з автоматичного управління *«Автоматика 2015»*. Одеса: Одеський національний політехнічний університет. 2015. С. 171–173.
5. Гусейн-Заде С. М. Разборчивая невеста. М.: МЦНМО, 2003. 24 с.
6. Stützle T., López-Ibáñez M., Pellegrini P., Maur M., M. de Oca, Birattari M., Michael Maur, Dorigo M. Parameter Adaptation in Ant Colony Optimization. Technical Report, IRIDIA, Université Libre de Bruxelles, 2010.

Modified ACO algorithm for solving the problem of constructing schedule of contracts execution for companies engaged in the provision of services is proposed. Using of proposed algorithm allows to increase efficiency and to minimize times for its resolving.

Key words: *planning of contracts execution, mathematical modeling, ACO, genetic algorithm.*

Одержано 14.02.2017

УДК 004.056.5

О. О. Перекопський, аспірант

Харківський національний університет радіоелектроніки, м. Харків

ПОРІВНЯЛЬНИЙ АНАЛІЗ ДОКАЗУ ВИКОНАНОЇ РОБОТИ ТА ВІЗАНТІЙСЬКОЇ ВІДМОВОСТІЙКОСТІ

Представлений порівняльний аналіз механізмів досягнення консенсусу на основі доказу виконаної роботи та Візантійської відмовостійкості, у контексті таких важливих властивостей регістру Blockchain, як управління ідентифікаторами вузлів та завершеності механізму досягнення консенсусу.

Ключові слова: *криптовалюта, механізм досягнення консенсусу,доказ виконаної роботи, Візантійська відмовостійкість, регістр Blockchain.*

Вступ. Криптовалюта Bitcoin продемонструвала практичну цінність глобального досягнення консенсусу серед тисячі вузлів, назавжди змінивши світ цифрових транзакцій. На ранніх стадіях розвитку криптовалюти Bitcoin, проблема продуктивності технології Blockchain, заснованої на імовірнісному доказі виконаної роботи, не була пріоритетною. Криптовалюта Bitcoin стала успішною, незважаючи на затримки досягнення консенсусу (до години) і теоретичної пікової пропускної спроможності тільки до 7 транзакцій в секунду.

На сьогоднішній день ситуація докорінно змінилася — низька продуктивність регістрів Blockchain на основі доказу виконаної роботи стає неактуальною. Зокрема, ряд сучасних платформ криптовалюти, призначених для довільних розподілених додатків на технології Blockchain, потребують набагато більш високої продуктивності. Однак такий підхід змушує платформи криптовалюти відійти від своєї

первісної мети і ввести домен протоколів реплікації баз даних і їх варіанти, що володіють Візантійською відмовостійкістю.

Визначення 1. Візантійська відмовостійкість — характеристика системи, стійкої до класу збоїв, відомих як проблема Візантійських генералів (узагальненням проблеми двох генералів), для яких існує доказ нерозв'язності.

Незважаючи на те, що протокол Bitcoin фактично не виконує досягнення консенсусу в традиційному сенсі в рамках розподілених обчислень, він дуже близький до консенсусу з імовірнісною угодою [1]. Метою створення криптовалют, таких як Bitcoin, є повне впорядкування транзакцій у розподіленому регістрі, який називається Blockchain. Технологія Blockchain складається з ланцюжка хешів блоків: кожен блок містить упорядкований набір транзакцій і хеш попереднього блоку (починаючи з вихідного блоку). Ключовою частиною доказу виконаної роботи є ланцюжок хешів [2]: блок містить одноразові номера, які майнер повинен встановити таким чином, щоб хеш всього блоку в результаті був менше, ніж відоме цільове значення, яке, як правило, є дуже невеликим числом.

Визначення 2. Майнінг — процес вирішення криптографічних завдань з використанням обчислювальних апаратних засобів, за допомогою якого транзакції перевіряються і додаються в регістр Blockchain.

Слід зазначити, що в криптовалюті Bitcoin, складність майнінга, обернено пропорційна цільовому значенню, яке регулюється динамічно протягом усього часу роботи системи. Регулювання проводиться за швидкістю виконання майнінга блока, і, побічно, в залежності від обчислювальної потужності вузлів, що беруть участь у системі. Це необхідно для підтримки очікуваного часу майнінга блоків — приблизно один блок кожні 10 хвилин [3]. Ця затримка 10 хвилин (на блок) часто згадується як частота блоку [4].

Порівняльний аналіз. Високорівневий порівняльний аналіз механізму досягнення консенсусу на основі доказу виконаної роботи і Візантійської відмовостійкості в контексті ряду важливих властивостей регістру Blockchain представлений в таблиці. Ці властивості включають у себе керування ідентифікаторами вузла, завершеності консенсусу (можливість тимчасових розгалужень в регістрі blockchain).

Таблиця

Високорівневий порівняльний аналіз доказу виконаної роботи і Візантійської відмовостійкості

Критерії	Доказ виконаної роботи	Візантійська відмовостійкість
Управління ідентифікаторами вузла	**відкрите, повністю децентралізоване**	дозволені вузли повинні знати ідентифікатори всіх інших вузлів
Завершеність консенсусу	Не виконується	**Виконується**

Записи, виділені жирним шрифтом, означають перевагу механізму досягнення консенсусу.

Управління ідентифікаторами вузлів. Найбільш принципова відмінність доказу виконаної роботи від Візантійської відмовостійкості полягає в управлінні ідентифікаторами вузла. Особливістю доказу виконаної роботи є децентралізоване управління ідентифікаторами. Наприклад, будь-який бажаючий може скачати код для майнера Bitcoin, і почати брати участь в протоколі, знаючи, в основному тільки один спеціальний робочий вузол.

Це дуже потужна особливість доказу виконаної роботи і головна причина, чому вони є так званим сімейством «відкритих» регістрів Blockchain, в яких може брати участь будь-який користувач. Доказ виконаної роботи пов'язано з атакою Сібіли в анонімних мережах [5]. Зокрема, в регістрах Blockchain, заснованих на доказі виконаної роботи, здатність вузла вплинути на результат досягнення консенсусу залежить від обчислювальної потужності вузла.

На противагу цьому, Візантійська відмовостійкість, як правило, вимагає, щоб кожен вузол знав весь набір своїх тимчасових вузлів, що беруть участь в консенсусі. Це, в свою чергу, вимагає (логічного) централізованого управління ідентифікаторами вузлів, в якому довірена сторона видає ідентифікатори і криптографічні сертифікати вузлів.

Важливо відзначити, що після початкового завантаження регістру Blockchain на основі Візантійської відмовостійкості, вузли, вже приєдналися до Blockchain, можуть самі діяти разом як розподілена довірена сторона і можуть реконфігурувати систему [6, 7]. Цей аспект Візантійської відмовостійкості ставить її в невигідне становище по відношенню до доказу виконаної роботи. Проте, в ряді нових додатків на базі технології Blockchain (наприклад, регістри банкінгу, фінансів, земельної власності і нерухомості) вимоги до відомих ідентифікаторів вузлів в будь-якому випадку може бути накладено на систему з юридичних причин. Це пояснює, чому механізм досягнення консенсусу на основі Візантійської відмовостійкості є технологією, яку вибирають для так званих «дозволених» регістрів Blockchain, що вимагають, щоб ідентифікатори учасників були відомі.

Остаточність досягнення консенсусу.

Визначення 3.Остаточністьдосягнення консенсусу — це властивість, яка полягає у тому, що коректний блок, доданий до регістру Blockchain в якийсь момент часу, не буде ніколи видалений з нього.

Формально визначення 3 може бути сформульовано таким чином:

Визначення 4. Завершеність консенсусу — якщо коректний вузол g додає блок b до своєї копії регістру Blockchain перед додаван-

ням блока b', то жоден коректний вузол d не додасть блок b' перед блоком b до своєї копії регістру Blockchain.

Остаточність механізму досягнення консенсусу не виконується регістром Blockchain на основі доказу виконаної роботи. Порушення остаточності досягнення консенсусу показано на рисунку, а. Це пояснюється тим, що крім уникнення необхідності управління ідентифікацією, доказ виконаної роботи виступає в якості випадкового механізму управління паралелізмом, в якому частота блоку регулюється таким чином, що колізії блоків (тобто одночасні додавання різних блоків до регістру Blockchain) зустрічаються рідко.

Слід зазначити, що так як такий механізм управління паралелізмом носить лише імовірнісний характер і поширення блоків по мережі займає деякий час [8], то такі колізії трапляються. Виникнення таких колізій призводить до тимчасових розгалужень на регістрі Blockchain, що показані на рисунку, б. Подібні колізії виникають на регістрі Blockchain на основі доказу виконаної роботи навіть при відсутності вузлів зловмисника.

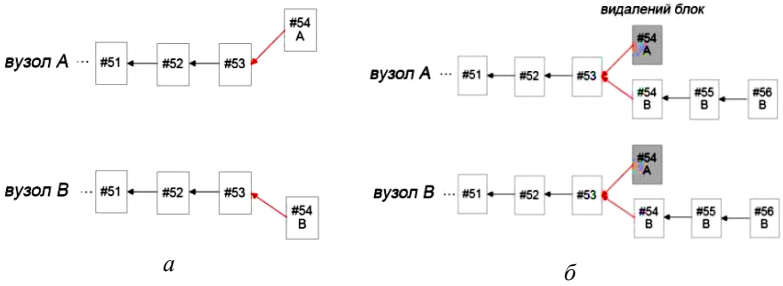

Рисунок. *а — порушення остаточності досягнення консенсусу; б — розгалуження та правило вирішення конфлікту на регістрі Blockchain*

Тимчасові розгалуження на регістрі Blockchain вирішуються за правилами, таким як правило найбільш довгої гілки в Bitcoin [3] або правило GHOST [9], варіант якого застосовується в Ethereum. Проте, сама наявність тимчасових розгалужень не припускає виконання завершеності механізму досягнення консенсусу. Відсутність завершеності консенсусу безпосередньо впливає на затримку досягнення консенсусу для Blockchain на основі доказу виконаної роботи. Це пояснюється тим, що транзакціям необхідно мати кілька наступних за ними блоків, щоб збільшити ймовірність того, що транзакція не буде в підсумку відкинута і видалена з регістру Blockchain (у разі багатоблокових підтверджень).

На противагу цьому, завершеність механізму досягнення консенсусу виконується всіма протоколами з Візантійською відмовостійкістю. Це дає регістрам на основі таких протоколів явну перевагу перед

доказом виконаної роботи, так як додатки, користувачі і смарт-контракти можуть мати моментальне підтвердження остаточного включення транзакції в регістр Blockchain.

Висновки. У роботі представлений порівняльний аналіз механізмів досягнення консенсусу на основі доказу виконаної роботи та Візантійської відмовостійкості, у контексті таких важливих властивостей регістру Blockchain, як управління ідентифікаторами вузлів та завершеності механізму досягнення консенсусу.

Таким чином для децентралізованих платформ, які не вимагають суворої ідентифікації учасників, необхідно застосовувати механізм досягнення консенсусу на основі доказу виконаної роботи. У системах, що виключають анонімність користувачів, навпаки, необхідно використовувати Візантійську відмовостійкість.

Набір властивостей, в контексті яких проводився порівняльний аналіз в даній роботі, безумовно, не є вичерпним. Напрямком для майбутнього дослідження є проведення порівняльного аналізу між розглянутими механізмами досягнення консенсусу в контексті наступних важливих властивостей регістру Blockchain: масштабованості з точки зору числа вузлів і клієнтів, що беруть участь в досягненні консенсусу; продуктивності (затримки, пропускної здатності, споживаної потужності), допустимої потужності зловмисника і існування доказів коректності протоколів, що лежать в основі регістру Blockchain.

Список використаних джерел:

1. Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin backbone protocol: Analysis and applications. In Advances in Cryptology — EUROCRYPT 2015. *34th Annual International Conference on the Theory and Applications of Cryptographic Techniques.* 2015. P. 281–310.
2. DworkC., NaorM. Pricing via processing or combatting junk mail. In Advances in Cryptology — CRYPTO '92, 12th Annual International Cryptology Conference. 1992. P. 139–147.
3. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2009.
4. Eyal I., Gencer A, Sirer E. BitcoinNG: A scalable blockchain protocol. In 13th USENIX Symposium on Networked Systems Design and Implementation, NSDI '16. 2016. 23 p.
5. John R. Douceur. The sybil attack. In Peer-to-Peer Systems, First International Workshop, IPTPS. 2002. P. 251–260.
6. Rodrigues R., Liskov B., Chen K. Automatic reconfiguration for large-scale reliable storage systems. IEEE Trans. Dependable Sec. Comput. Vol. 9(2). 2012. P. 145–158.
7. Bessani A., Sousa J., Alchieri E. State machine replication for the masses with BFT-SMART. In 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN. 2014. P. 355–362.
8. Decker C., Wattenhofer R. Information propagation in the Bitcoin network. In 13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P. 2013. P. 1–10.

9. Sompolinsky Y., Zohar A. Secure high-rate transaction processing in Bitcoin. In Financial Cryptography and Data Security. 19th International Conference, FC. 2015. P. 507–527.

This paper is denoted to comparative analysis of the consensus mechanisms based on proof of work and Byzantine fault-tolerance in the context of important properties of Blockchain ledger, such as the node identifiers management and finality of consensus mechanism.

Key words: *Bitcoin, Blockchain ledger, consensus mechanism, proof-of-work, Byzantine fault-tolerance.*

Одержано 15.02.2017

УДК 519.6

Ю. І. Першина, д-р. фіз.-мат. наук, доцент,
О. В. Шилін, аспірантка

Українська інженерно-педагогічна академія, м. Харків

МЕТОД ВІДНОВЛЕННЯ 3D ОБ'ЄКТА З ВИКОРИСТАННЯМ ПОЛІНОМІАЛЬНОЇ ІНТЕРФЛЕТАЦІЇ

Викладено метод відновлення внутрішньої структури тривимірного тіла за допомогою поліноміальної інтерфлетації з використанням відомих томограм (слідів), що лежать на системі довільних площин, який є узагальненням методу відновлення тіла за відомими томограмами на системі трьох груп паралельних площин. Проведений чисельний експеримент цього методу.

Ключові слова: *інтерфлетація, відновлення, томограма, сліди.*

Вступ. В багатьох областях науки та техніки, таких як медицина, геофізика, електронна мікроскопія, астрофізика, промислова дефектоскопія, діагностика плазми та інших, виникає проблема визначення внутрішньої структури об'єкта найбільш зручним способом. Для її розв'язання в багатьох випадках неприйнятні прямі методи дослідження, що пов'язані з руйнуванням об'єкта. Тому при неруйнівному контролі тривимірних об'єктів, при проведенні наукових досліджень у різних областях науки і техніки тощо, знайшли широке застосування комп'ютерні томографи [1], які дозволяють відновлювати внутрішню структуру тіла не розрізаючи його. При цьому виник новий клас задач — задач відновлення внутрішньої структури тривимірного тіла за відомими його томограмами на декількох площинах.

Виділимо основні риси та особливості томографічних методів. Привабливіша риса полягає у тому, що способи вимірювань не руйну-