися Виконавцем. Кожен алгоритм бібліотеки доповнюється алгоритмом оцінки обчислювальної складності (для визначення винагороди) та алгоритмом перевірки правильності обчислення (опціонально).

Протокол роботи системи складається з трьох етапів: подання запиту на виконання алгоритму Замовником, виконання алгоритму Виконавцем та підтвердження блоку з виплатою винагороди Майстер-

вузлом. На першому етапі Замовник обирає необхідний алгоритм з множини допустимих алгоритмів та оцінює складність алгоритму, визначає залежність значення винагороди від складності алгоритму, формує транзакцію, що містить власний ідентифікатор, ідентифікотор алгоритму, вхідні дані, серіалізовані у байтовий рядок, а також значення винагороди. На другому етапі Виконавець обирає з пулу транзакцій запит на виконання алгоритму, перевіряє платіжеспроможність Замовника, обчислює алгоритм за відомими вхідними даними. Після цього, посилає до блокчейну транзакцію, до якої включає власний ідентифікатор, ідентифікатор транзакції-запиту Замовника, $E_s(q)$ — результат q обчислення алгоритму, зашифрований на спільному ключі s Виконавця та Замовника (обчислюється за допомогою неінтерактивного протоколу Діффі–Хеллмана на основі пар власних ключів), а також $Proof(x_i, q)$ — доведення наявності результату без розголошення, що обчислюється на основі приватного ключа Виконавця та власне результату. На третьому етапі Майстер-вузол завантажує транзакції, відкидаються неплатоспроможні Замовники та Виконавці з балансом гаманця, що не дозволяє сплатити штраф у випадку необхідності, розглядаються запити на виконання, що мають невичерпаний термін дії. Для кожного такого запиту збираються відповіді Виконавців. Принцип перевірки правильності результату полягає у порівнянні всіх відповідей, той результат, який співпадає у більшості вважається найдостовірнішим. Для цього, Майстер попарно порівнює значення $Proof(x_i, q)$ за допомогою функції $Compare(\cdot)$ (перевірка відбувається без розкриття значення q а також без можливості підробити значення без знання секретного ключа x_i завдяки неінтерактивному протоколу доведення без розголошення). Далі, найбільша за сумою гаманців множина однакових результатів вважається найбільш достовірною та кожен її член має отримати винагороду пропорційно до свого балансу (конкретна функція розподілу виграшу може бути довільною, але обов'язкова умова $a(x+y) \geq a(x) + a(y)$, де $a(x)$ — винагорода Виконавця з балансом x). Решта Виконавців (відповіді яких є недостовірними) виплачують штраф на користь Майстер-вузла (функція нарахування штрафу $p(x)$ також довільна, але з додатковою умовою $p(x+y) \leq p(x) + p(y)$). Далі, Майстер вузол формує відповідні транзакції з винагородами та штрафами, перевіряє визначену кількість попередніх блоків (згідно з загальним процесом перевірки для даного блокчейну) та підписує новий блок.

Список використаних джерел:

1. Кудин А. М. Блокчейн и криптовалюты на основаниии «доказательства точности». *Математичне та комп'ютерне моделювання.* Серія: Технічні науки : зб. наук. праць. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2017. Вип. 15. С. 104–108.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. 9 p.
3. Rosenfeld M. Analysis of hashrate-based double-spending. 2014. 13 p.
4. Pinzon C., Rocha C. Double-Spend Attack Models with Time Advantage for Bitcoin. *Electronic Notes in Theoretical Computer Science.* 2016. Vol. 329. P. 9–103.
5. Pinson P., Lewenberg Y., Sompolinsky Y. Inclusive Block Chain Protocols. 20 p.
6. Grunspan C., Perez-Marco R. DOUBLE SPEND RACES. 35 p.
7. Трауб Д., Васильковский Г., Вожьняковский Х. Информация, неопределенность, сложность. М. : Мир, 1988. 184 с.
8. Steiner M., Tsudik G., Waidner M. Diffie-Hellman key distribution extended to groups, 1996.
9. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. 816 p.
10. Ben-David A., Nisan N., Pinkas B. FairplayMP: a system for secure multi-party computation. *Computer and Communications Security — CCS 2008*, ACM. 2008. P. 257–266.

THEORETICAL FOUNDATIONS AND APPLICATION OF BLOCKCHAIN: IMPLEMENTATION OF NEW PROTOCOLS OF CONSENSUS AND CROWDSOURCING COMPUTING

The analysis of existing blockade technologies, their algorithms of consensus and resistance to known block substitution attacks is given. The main ideas and variants of practical implementation of the new «Proof-of-accuracy» consensus protocol developed by the authors are presented. The project of BlockChein-system, which provides services of calculations in the mode of crowdsourcing, is presented.

Key words: *blockchain, consensus protocols, wrong block attack attacks, crowdsourcing.*

Одержано 01.02.2019