УДК 004.056/.523:004.774REST API
DOI: https://doi.org/10.17721/ISTS.2024.8.56-59

Іван ПАРХОМЕНКО, канд. техн. наук, доц.
ORCID ID: 0000-0001-6889-9284
e-mail: ivan.parkhomenko@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Роман ОГІЄВИЧ, асп.
ORCID ID: 0009-0003-7948-1125
e-mail: r.ohiievych@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

МОДЕЛІ АВТОРИЗАЦІЇ ДЛЯ ВЗАЄМОДІЇ ВУЗЛІВ БЕЗ ДОВІРИ В ПУБЛІЧНИХ ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖАХ

В с т у п . ***Децентралізовані мережі стали основою для нових технологій, що забезпечують безпеку та прозорість операцій без потреби в централізованих контролювальних органах. Вказані мережі дозволяють здійснювати взаємодію між вузлами без попередньої довіри. Проте забезпечення надійної та ефективної авторизації в таких мережах є викликом через відсутність єдиного авторизаційного центру. Це створює потребу в розробленні нових моделей, що дозволяють безпечно керувати доступом до ресурсів на основі взаємодії між вузлами. Однією з основних проблем є те, що кожен вузол може бути потенційно шкідливим, і традиційні моделі авторизації, що використовуються в централізованих системах, не можуть забезпечити належний рівень безпеки. Метою цієї роботи є дослідження нових підходів до авторизації в публічних децентралізованих мережах, які не потребують довіри між учасниками.***

М е т о д и . ***Досліджено моделі авторизації, засновані на репутації та доказах корисної роботи – Proof of Useful Work (PoUW), що перспективні для децентралізованих систем. Модель репутації передбачає надання прав доступу на основі попередньої активності вузла в мережі, де кожен вузол накопичує бали репутації за виконання певних завдань. Друга модель PoUW дозволяє вузлам отримувати авторизацію за кількість виконаних корисних обчислень. Це уможливлює не лише підвищення рівня безпеки мережі, але і стимулювання вузлів до виконання обчислювальних завдань, що мають практичну цінність для спільноти.***

Р е з у л ь т а т и . ***Моделювання показало, що обидві моделі дозволяють ефективно забезпечити безпеку та надійність взаємодії між вузлами. Вузли з високим рівнем репутації або ті, що виконали значний обсяг корисних обчислень, отримують доступ до критично важливих ресурсів мережі. Впровадження таких підходів дозволяє знизити ризик шкідливої активності, оскільки вузли, які не виконують корисних дій, обмежуються у правах доступу.***

В и с н о в к и . ***Запропоновані моделі авторизації на основі репутації та Proof of Useful Work продемонстрували високу ефективність у публічних децентралізованих мережах. Вони дозволяють здійснювати безпечну взаємодію між вузлами без потреби у довірі, що робить ці підходи перспективними для майбутнього впровадження в різних сферах. Використання цих моделей забезпечує динамічне керування доступом до ресурсів, мінімізуючи ризики шкідливої діяльності.***

К л ю ч о в і с л о в а : ***авторизація, децентралізовані мережі, репутація, Proof of Useful Work, безпека, взаємодія без довіри.***

Вступ

Сучасні публічні децентралізовані мережі, такі як блокчейн та peer-to-peer (P2P) системи, стають все популярнішими у багатьох сферах (Nakamoto, 2008, с. 1), зокрема й у фінансових операціях, керуванні даними й обчисленнях. Децентралізація забезпечує високий рівень безпеки та незалежності від централізованих органів (Buterin, 2014), однак, вона також створює значні виклики у сфері керування доступом до ресурсів і даних. Відсутність довіри між вузлами мережі означає, що традиційні моделі авторизації, засновані на централізованому контролі, не можуть бути ефективно застосовані в таких середовищах.

Однією з основних проблем, що виникають перед децентралізованими системами, є забезпечення безпечної та ефективної авторизації вузлів. Кожен вузол мережі може бути потенційно шкідливим або ненадійним, тому необхідно впроваджувати нові механізми авторизації, які не залежать від централізованих структур. У контексті цього дослідження особлива увага приділяється моделюванню авторизації на основі репутації вузлів та концепції Proof of Useful Work (PoUW), що дозволяють забезпечити безпеку взаємодії між вузлами без необхідності попередньої довіри.

Метою цієї статті є аналіз і розроблення нових моделей авторизації для децентралізованих систем, які зможуть розв'язати проблему довіри між вузлами та забезпечити безпечну і прозору взаємодію.

Методи

Децентралізовані мережі, такі як блокчейн та інші peer-to-peer системи, сприяли розвитку нових підходів до авторизації, які забезпечують безпечну взаємодію між вузлами без централізованого контролю (Nakamoto, 2008, с. 2). У цьому розділі розглянуто основні моделі авторизації, зокрема на основі репутації, Proof of Work (PoW), Proof of Stake (PoS) і Proof of Useful Work (PoUW).

PoW і PoS є основними моделями консенсусу в багатьох децентралізованих системах, включаючи Bitcoin та Ethereum. У PoW вузли виконують складні обчислювальні задачі для підтвердження транзакцій і забезпечення безпеки мережі, що дозволяє уникнути централізованого контролю, але вимагає значних енергетичних витрат (Bonneau et al., 2015, с. 106). У PoS, навпаки, вузли можуть підтверджувати транзакції на основі кількості криптовалюти, якою вони володіють, що значно зменшує енергоспоживання, але може призвести до централізації, оскільки вузли з більшими ресурсами мають більше повноважень (Buterin, 2014).

Один із найвідоміших протоколів PoS – це Ouroboros, який використовує різноманітні механізми для забезпечення безпеки та децентралізації. Цей протокол забезпечує високий рівень безпеки за рахунок розподілу прав верифікації залежно від часу утримання та кількості монет, що дозволяє створювати децентралізовані та надійні мережі (Kiayias et al., 2017, с. 360).

PoUW є інноваційною моделлю консенсусу, яка поєднує безпеку та корисну роботу. Відмінність PoUW від PoW полягає в тому, що вузли виконують не просто обчислення, а завдання з реальним практичним значенням, наприклад, оброблення наукових даних або великих обсягів інформації. Це дозволяє мережам

ISSN 2707-1758

використовувати ресурси раціональніше, надаючи вузлам можливість виконувати корисні завдання й одночасно забезпечувати безпеку мережі (Ball et al., 2017).

Цей підхід також стимулює вузли виконувати корисні для спільноти обчислення, зменшуючи ризики шкідливої активності та сприяючи ефективному розподілу ресурсів.

Репутаційні системи є альтернативним підходом для забезпечення авторизації в децентралізованих мережах. У репутаційних моделях кожен вузол накопичує бали репутації, що дозволяє оцінювати надійність вузла на основі його попередньої активності та взаємодії з іншими вузлами. Це дає можливість мережам працювати без централізованого контролю і стимулює вузли підтримувати високу репутацію для отримання доступу до ресурсів.

Дослідження також показують, що репутаційні моделі допомагають зменшити ризики шкідливої діяльності, оскільки вузли з низьким рівнем репутації мають обмежений доступ до важливих ресурсів мережі (Jøsang, Ismail, & Boyd, 2007, с. 618–644). Репутаційні системи широко використовують у соціальних мережах та інших онлайн-середовищах, де необхідно оцінювати надійність користувачів на основі їхньої поведінки.

Різні моделі авторизації відіграють важливу роль у керуванні доступом у децентралізованих мережах. Деякі дослідження свідчать, що такі мережі можуть працювати як "егалітарне суспільство" або ж як "доброзичлива диктатура", де вузли з високим рівнем репутації чи ресурсів отримують більші повноваження (Azouvi, Maller, & Meiklejohn, 2018, с. 127–143). Це дозволяє забезпечити стійкість і безпеку мережі, але вимагає ретельного балансування між децентралізацією та контролем для уникнення централізації.

Результати

У процесі дослідження проаналізовано дві моделі авторизації у публічних децентралізованих мережах: модель на основі репутації та модель Proof of Useful Work. Для кожної з них створено симуляційну мережу з 10 вузлів, де кожен вузол виконував певні завдання, за які отримував відповідні бали репутації або обчислювальні ресурси. В результаті вдалося отримати показники ефективності авторизації вузлів і динаміки зміни їхніх прав доступу до ресурсів мережі.

Модель авторизації на основі репутації передбачає, що кожен вузол накопичує бали репутації за виконання корисних дій для мережі, таких як оброблення транзакцій або надання обчислювальних ресурсів. Репутацію вузла розраховують за формулою

$$R_i = \sum_{j=1}^{n} \frac{W_j \cdot A_{ij}}{T_j}, \quad (1)$$

де R_i – репутація вузла *i*, A_{ij} – кількість виконаних дій вузлом і для вузла *j*, W_j – вага дії (важливість завдання для мережі), T_j – час, що минув з моменту виконання дії.

Ця формула дозволяє оцінити, наскільки важливими для мережі були виконані вузлом дії, і враховує як кількість дій, так і їхню важливість для загальної роботи системи.

Таблиця 1

Репутаційні значення вузлів до та після взаємодії

Вузол	Початкова репутація	Кінцева репутація
1	0.10	0.80
2	0.30	0.85
3	0.25	0.75
4	0.20	0.70
5	0.35	0.85
6	0.40	0.90
7	0.50	0.95
8	0.45	0.90
9	0.55	1.00
10	0.60	0.95

На основі результатів моделювання (табл. 1) можна дійти висновку, що вузли, які виконували більшу кількість завдань і взаємодіяли з іншими вузлами, отримали значно більше репутаційних балів і, відповідно, підвищили свій рівень авторизації. Репутація вузлів прямо корелює з їхньою активністю у мережі, що дозволяє зменшити ризики шкідливої активності з боку вузлів із низькою репутацією.

Модель PoUW базується на концепції, що вузли в децентралізованій мережі повинні виконувати обчислення, корисні для її функціонування, за що отримують права доступу до ресурсів. На відміну від традиційних моделей, таких як PoW, де вузли виконують обчислення, які мають обмежене практичне застосування (напр., пошук хеша для верифікації блока), PoUW стимулює вузли до виконання завдань, які приносять реальну користь спільноті (напр., обчислення наукових моделей, оброблення великих даних).

Основні принципи роботи моделі PoUW:

1. Корисні обчислення: вузли, замість витрачання ресурсів на розв'язання криптографічних задач виконують корисні для мережі обчислення. Ці обчислення можуть включати в себе наукові розрахунки, аналіз даних або інші задачі, що мають практичну цінність. Чим більше корисних обчислень виконав вузол, тим більше він отримує прав доступу до ресурсів мережі.
2. Рівень авторизації: авторизація вузла залежить від кількості виконаних ним корисних обчислень. Чим більше обчислень виконує вузол, тим вищий його рівень авторизації, що дозволяє йому доступ до більш критич-

но важливих ресурсів, таких як керування транзакціями, зберігання даних або підтвердження операцій.

Рівень авторизації визначається кількістю виконаних вузлом обчислень, що можна подати у вигляді формули

$$D_i = \frac{C_i}{C_{\max}}, \quad (2)$$

де D_i – рівень авторизації вузла i, C_i – кількість виконаних обчислень вузлом i, $C_{\max}$ – максимальна кількість обчислень, виконаних у мережі.

Ця формула забезпечує вузлам, які виконують більше корисних обчислень, вищий рівень авторизації. У свою чергу, вузли з меншою кількістю обчислень отримують менші права доступу, що гарантує рівний розподіл ресурсів відповідно до внеску кожного вузла.

Для аналізу стабільності роботи мережі та розподілу прав доступу проведено розрахунок показника Герста, що дозволяє оцінити, чи є динаміка репутаційної авторизації вузлів стійкою. Показник Герста розраховують за формулою

$$\frac{\log(R/S)}{\log(N)}, \quad (3)$$

де R/S – відношення амплітуди до стандартного відхилення, N – кількість даних.

Результати розрахунків показали, що для вузлів із високою репутацією показник Герста наближається до 0.9, що свідчить про їхню стабільність у накопиченні прав доступу. Вузли з низькою репутацією мали нижчі значення показника Герста (близько 0.5), що свідчить про нестабільність їхньої авторизації.

Дискусія і висновки

За результатами проведеного дослідження моделей авторизації вузлів у публічних децентралізованих мережах на основі репутації та PoUW можна зробити такі висновки.

Ефективність моделі авторизації на основі репутації: вузли, що активно виконували корисні для мережі дії, отримували значні покращення у рівні своєї репутації. Це забезпечувало їм доступ до більш критичних ресурсів мережі, таких як підтвердження транзакцій та управління обчислювальними завданнями. Зокрема, вузли з початково низькою репутацією, які виконали значну кількість завдань, змогли підвищити свою репутацію на 60–70 %. Це підтверджує, що модель на основі репутації є справедливим підходом до авторизації у децентралізованих мережах.

Модель PoUW забезпечує стимулювання активної участі вузлів: ця модель показала свою ефективність у забезпеченні високого рівня авторизації для тих вузлів, які виконують реальні обчислювальні завдання для мережі. Вузли, що виконали більше обчислень, отримали вищий рівень авторизації. Це дозволило їм доступ до критичних операцій, таких як зберігання важливих даних та керування транзакціями. У такий спосіб PoUW створює ефективний механізм мотивації вузлів до участі у корисній діяльності.

Динамічність і гнучкість авторизації: обидві моделі авторизації є динамічними, оскільки права доступу вузлів постійно коригуються залежно від їхньої активності та внеску у мережу. Це забезпечує справедливий розподіл ресурсів і захист від шкідливої діяльності з боку малоефективних або потенційно шкідливих вузлів. Вузли, які не виконують достатньої кількості завдань або порушують правила мережі, автоматично втрачають права доступу, що мінімізує ризик зловживань.

Безпека та стійкість мережі: за допомогою розрахунку показника Герста встановлено, що вузли з високою репутацією та значними обчислювальними ресурсами демонструють стабільну поведінку та високу стійкість у накопиченні прав доступу. Це свідчить про те, що мережа стає безпечнішою завдяки автоматичному відсіву вузлів із низькою активністю або недобросовісною поведінкою.

Мінімізація ризиків шкідливої активності: завдяки репутаційній моделі вузли з низькою активністю не можуть отримати високий рівень доступу до важливих ресурсів, що захищає мережу від можливих атак або недобросовісної поведінки. Модель PoUW, у свою чергу, стимулює вузли до виконання корисних обчислень, що також знижує ризики шкідливої активності, оскільки вузли-зловмисники не отримують достатньо прав доступу.

Запропоновані моделі можуть бути успішно інтегровані у різні типи децентралізованих систем, такі як блокчейн-платформи, peer-to-peer файлообмінники, децентралізовані обчислювальні системи тощо. Застосування репутаційної системи або PoUW дозволить підвищити надійність і безпеку таких систем, забезпечуючи справедливий розподіл ресурсів і захист від шкідливої активності.

Можливості для подальших досліджень: подальші дослідження можуть бути спрямовані на розширення можливостей моделей авторизації, зокрема й через упровадження додаткових механізмів захисту від маніпуляцій репутацією або обчислювальними ресурсами. Також є перспективи для інтеграції цих моделей з іншими підходами, що дозволить створити ще більш гнучкі та безпечні авторизаційні системи для публічних децентралізованих мереж.

Результати дослідження демонструють, що впровадження моделей авторизації на основі репутації та PoUW у публічних децентралізованих мережах значно підвищує рівень безпеки, стійкості та справедливості взаємодії між вузлами. Це дозволяє мережі функціонувати без централізованого контролю, забезпечуючи водночас прозорість і захист від шкідливої активності.

Внесок авторів: Іван Пархоменко – концептуалізація; методологія; аналіз джерел, підготування огляду літератури або теоретичних засад дослідження; Роман Огієвич – збір емпіричних даних та їх валідація; емпіричне дослідження.

Список використаних джерел

Azouvi, S., Maller, M., & Meiklejohn, S. (2018). Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance. *Financial Cryptography and Data Security*, 127–143. https://doi.org/10.1007/978-3-662-58387-6_9

Buterin, V. (2014). *Ethereum White Paper*. A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Ball, M., Rosen, A., Sabin, M., & Vasudevan, P. (2017). *Proofs of Useful Work.* IACR Cryptology ePrint Archive. https://eprint.iacr.org

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. *Annual International Cryptology Conference* (pp. 357–388). https://doi.org/10.1007/978-3-319-63688-7_12

ISSN 2707-1758

Nakamoto, S. (2008). Bitcoin. A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

References

Azouvi, S., Maller, M., & Meiklejohn, S. (2018). Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance. *Financial Cryptography and Data Security*, 127–143. https://doi.org/10.1007/978-3-662-58387-6_9

Buterin, V. (2014). *Ethereum White Paper*. A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Ball, M., Rosen, A., Sabin, M., & Vasudevan, P. (2017). *Proofs of Useful Work.* IACR Cryptology ePrint Archive. https://eprint.iacr.org

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. *Annual International Cryptology Conference* (pp. 357–388). https://doi.org/10.1007/978-3-319-63688-7_12

Nakamoto, S. (2008). *Bitcoin.* A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

Отримано редакцією журналу / Received: 01.10.24
Прорецензовано / Revised: 27.10.24
Схвалено до друку / Accepted: 13.11.24

Ivan PARKHOMENKO PhD, Assoc. Prof.
ORCID ID: 0000-0001-6889-9284
e-mail: ivan.parkhomenko@knu.ua
Taras Shevchenko National University of Kyiv, Ukraine

Roman OHIIEVYCH, PhD Student
ORCID ID: 0009-0003-7948-1125
e-mail: r.ohiievych@gmail.com
Taras Shevchenko National University of Kyiv, Ukraine

AUTHORIZATION MODELS FOR TRUSTLESS NODE INTERACTION IN PUBLIC DECENTRALIZED NETWORKS

Background. ***Decentralized networks, such as blockchain and peer-to-peer systems, have become the foundation for new technologies that ensure the security and transparency of operations without the need for centralized control authorities. These networks enable interaction between nodes without prior trust. However, ensuring reliable and efficient authorization in such networks presents a challenge due to the absence of a single authorization center. This creates the need to develop new models that allow secure access management based on the interaction between nodes. One of the main issues is that each node can potentially be malicious, and traditional authorization models used in centralized systems cannot provide the necessary level of security. The purpose of this study is to explore new approaches to authorization in public decentralized networks that do not require trust between participants.***

Methods. ***The research investigates reputation-based authorization models and Proof of Useful Work (PoUW) models, which show promise for decentralized systems. The reputation model grants access rights based on the node's previous activity in the network, where each node accumulates reputation points for completing specific tasks. The second model, PoUW, allows nodes to gain authorization based on the number of useful computations performed. This approach not only enhances network security but also incentivizes nodes to carry out computational tasks that have practical value for the community.***

Results. ***Modeling has shown that both models effectively ensure the security and reliability of interaction between nodes. Nodes with a high reputation level or those that have completed a significant volume of useful computations gain access to critical network resources. The implementation of such approaches reduces the risk of malicious activity, as nodes that do not perform useful actions are restricted in their access rights.***

Conclusions. ***The proposed authorization models based on reputation and Proof of Useful Work have demonstrated high efficiency in public decentralized networks. They enable secure interaction between nodes without the need for trust, making these approaches promising for future implementation in various fields. The use of these models provides dynamic access management to resources, minimizing the risks of malicious activity.***

Keywords: ***authorization, decentralized networks, reputation, Proof of Useful Work, security, trustless interaction.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.