https://doi.org/10.31891/2307-5732-2025-351-20
УДК 004.82

**ЄЩЕНКО МИКОЛА**
Національний університет «Києво-Могилянська академія»
https://orcid.org/0000-0002-5549-3565
e-mail: m.yeshchenko@ukma.edu.ua

# МОДЕЛЮВАННЯ АТАК НА БЛОКЧЕЙН ТА МЕХАНІЗМІВ ЇХНЬОЇ ПРОТИДІЇ ВИКОРИСТОВУЮЧИ МУЛЬТИАГЕНТНІ СИСТЕМИ

*Зростання інтересу до блокчейну та криптовалют стимулює дослідження та використання атак, які можуть бути спрямовані на різні частини системи. Наприклад, деякі атаки спрямовані на мережу або саму систему через шардинг, DDOS-атаки або атаки через червоточину. Деякі інші атаки, такі як атака 51%, мають на меті отримати більшу частку виробничих потужностей системи. Завдяки цим повноваженням зловмисник або група зловмисників можуть задля власної користі переписувати блокчейн, виконувати атаки з подвійними витратами або цензурувати будь-яку сутність на свій вибір.*

*Інші типи атак поєднують кілька векторів атак в один, будуючи конкурентоспроможний ланцюжок за допомогою необізнаних учасників, які раніше були ізольовані від мережі за допомогою атаки затемнення. Також існують методи атак, що спираються використання помилок смарт-контрактів/децентралізованих програм. Більшість децентралізованих програм сприйнятливі до атак фаворитизму, за яких зловмисник несправедливо використовує інформацію, пов'язану з подіями, які ще не були записані в блокчейні.*

*Наданий перелік векторів атак, незважаючи на його невичерпність, спрямований на те, щоб підкреслити той факт, що системи блокчейн мають вразливості. Наявність останніх вказує на необхідність просування детальної інформації про механізми убезпечення блокчейну через їх моделювання.*

*Ця стаття покликана вивчити можливості моделювання найпоширеніших типів атак на блокчейн за допомогою організаційно-орієнтованого методу моделювання, а також показати на практиці метод моделювання регуляційних механізмів через відтворення спеціальних метаагентів – регуляційних агентів – які відповідають за злагоджену роботу всієї системи, і зокрема сприяють опору атак на мережу шляхом перевірки пропонованих транзакцій на відповідність закладеним правилам, що дозволяє прийняти рішення про їхнє схвалення чи відхилення.*

*Подальші дослідження можуть стосуватися моделювання мотивації агентів системи у разі відхилення транзакції регуляційними агентами.*

*Ключові слова: блокчейн, мультиагентні системи, моделювання, смарт-контракти, регуляційні агенти.*

**YESHCHENKO MYKOLA**
National University of Kyiv-Mohyla Academy

## MODELING BLOCKCHAIN ATTACKS AND MECHANISMS OF THEIR COUNTERACTION USING MULTI-AGENT SYSTEMS

*The growing interest in blockchain and cryptocurrencies is driving the research and use of attacks that can target different parts of the system. For example, some attacks target the network or the system itself through sharding, DDOS attacks, or wormhole attacks. Some other attacks, such as the 51% attack, aim to acquire a majority share of the production capacity in the system. With these powers, an attacker or group of attackers can rewrite the blockchain at will, perform double-spend attacks, or censor any entity they choose.*

*Other attack types combine multiple attack vectors into one, building a competitive chain using unknown participants that were previously isolated from the network via an obfuscation attack. Other attack methods also exist through exploitation of smart contracts/decentralized applications bugs. Most decentralized applications are susceptible to favouritism attacks, where an attacker unfairly exploits information related to events that have not yet been recorded on the blockchain.*

*Provided list of attack vectors, despite its inexhaustibility, is aimed to emphasize the fact that blockchain systems have vulnerabilities. The presence of the latter indicates the need to promote detailed information about blockchain security mechanisms through their simulation.*

*This article is designed to explore the possibilities of modeling the most common types of attacks on the blockchain by using an organization-oriented modeling method, as well as to show in practice the method of modeling regulatory mechanisms through the reproduction of special meta-agents – regulatory agents – responsible for the coordinated operation of the entire system, and in particular contributing to resistance attacks on the network by checking the proposed transactions for compliance with the rules laid down in them, which results in endorsement or rejection of the former.*

*Further research may involve modeling the motivation of system agents in the event of rejection of transactions by regulatory agents.*

*Keywords: blockchain, multi-agent systems, modeling, smart-contracts, regulatory agents.*

Стаття надійшла до редакції / Received 11.04.2025
Прийнята до друку / Accepted 26.04.2025

### Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Швидке набуття популярності технологією блокчейн призвело до динамічного поширення рішень на її основі. І хоча блокчейн часто є правильним вибором для розробки розподілених застосунків, його використання без достатнього розуміння природи технології може призвести до неефективності або ж навіть утворення вразливостей у створюваній програмі. Моделювання атак на блокчейн та засобів їхньої протидії за допомогою мультиагентних систем покликане наочно

проілюструвати потенційні небезпеки викликані особливостями реалізації блокчейну, та дедалі заохотити її обізнане використання у медичній, фінансовій, правовій та інших галузях.

**Аналіз досліджень та публікацій**

Статті [1-5] досліджують різні види атак на блокчейн, в тому числі найбільш поширені – атаки червоточини, фаворитні та атаки затемнення. Автори [6-10] доводять загальні можливості моделювання технології блокчейн через використання мультиагентних систем, але не вдаються до детального аналізу та подальшого утворення безпекових механізмів блокчейну.

Проведений аналіз показав, що останні дослідження за темою бракують моделювання регуляційної частини технології блокчейн, яка є важливою частиною для його функціонування.

**Формулювання цілей статті**

**Метою роботи є:** моделювання засобами мультиагентних систем регуляційних механізмів блокчейну, що відповідають за протидію найбільш розповсюдженим типам атак, задля розповсюдження відомостей про технічні особливості, що має сприяти поширенню обізнаного використання технології блокчейн.

**Виклад основного матеріалу**

**Атаки на блокчейн**

Наразі відомі такі 3 найбільш розповсюджені типи атак на системи блокчейн:

- Атаки червоточини [1, 2] – спираються на створенні підмережі із злочинних вузлів, які передаватимуть інформацію швидше за існуючі зв'язки в системі задля подальших маніпуляцій з нею;
- Фаворитні атаки [3, 4] – характеризуються намаганням набути контроль (наприклад, через здобуття переважної частки виробничих потужностей в системі) задля подальших маніпуляцій механізмами блокчейну на користь зловмисників;
- Атаки затемнення [5] – намагаються будувати змагальний ланцюг шляхом залучення необізнаних учасників, що до цього перебували в ізольованому від мережі стані.

Розглянемо кожен тип детальніше.

**Фаворитні атаки**

У цій атаці зловмисник постійно відстежує транзакції, що очікують в черзі на розгляд, і користується перевагами процесу відбору/створення блоку транзакцій, щоб запустити іншу транзакцію в прибутковий спосіб. Наприклад, на децентралізованій біржі зловмисник може побачити, що користувач має намір придбати значну кількість певного активу, і тому очікує, що ціна значно зросте. У такій ситуації зловмисник може спробувати ініціювати транзакцію-фаворит, яка б виконалася до згаданої користувацької транзакції, щоб придбати частину активу раніше чесного користувача та отримати прибуток від атаки. Зловмисник може зробити це, ініціювавши транзакцію з великою комісією, таким чином гарантуючи, що творці блоку виберуть саме її, або ж просто будучи творцем блоку. Ця атака не використовує жодної вразливості та не відхиляється від протоколу, і є можливою лише завдяки тому факту, що блокчейн робить майбутні події та наміри відомими кожному учаснику заздалегідь.

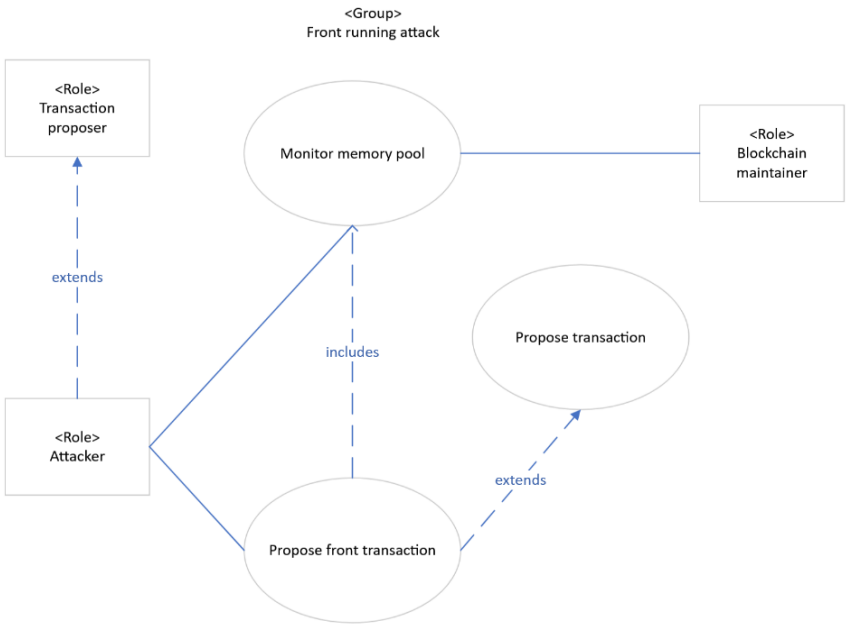


**Рис. 1. Організаційна структура фаворитної атаки**

Ця атака моделюється за допомогою ролі зловмисника, яка відрізняється від Transaction Proposer, як показано на рисунку 1. Зловмисник покладається на роль Blockchain Manager, щоб отримати поточну інформацію про незавершені транзакції через поведінку Monitor Memory Pool. Коли в пулі пам'яті знайдено вигідний початковий сценарій, зловмисник створює початкову транзакцію та пропонує її мережі за допомогою відхиленої поведінки Propose Front Transaction (пропонування транзакції-фаворита).

**Атака затемнення**

У даному типі атаки [2] зловмисник встановлюється між своєю жертвою(-ами) та рештою системи, розділяючи мережу. Потім зловмисник контролює, що надсилає та отримує жертва(-и). Зловмисник може заразити мережевий маршрутизатор або безпосередньо агента, щоб контролювати як вхідний, так і вихідний трафік. Агенти-жертви не знають, що вони заражені, і можуть отримувати інші блоки та транзакції, ніж решта системи, залежно від того, що зловмисник хоче повідомити. Вплив такої атаки може варіюватися від збільшення затримки розповсюдження до створення змагальних ланцюгів, що, можливо, призведе до спроб подвійних витрат. Наприклад, у разі створення змагального ланцюга в блокчейні PoW, жертви можуть здійснювати майнінг у змагальному ланцюзі, створеному зловмисником, не підозрюючи про це, таким чином сприяючи зловмисним намірам зловмисника, поводячись коректно відносно протокола, як описано в [5].

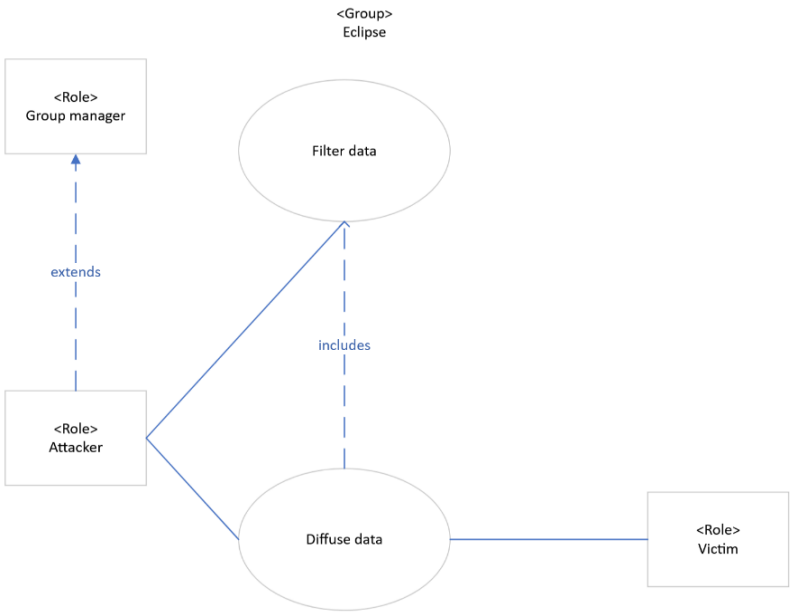


**Рис. 2. Організаційна структура атаки затемнення**

Атаку затемнення можна змоделювати за допомогою загальної моделі, як показано на рисунку 2. Погляд жертви на систему блокчейн контролюється відхиленням ролі супроводжуючого блокчейн від зловмисника, який фільтрує та розповсюджує лише ті дані, які він хоче, щоб бачила його жертва. Подібним чином будь-які дані, отримані від агентів-жертв, будуть відфільтровані, перш ніж бути збереженими або переданими в усю систему блокчейну. Ізольовані агенти моделюються як агенти з роллю жертви, тобто, хоч вони і вважають себе підключеними до всієї системи блокчейну, насправді вони підключені лише до зловмисника та, можливо, інших жертв. Роль жертви не передбачає будь-яких поведінкових відхилень.

**Атака червоточини**

Під час атаки через червоточину два або більше зловмисників, розташованих у різних точках мережі, створюють накладену мережу для передачі інформації швидше, ніж в основній мережі P2P. Вони роблять це шляхом зміни/додавання до ролей Propose Transaction і Propose Block і їх пов'язаної поведінки. Ця атака спрямована на отримання несправедливої переваги над іншими учасниками, покладаючись виключно на довший час розповсюдження мережі P2P [5]. Крім того, зловмисники також можуть вибрати передачу лише релевантної інформації відповідно до своїх критеріїв, такої як дуже цінні транзакції або ініціювання нового блоку.

Як показано на рисунку 3, ця атака моделюється через роль Attacker, яка довизначає загальну дифузну поведінку. Всі отримані дані будуть оброблені поведінкою Filter Data, щоб оцінити їх релевантність для зловмисників перед передачею через червоточину за допомогою методу Diffuse Data through Wormhole. На рисунку 3 показано, як зловмисники можуть створити таку червоточину, щоб подолати погану топологію мережі. У будь-який момент часу зловмисник може додати нового агента до групи. Зловмисники можуть це зробити, оскільки всі вони мають роль Group Manager і, отже, можуть розширити свою атаку, якщо це буде визнано потрібним та вигідним.

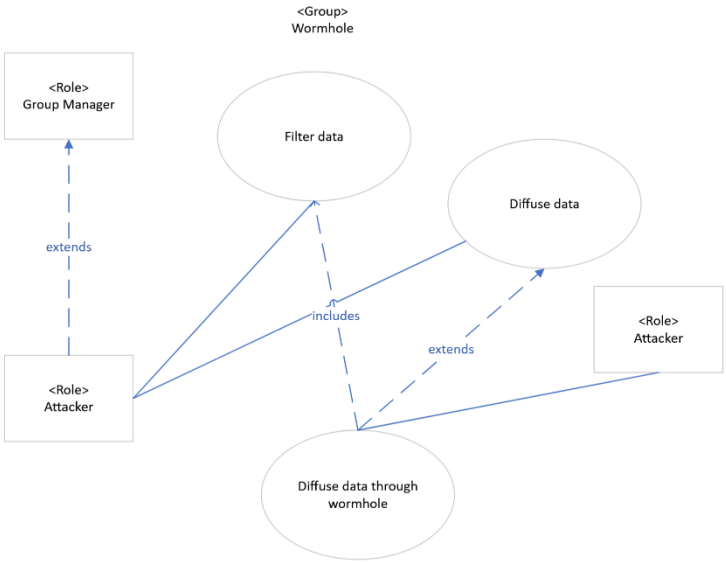


**Рис. 3. Організаційна структура атаки червоточини**

**Моделювання регуляційних механізмів блокчейну**

Статті [6-10] надають достатньо інформації для створення загальної моделі блокчейну засобами мультиагентних систем. Розглянемо детальніше, що необхідно для моделювання регуляційної частини технології блокчейн.

Мультиагентні системи можуть бути ефективно використані для моделювання регуляційних механізмів у блокчейн-мережах, спрямованих на досягнення різних цілей, таких як оптимізація процесів та моніторинг небажаної поведінки.

Одним із ключових аспектів є роль регуляційних агентів. В рамках MAS можна створювати моделі регуляційних органів як спеціальних метаагентів, що функціонують у мережі блокчейн. Такі агенти забезпечують дотримання встановлених норм і правил, відстежуючи транзакції та взаємодії учасників мережі. Вони спроектовані для виявлення відхилень від заздалегідь визначених стандартів і впровадження відповідних заходів. Динамічна адаптація регуляційних механізмів можлива через впровадження алгоритмів машинного навчання.

Іншим важливим напрямком є використання смарт-контрактів для регулювання. Вони можуть бути впроваджені в блокчейн-мережу для автоматичного дотримання регуляційної політики. MAS дозволяє моделювати ці контракти як автономних агентів, здатних виконувати визначені правила та застосовувати санкції або надавати винагороди відповідно до поведінки учасників мережі, тим самим заохочуючи чи пригнічуючи окремо взятих агентів залежно від патернів їхньої поведінки.

Загалом мультиагентні системи надають універсальну структуру для моделювання механізмів регулювання в мережах блокчейн, що дозволяє оптимізацію під різні цілі, одночасно забезпечуючи дотримання нормативних вимог і виявлення небажаної поведінки.

**Регуляційні агенти**

Регуляційні агенти можуть бути реалізовані в рамках мультиагентної системи (MAS) з використанням мов програмування або платформ, які підтримують моделювання та імітацію агентів. Для впровадження таких агентів необхідно спершу визначити їх архітектуру, що включає внутрішній стан, процеси прийняття рішень, протоколи зв'язку та механізми взаємодії з іншими агентами й мережею блокчейн. Окрім цього, важливо створити середовище, в якому ці агенти функціонуватимуть, тобто забезпечити наявність таких елементів, як мережа блокчейн, смарт-контракти, історія транзакцій, топологія мережі та інші фактори, що можуть впливати на їх поведінку. Необхідно розробити логіку, засновану на правилах, що регулюватимуть поведінку агентів. Ці правила, закодовані через логічні твердження, обмеження та умови, визначатимуть прийнятну поведінку в мережі блокчейн. Додатково, агенти повинні мати алгоритми для моніторингу та виявлення небажаної поведінки, що дозволяють аналізувати транзакційні дані, мережеву активність та іншу відповідну інформацію для виявлення аномалій або порушень регуляційної політики.

Для ефективного реагування регуляційними агентами на порушення або відхилення від встановлених правил, потрібно розробити механізми прийняття рішень. Ці механізми дозволяють агентам видавати попередження, накладати штрафи, ініціювати розслідування або повідомляти інші регуляційні органи. Крім того, важливим є визначення протоколів комунікації між агентами та іншими учасниками мережі, що забезпечують співпрацю, обмін інформацією та скоординовані відповіді на нормативні виклики. Для адаптивної поведінки і постійного вдосконалення необхідно включити алгоритми навчання, що дозволяють агентам вчитися на минулому досвіді, зворотному зв'язку з середовища та взаємодії з іншими агентами.

Інтеграція регуляційних агентів в блокчейн-мережу є важливим етапом, що вимагає використання відповідних інтерфейсів, API або проміжного програмного забезпечення для доступу до даних транзакцій та інших ресурсів мережі. Після цього необхідно провести тестування та валідацію агентів у симуляційних середовищах або на реальних даних для оцінки їх ефективності. В кінцевому рахунку, після розгортання агентів у блокчейн-мережі, важливо постійно відслідковувати їх ефективність у реальному часі, оновлювати та обслуговувати їх з метою адаптації до нових викликів, змін нормативних вимог і нових загроз.

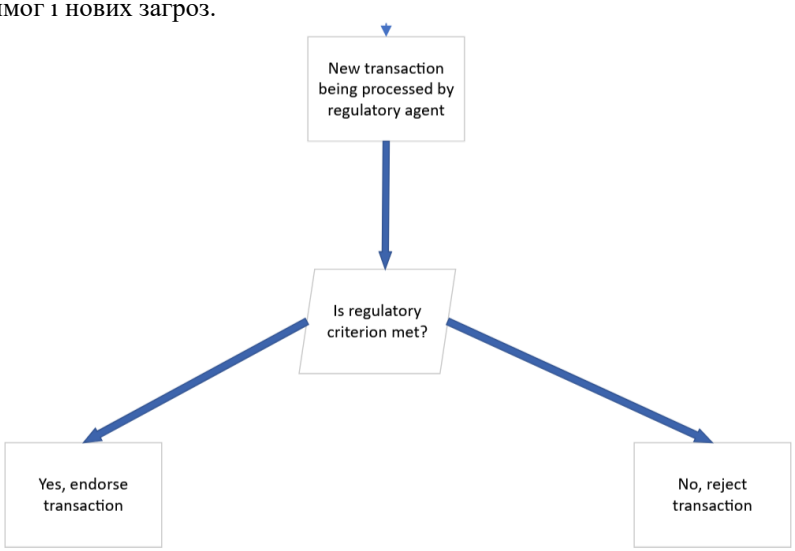


**Рис. 4. Перевірка транзакції регуляційним агентом**

Дотримуючись цих кроків, регулюючі агенти можуть бути ефективно впроваджені в мультиагентну систему для забезпечення дотримання правил, моніторингу поведінки та підтримки цілісності мереж блокчейн. Що і було зроблено практично шляхом впровадження регуляційного індосанта угоди (Transaction Regulatory Endorser). Він дозволяє встановлювати максимально допустиму суму транзакції. Кожна транзакція під час її схвалення проходить перевірку, під час якої з'ясовується чи запрошена сума менша за встановлений ліміт, що показано на рисунку 4. У випадку невдачі транзакція відбраковується. Похідні від даного класу агенти є регуляційними та не допускають шкідливі транзакції за описаним правилом. Аналогічним чином можуть бути встановлені й будь-які інші регуляційні правила, за дотриманням яких будуть слідкувати агенти даного типу.

Залишається детально не розглянутим питання мотивації агентів системи за результатами проходження перевірок регуляційними агентами.

## Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Незважаючи на ряд відомих атак на блокчейн, сфера його застосування продовжує зростати через актуальність використання розподілених систем. Дана стаття покликана сприяти цьому явищу, надаючи подробиці особливостей реалізації технології блокчейн через абстракцію мультиагентних систем. Проаналізовані публікації та пропоновані ними моделі блокчейну стали підгрунтям для моделювання його принципів регуляції в цій статті.

Недоліки дизайну блокчейну, що експлуатуються у розглянутих поширених типах атак, частково покриті закладеними в технології механізмами. Досліджена саморегуляція – один з них. Вдало змодельована особливість до саморегуляції блокчейну через використання спеціального типу агентів – регуляційних – доводить комплексність модельованої технології та дозволяє поглянути на відомі принципи її роботи під новим кутом.

Темою подальших досліджень може бути моделювання мотивації агентів системи у випадку відхилення транзакції регуляційними агентами.

## Література

1. BDoS: Blockchain Denial-of-Service / Michael Mirkin et al. // CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event USA. – New York, NY, USA, 2020. – DOI: https://doi.org/10.1145/3372297.3417247.

2. Apostolaki M. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies / Maria Apostolaki, Aviv Zohar, Laurent Vanbever // 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017. – [S. l.], 2017. – DOI: https://doi.org/10.1109/sp.2017.29.

3. Eyal I. Majority Is Not Enough: Bitcoin Mining Is Vulnerable / Ittay Eyal, Emin Gün Sirer // Financial Cryptography and Data Security. – Berlin, Heidelberg, 2014. – P. 436–454. – DOI:

https://doi.org/10.1007/978-3-662-45472-5_28.

4. Sapirshtein A. Optimal Selfish Mining Strategies in Bitcoin / Ayelet Sapirshtein, Yonatan Sompolinsky, Aviv Zohar // Financial Cryptography and Data Security. – Berlin, Heidelberg, 2017. – P. 515–532. – DOI: https://doi.org/10.1007/978-3-662-54970-4_30.

5. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack / Kartik Nayak [et al.] // 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 21–24 March 2016. – [S. l.], 2016. – DOI: https://doi.org/10.1109/eurosp.2016.32.

6. From Agents to Blockchain: Stairway to Integration / Giovanni Ciatto et al. // Applied Sciences. – 2020. – Vol. 10, no. 21. – P. 7460. – DOI: https://doi.org/10.3390/app10217460

7. Santana C. Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda / Carlos Santana, Laura Albareda // Technological Forecasting and Social Change. – 2022. – Vol. 182. – P. 121806. – DOI: https://doi.org/10.1016/j.techfore.2022.121806

8. Alharby M. BlockSim: An Extensible Simulation Tool for Blockchain Systems / Maher Alharby, Aad van Moorsel // Frontiers in Blockchain. – 2020. – Vol. 3. – DOI: https://doi.org/10.3389/fbloc.2020.00028

9. Decentralized Autonomous Organizations: Concept, Model, and Applications / Shuai Wang et al. // IEEE Transactions on Computational Social Systems. – 2019. – Vol. 6, no. 5. – P. 870–878. – DOI: https://doi.org/10.1109/tcss.2019.2938190

10. Rocha H. Preliminary steps towards modeling blockchain oriented software / Henrique Rocha, Stéphane Ducasse // ICSE '18: 40th International Conference on Software Engineering, Gothenburg Sweden. – New York, NY, USA, 2018. – DOI: https://doi.org/10.1145/3194113.3194123

**References**

1. BDoS: Blockchain Denial-of-Service / Michael Mirkin et al. // CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event USA. – New York, NY, USA, 2020. – DOI: https://doi.org/10.1145/3372297.3417247.

2. Apostolaki M. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies / Maria Apostolaki, Aviv Zohar, Laurent Vanbever // 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017. – [S. l.], 2017. – DOI: https://doi.org/10.1109/sp.2017.29.

3. Eyal I. Majority Is Not Enough: Bitcoin Mining Is Vulnerable / Ittay Eyal, Emin Gün Sirer // Financial Cryptography and Data Security. – Berlin, Heidelberg, 2014. – P. 436–454. – DOI: https://doi.org/10.1007/978-3-662-45472-5_28.

4. Sapirshtein A. Optimal Selfish Mining Strategies in Bitcoin / Ayelet Sapirshtein, Yonatan Sompolinsky, Aviv Zohar // Financial Cryptography and Data Security. – Berlin, Heidelberg, 2017. – P. 515–532. – DOI: https://doi.org/10.1007/978-3-662-54970-4_30.

5. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack / Kartik Nayak [et al.] // 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 21–24 March 2016. – [S. l.], 2016. – DOI: https://doi.org/10.1109/eurosp.2016.32.

6. From Agents to Blockchain: Stairway to Integration / Giovanni Ciatto et al. // Applied Sciences. – 2020. – Vol. 10, no. 21. – P. 7460. – DOI: https://doi.org/10.3390/app10217460

7. Santana C. Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda / Carlos Santana, Laura Albareda // Technological Forecasting and Social Change. – 2022. – Vol. 182. – P. 121806. – DOI: https://doi.org/10.1016/j.techfore.2022.121806

8. Alharby M. BlockSim: An Extensible Simulation Tool for Blockchain Systems / Maher Alharby, Aad van Moorsel // Frontiers in Blockchain. – 2020. – Vol. 3. – DOI: https://doi.org/10.3389/fbloc.2020.00028

9. Decentralized Autonomous Organizations: Concept, Model, and Applications / Shuai Wang et al. // IEEE Transactions on Computational Social Systems. – 2019. – Vol. 6, no. 5. – P. 870–878. – DOI: https://doi.org/10.1109/tcss.2019.2938190

10. Rocha H. Preliminary steps towards modeling blockchain oriented software / Henrique Rocha, Stéphane Ducasse // ICSE '18: 40th International Conference on Software Engineering, Gothenburg Sweden. – New York, NY, USA, 2018. – DOI: https://doi.org/10.1145/3194113.3194123