УДК 004.82, 004.832
DOI: 10.18523/2617-3808.2024.7.51-57

Єщенко М. С.

МОДЕЛЮВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

У статті розглянуто ключові характеристики технології блокчейну і підходи до комплексного моделювання блокчейну з відтворенням усіх його атрибутів. Визначено найбільш перспективний спосіб моделювання для подальшого дослідження.

Ключові слова: блокчейн, мультиагентні системи, моделювання.

Вступ

Блокчейн є дуже привабливою технологією, оскільки він надає публічний, відкритий тільки для додавання, незмінний і впорядкований журнал транзакцій. Системи блокчейну за своєю суттю є міждисциплінарними, оскільки вони поєднують різні сфери, такі як криптографія, мультиагентні системи, розподілені системи, соціальні системи, економіка та фінанси. Крім того, вони мають дуже активну та динамічну екосистему, де постійно розробляються нові блокчейн-платформи та алгоритми завдяки інтересу громадськості та галузей до цієї технології. З огляду на складність і багатогранність блокчейну, його представлення — моделювання — іншими, більш відомими засобами має посприяти поліпшенню розуміння можливостей та особливостей цієї технології.

Ця стаття покликана дослідити основні способи моделювання технології блокчейну і визначити найбільш перспективний для подальшого дослідження можливостей моделювання всіх аспектів технології блокчейну.

Попередні відомості про блокчейн-системи

Структура даних блокчейну

Структуру даних блокчейну можна моделювати як динамічне дерево, відкрите лише для додавання, в якому кожен блок містить криптографічне посилання на попередній блок. Кореневий блок також відомий як блок генезису. Найдальший блок від блоку генезису називають головою блокчейну.

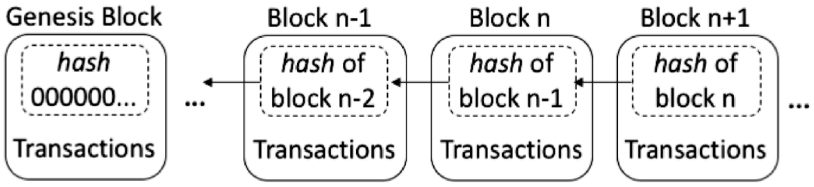

Рис. 1. Структура даних блокчейну [22]

Основи систем блокчейну

Із технічного погляду, усі учасники зберігають непідтверджені транзакції у власних пулах пам'яті, а підтверджені транзакції — у своїх локальних блокчейнах.

Є два основні типи учасників для всіх типів блокчейн-систем: користувачі та автори блоків. Користувачі створюють транзакції із певною винагородою і пропонують їх, поширюючи мережею блокчейну для підтвердження (тобто повного впорядкування та криптографічного пов'язання з блокчейном). Кожен учасник, отримуючи запропоновану транзакцію, підтверджує та поширює її для своїх сусідів. Після отримання певної кількості транзакцій автори блоків вибирають транзакції для підтвердження та впорядковують їх, створюючи спеціальний блок за допомогою механізму консен-

сусу блокчейну, наприклад, Proof-of-Work (PoW), Proof-of-Stake (PoS), Делегованого Proof-of-Stake (DPoS), Візантійської відмовостійкості (BFT). Залежно від механізму, який використовують, і технології блокчейну, ініціаторів (пропонентів) створення блоків називають «майнерами» [15], «валідаторами» [24], «пекарями» [7], «замовниками» [10], «членами комітетів» [2] тощо. Успішний пропонент блоку пропонує свій блок, поширюючи його в мережу для додавання до локальних блокчейнів. Кожен учасник, який отримує запропонований блок, перевіряє його на свій локальний блокчейн і поширює його для своїх сусідів. Після включення свого блоку всіма учасниками відповідний успішний ініціатор блоку отримує винагороду R + Fi, де R — статична винагорода за блок, а Fi — загальна сума винагород за транзакції, включені в блок i. Отже, користувач і учасники, що пропонують блок, разом підтримують спільну структуру даних, яку називають блокчейном.

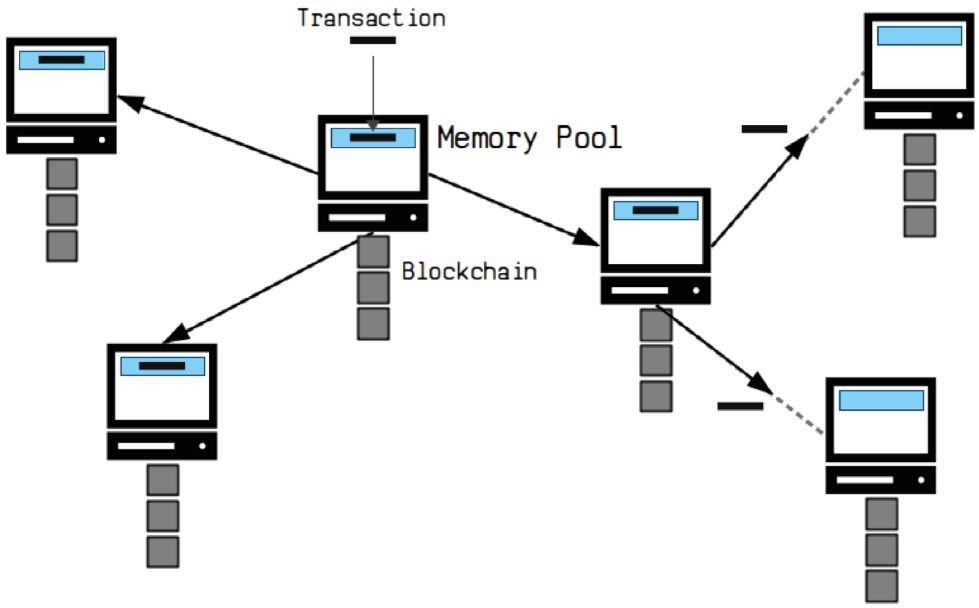

Рис. 2. Зберігання транзакцій

Щоб покращити свої можливості створення блоків, автори блоків можуть інвестувати в обладнання, капітал або інші агенти залежно від механізму консенсусу, який використовують. Наприклад, у блокчейні PoW вони можуть інвестувати в нове обладнання, оскільки що більша обчислювальна потужність у них є, то легше їм створювати блоки. У блокчейні PoS вони можуть інвестувати в ставки, оскільки що більше у них заблокованих ставок, то більше шансів увійти до комітету. На додаток до PoS, у блокчейнах DPoS вони також можуть інвестувати в інших пропонентів блоків, делегуючи свої частки.

Хоча блокчейни спочатку забезпечували лише операції, пов'язані з криптовалютою, у 2014 р. було представлено підтримку повних за Тьюрингом смарт-контрактів (SC), які кодують довільну логіку оброблення даних [24]. Завдяки цьому прогресу блокчейни еволюціонували від простих криптовалютних платформ до розподілених транзакційних і логічних систем. У блокчейнах із підтримкою смарт-контрактів транзакції, що складаються із викликів смарт-контрактів, виконують усі учасники, які бажають постійно підтримувати стан блокчейну. Сьогодні такі блокчейн-системи можна розглядати як децентралізовані комп'ютери світового масштабу, найвідомішим прикладом яких є Ethereum [3].

Підходи до моделювання технології блокчейн

Модель — це абстракція деяких аспектів наявної чи планованої системи. Моделі слугують певним цілям, наприклад для представлення зрозумілого людині опису деяких аспектів системи або інформації у формі, яку можна ефективно проаналізувати. У контексті блокчейну існує невелика кількість досліджень, які спрямовані безпосередньо на моделювання [8; 9]. На основі наявних досліджень у літературі про блокчейн було визначено такі парадигми моделювання: процесно-орієнтова-

ну, об'єктно-орієнтовану, теоретико-графову та агентно-орієнтовану парадигми. Кожну буде описано з метою висвітлення інформації про те, як вони моделюють учасників (тобто користувачів і ініціаторів блоків), взаємодії, поведінку та структури даних (наприклад, блокчейни, транзакції) за допомогою надаваних ними абстракцій.

Процесно-орієнтована парадигма

У процесно-орієнтованій парадигмі (вона ж парадигма розподіленого програмування) система охоплює кілька розподілених процесів (абстракція процесу може представляти фізичний або віртуальний комп'ютер, процесор у комп'ютері або певний потік виконання в паралельній системі), пов'язаних комунікаційними каналами (наприклад, спільною пам'яттю або консенсусом), які співпрацюють над певним спільним завданням [4].

Процеси виконують призначений їм розподілений алгоритм через набір компонентів, що реалізують алгоритм у цих процесах. Канали дають змогу процесам транслювати повідомлення, запускаючи події. Спільна пам'ять дозволяє локально здійснювати прямий доступ до ресурсу з, можливо, багатьох процесів. Механізми консенсусу спрямовані на надання процесу для узгодження спільного рішення/результату в рамках децентралізованої системи. Ця парадигма спрямована на створення та/або аналіз систем, які є надійними (пропонуючи надійність і безпеку) і мають передбачувану поведінку навіть за негативного впливу навколишнього середовища (пропонуючи толерантність до несправностей).

Багато досліджень використовують цю парадигму для аналізу [5; 18] та/або побудови блокчейнів [15; 10; 24], залучаючи такі пов'язані абстракції: учасники (наприклад, користувачі та пропоненти блоків) моделюються як процеси, взаємодії — як канали, блокчейн — як спільна пам'ять, а прийняття рішення про загальний блок представлено за допомогою консенсусних абстракцій.

Наприклад, [5] показує, що деякі ініціатори блоків у блокчейні біткойн (також відомі як майнери) можуть відхилятися від своєї номінальної поведінки, таким чином отримуючи несправедливу перевагу, яка, як наслідок, знижує надійність системи. Пізніше [19] будує та вдосконалює обидва [5; 18], надаючи гібридну стратегію, що відхиляється як на рівні створення блоку, так і на мережевому рівні, ефективно досягаючи несправедливої переваги для майнерів, водночас змушуючи інших агентів працювати на майнерів, які відхиляються.

Теоретико-графова парадигма

Теоретико-графова парадигма зосереджена на топології, а отже, на сполучних властивостях алгебраїчних/математичних об'єктів. У контексті розподілених обчислень ці об'єкти є узагальненнями графів, а їхні властивості зв'язування пов'язані з обчислюваністю розподілених алгоритмів. Використання певних топологічних властивостей геометричних об'єктів більшої розмірності для підтвердження результатів розподілених алгоритмів називають топологічним підходом до розподілених обчислень. Методи з комбінаторної та алгебраїчної топології мають розширену характеристику синхронних та асинхронних розподілених алгоритмів, а також їх розв'язуваність [16]. У теорії графів вершина — це точка в графі. Вершини з'єднані між собою ребрами, які представляють відношення між двома вершинами.

У цій парадигмі учасники моделюються за допомогою абстракцій вершин, транзакції — за допомогою абстракцій країв, взаємодії — за допомогою абстракцій симплексу та/або граней, а шахрайство моделюється як абстракції просторово-часового шаблону.

Здатність структур теорії пучків розшифровувати глобальну інформацію з локальної інформації призвела до різноманітності застосувань, як-от тих, що були запропоновані для моделювання одночасних процесів у розподілених системах [12], семантики для об'єктно-орієнтованих мов програмування [23] та представлень інформаційних систем [17]. У [14] досліджуються топологічні моделі розподілених обчислень для технологій блокчейну, орієнтованих на масштабованість. Для цього автор моделює блок як пучок і розробляє теорію розподілених консенсусних протоколів.

Об'єктно-орієнтована парадигма

В об'єктно-орієнтованій парадигмі система складається з кількох об'єктів (також відомих як екземпляри класів), які взаємодіють із локальними або віддаленими викликами методів (також їх нази-

вають передаванням повідомлень) [11]. Класи мають певні обов'язки, і вони інкапсулюють дані (у формі абстракцій атрибутів) і код (у формі абстракцій методів), який маніпулює цими даними, і пов'язані один з одним за допомогою абстракцій асоціацій. Ця парадигма спрямована на створення та/або аналіз систем, які можна розвивати (тобто легко розширювати) і підтримувати (тобто легко виправляти).

Кілька досліджень явно використовують цю парадигму в літературі про блокчейн [1; 13]. У цих дослідженнях учасники моделюються як клас, взаємодії — як асоціації, блокчейн — як клас, а рішення щодо спільного блоку — як абстракції методу.

Наприклад, [1] пропонує загальну модель блокчейну PoW із метою створення розширюваного симулятора блокчейну. Наразі вони можуть моделювати та імітувати як Bitcoin, так і Ethereum 1.0 і перевіряти свої результати на історичні дані. Вони сумісні з блокчейном PoS, враховуючи кілька модифікацій. Як інший приклад, [13] пропонує нотацію на основі UML для підтримки дизайну смарт-контракту. Зокрема, вони додають стереотипи для діаграм класів і послідовностей UML, щоб краще виразити сутності та взаємодію між ними.

Агентно-орієнтована парадигма

У агентно-орієнтованій парадигмі система складається з кількох автономних агентів, які здатні сприймати своє оточення, міркувати незалежно (реактивно чи проактивно) і впливати на своє оточення [6; 25], утворюючи таким чином так звану мультиагентну систему (MAS). Ця парадигма спрямована саме на створення та/або аналіз систем, які мають деякий ступінь відкритості, автономності, розумності та складності. Моделювання через MAS розглядалося з двох основних поглядів: орієнтованого на агента та орієнтованого на організацію. У той час як перший зосереджується на внутрішній архітектурі агента, другий спирається на структуру системи та першочергово розглядає агентів як порожні оболонки, щоб зосередитися на організаційних аспектах MAS. Агент — це суб'єкт системи, який покладається на певний ступінь автономії для досягнення своєї мети або виконання своїх функцій пасивно чи активно. Координація — це засіб, за допомогою якого агенти обмінюються інформацією або ресурсами для досягнення мети.

Багато досліджень використовують цю парадигму як агентоцентрований засіб для аналізу блокчейнів [20; 21]. У цих дослідженнях учасники моделюються як агенти, взаємодії — як координаційні абстракції, блокчейн — як спільні знання, а прийняття рішення щодо спільного блоку моделюється за допомогою цілей, стратегій або ігрових абстракцій.

Наприклад, [21] використовує загальний підхід Reinforcement Learning (RL) для виявлення атак на різні системи блокчейнів за допомогою симуляції на основі RL і стратегічного пошуку, водночас досить обмежений процесами створення блоків у блокчейнах PoW. Мета подібна до [5], тобто виявлення векторів атак і слабких місць у блокчейні. Хоча цей пошук є експериментальним, на відміну від аналітичного, він здатний зрозуміти деякі багатоагентні взаємодії та обмеження, що виникають через багато різнорідних агентів, кожен з яких має певну мету. Інший приклад: [20] фокусується на метаагентах, тобто агентах, які діють на кілька гіперпараметрів блокчейну, щоб збалансувати компроміс між безпекою та пропускною здатністю. Це спосіб оптимізації продуктивності блокчейну, що зберігає безпеку й надійність системи через RL.

Висновки

Моделі забезпечують абстракції, які використовують для представлення та передавання важливої інформації, без зайвих деталей, і допомагають впоратися зі складністю досліджуваної проблеми або розробленого рішення. Отже, вкрай важливо використовувати оптимальний підхід до моделювання. Беручи до уваги попередні дослідження, можна побачити, що всі розглянуті підходи до моделювання блокчейну розроблено з метою детального моделювання конкретних аспектів та/або задач, розв'язуваних за допомогою застосування блокчейну (наприклад, цільові дослідження топології мережі, як правило, використовують парадигму теорії графів), що, своєю чергою, робить їх досить специфічними й унеможливлює загальне застосування.

З усіх розглянутих методів моделювання можна виділити агентно-орієнтований як найбільш перспективний з погляду його універсальності та близькості парадигми мультиагентних систем до структури блокчейну. Враховуючи всі попередньо наголошені особливості, наступним логічним

кроком у моделюванні блокчейну можна назвати визначення загального способу моделювання блокчейну шляхом зміщення акценту в агентно-орієнтованому підході рівнем вище — з внутрішніх деталей на структурні та організаційні особливості. Пропонується розглянути так званий організаційно-орієнтований підхід для моделювання технології блокчейну з усіма її особливостями, який мав би логічно доповнити та, ймовірно, поліпшити раніше розглянуті досягнення з моделювання технології блокчейну.

Список літератури

1. Alharby M. BlockSim: An Extensible Simulation Tool for Blockchain Systems / Maher Alharby, Aad van Moorsel // Frontiers in Blockchain. — 2020. — Vol. 3. — https://doi.org/10.3389/fbloc.2020.00028.
2. Buchman E. The latest gossip on BFT consensus / E. Buchman, J. Kwon, Z. Milosevic. — 2018. — https://doi.org/10.48550/arXiv.1807.04938.
3. Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform [Electronic resource] / V. Buterin. — 2014. — Mode of access: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (date of access: 22.07.2024). — Title from screen.
4. Cachin C. Introduction to Reliable and Secure Distributed Programming / C. Cachin. — 2nd ed. — New York, NY, USA : Springer Publishing Company, Incorporated, 2011. — 386 p.
5. Eyal I. Majority is not enough: Bitcoin mining is vulnerable / I. Eyal, E. G. Sirer // International Conference on Financial Cryptography and Data Security, Christ Church, 3–7 March 2014. — [S. l.], 2014. — https://doi.org/10.48550/arXiv.1311.0243.
6. Ferber J. Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence / J. Ferber. — Boston, MA, USA : Addison-Wesley Reading, 1999. — 509 p.
7. Goodman L. M. Tezos–A Self-Amending Crypto-Ledger White Paper [Electronic resource] / L. M. Goodman. — 2014. — Mode of access: https://www.tezos.com/static/papers/whitepaper.pdf (date of access: 22.07.2024). — Title from screen.
8. Gürcan Ö. Multi-Agent Modelling of Fairness for Users and Miners in Blockchains / Önder Gürcan // Communications in Computer and Information Science. — Cham, 2019. — Pp. 92–99. — https://doi.org/10.1007/978-3-030-24299-2_8.
9. Gürcan Ö. On Using Agent-based Modeling and Simulation for Studying Blockchain Systems / O. Gürcan // JFMS 2020–Les Journées Francophones de la Modélisation et de la Simulation–Convergences entre la Théorie de la Modélisation et la Simulation et les Systèmes Multi-Agents. — [S. l.], 2020. — https://doi.org/10.48550/arXiv.2405.01574.
10. Hyperledger fabric / Elli Androulaki [et al.] // EuroSys'18: Thirteenth EuroSys Conference 2018, Porto Portugal. — New York, NY, USA, 2018. — https://doi.org/10.1145/3190508.3190538.
11. Larman C. Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development / C. Larman. — 3rd ed. — Upper Saddle River, NJ, USA : Prentice Hall PTR, 2004. — 736 p.
12. Malcolm G. Sheaves, Objects, and Distributed Systems / Grant Malcolm // Electronic Notes in Theoretical Computer Science. — 2009. — Vol. 225. — Pp. 3–19. — https://doi.org/10.1016/j.entcs.2008.12.063.
13. Marchesi L. ABCDE – agile block chain DApp engineering / Lodovica Marchesi, Michele Marchesi, Roberto Tonelli // Blockchain: Research and Applications. — 2020. – Vol. 1, no. 1–2. — Pp. 100002. — https://doi.org/10.1016/j.bcra.2020.100002.
14. Meldman-Floch W. Blockchain Cohomology / W. Meldman-Floch. — [S. l.], 2018. — https://doi.org/10.48550/arXiv.1805.07047.
15. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / S. Nakamoto // SSRN Electronic Journal. — 2008. — https://doi.org/10.2139/ssrn.3440802.
16. Nowak T. Topology in Distributed Computing [Electronic resource] : Master's Thesis / T. Nowak. — Vienna, Austria, 2010. — Mode of access: https://publik.tuwien.ac.at/files/PubDat_194085.pdf (date of access: 22.07.2024). — Title from screen.
17. Sagar P. V. Sheaf Representation of an Information System / Pyla Vamsi Sagar, M. Phani Krishna Kishore // International Journal of Rough Sets and Data Analysis. — 2019. — Vol. 6, no. 2. — Pp. 73–83. — https://doi.org/10.4018/ijrsda.2019040106.
18. Sapirshtein A. Optimal selfish mining strategies in bitcoin / A. Sapirshtein, Y. Sompolinsky, A. Zohar // International Conference on Financial Cryptography and Data Security. — [S. l.], 2016. — https://doi.org/10.48550/arXiv.1507.06183.
19. Selfish Behavior in the Tezos Proof-of-Stake Protocol / M. Neuder [et al.]. — [S. l.], 2020. — https://doi.org/10.48550/arXiv.1912.02954.
20. SkyChain: A Deep Reinforcement Learning-Empowered Dynamic Blockchain Sharding System / Jianting Zhang [et al.] // ICPP '20: 49th International Conference on Parallel Processing, Edmonton AB Canada. — New York, NY, USA, 2020. — https://doi.org/10.1145/3404397.3404460.
21. SquirRL: Automating Attack Discovery on Blockchain Incentive Mechanisms with Deep Reinforcement Learning / C. Hou [et al.] // In Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, 21–24 February 2021. — [S. l.]. — https://doi.org/10.48550/arXiv.1912.01798.
22. Towards a Performance Evaluation of Private Blockchain Frameworks using a Realistic Workload / Marcela T. Oliveira [et al.] // 2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 19–21 February 2019. — [S. l.], 2019. — https://doi.org/10.1109/icin.2019.8685888.
23. Wolfram D. A Sheaf Semantics for FOOPS Expressions [Electronic resource] / D. Wolfram, J. Goguen // In Proceedings of the Object-Based Concurrent Computing, ECOOP'91 Workshop, Geneva, 15–16 July 1991. — [S. l.], 1991. — Mode of access: https://www.researchgate.net/publication/220842390_A_Sheaf_Semantics_for_FOOPS_Expressions (date of access: 22.07.2024). — Title from screen.
24. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger [Electronic resource] / Gavin Wood. — 2014. — Mode of access: http://cryptochainuni.com/wp-content/uploads/Ethereum-A-Secure-Decentralised-Generalised-Transaction-Ledger-Yellow-Paper.pdf (date of access: 22.07.2024). — Title from screen.
25. Wooldridge M. An Introduction to MultiAgent Systems / M. Wooldridge. — 2nd ed. — Hoboken, NJ, USA : John Wiley & Sons, 2009. — 488 p.

References

Alharby, M., & van Moorsel, A. (2020). BlockSim: An extensible simulation tool for blockchain systems. *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.00028.

Androulaki, E., et al. (2018). *Hyperledger fabric*. EuroSys '18: Thirteenth EuroSys Conference, Porto, Portugal. https://doi.org/10.1145/3190508.3190538.

Buchman, E., Kwon, J., & Milosevic, Z. (2018). *The latest gossip on BFT consensus*. arXiv. https://doi.org/10.48550/arXiv.1807.04938.

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. [White paper]. https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

Cachin, C. (2011). *Introduction to Reliable and Secure Distributed Programming* (2nd ed.). Springer Publishing Company.

Eyal, I., & Sirer, E. G. (2014). *Majority is not enough: Bitcoin mining is vulnerable.* International Conference on Financial Cryptography and Data Security, Christ Church. https://doi.org/10.48550/arXiv.1311.0243.

Ferber, J. (1999). *Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence*. Addison-Wesley Reading.

Goodman, L. M. (2014). *Tezos–A self-amending crypto-ledger white paper*. https://www.tezos.com/static/papers/whitepaper.pdf.

Gürcan, Ö. (2019). Multi-agent modelling of fairness for users and miners in blockchains. *Communications in Computer and Information Science*, *92–99*. https://doi.org/10.1007/978-3-030-24299-2_8.

Gürcan, Ö. (2020). *On using agent-based modeling and simulation for studying blockchain systems*. JFMS 2020 — Les Journées Francophones de la Modélisation et de la Simulation. https://doi.org/10.48550/arXiv.2405.01574.

Hou, C., et al. (2021). *SquirRL: Automating attack discovery on blockchain incentive mechanisms with deep reinforcement learning*. Proceedings of the Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.48550/arXiv.1912.01798.

Larman, C. (2004). *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development* (3rd ed.). Prentice Hall PTR.

Malcolm, G. (2009). Sheaves, objects, and distributed systems. *Electronic Notes in Theoretical Computer Science*, *225*, 3–19. https://doi.org/10.1016/j.entcs.2008.12.063.

Marchesi, L., Marchesi, M., & Tonelli, R. (2020). ABCDE — Agile blockchain DApp engineering. *Blockchain: Research and Applications*, *1* (1–2), 100002. https://doi.org/10.1016/j.bcra.2020.100002.

Meldman-Floch, W. (2018). *Blockchain cohomology*. arXiv. https://doi.org/10.48550/arXiv.1805.07047.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3440802.

Neuder, M., et al. (2020). *Selfish behavior in the Tezos proof-of-stake protocol*. arXiv. https://doi.org/10.48550/arXiv.1912.02954.

Nowak, T. (2010). *Topology in distributed computing*. [Master's thesis]. Vienna, Austria. https://publik.tuwien.ac.at/files/PubDat_194085.pdf.

Sagar, P. V., & Kishore, M. P. K. (2019). Sheaf representation of an information system. *International Journal of Rough Sets and Data Analysis*, *6* (2), 73–83. https://doi.org/10.4018/ijrsda.2019040106.

Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016). *Optimal selfish mining strategies in bitcoin*. International Conference on Financial Cryptography and Data Security. https://doi.org/10.48550/arXiv.1507.06183.

Oliveira, M. T., et al. (2019). *Towards a performance evaluation of private blockchain frameworks using a realistic workload*. 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France. https://doi.org/10.1109/icin.2019.8685888.

Wolfram, D., & Goguen, J. (1991). *A sheaf semantics for FOOPS expressions*. Proceedings of the Object-Based Concurrent Computing, ECOOP'91 Workshop, Geneva. https://www.researchgate.net/publication/220842390_A_Sheaf_Semantics_for_FOOPS_Expressions.

Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. [White paper]. http://cryptochainuni.com/wp-content/uploads/Ethereum-A-Secure-Decentralised-Generalised-Transaction-Ledger-Yellow-Paper.pdf.

Wooldridge, M. (2009). *An Introduction to MultiAgent Systems* (2nd ed.). John Wiley & Sons.

Zhang, J., et al. (2020). *SkyChain: A deep reinforcement learning-empowered dynamic blockchain sharding system*. ICPP '20: 49th International Conference on Parallel Processing, Edmonton, AB, Canada. https://doi.org/10.1145/3404397.3404460.

M. Yeshchenko

MODELING BLOCKCHAIN TECHNOLOGY

Blockchain is a very attractive technology because it provides a public, append-only, immutable, and ordered transaction log. Blockchain systems are inherently interdisciplinary as they combine different fields such as cryptography, multi-agent systems, distributed systems, social systems, economics, and finance. Additionally, they have a highly active and dynamic ecosystem where new blockchain platforms and algorithms are constantly being developed due to public and industry interest in the technology. Given the complexity and multifaceted nature of the blockchain, its presentation – modeling – via other, more well-known means should contribute to a better understanding of the capabilities and features of this technology.

First, the peculiarities and challenges of blockchain modeling are considered, which are mainly based on blockchain data structure, transactions, and consensus mechanism usage.

Later, a comparative analysis of four different modeling paradigms is carried out. The process-oriented approach is discussed first and provides an understanding of how blockchain nodes may be represented by components, while their behavior may be constructed as an algorithm executed by individual components. The graph-theoretic paradigm offers a more visual representation of the subject matter while providing

distributed algorithm capabilities. The object-oriented way of modeling offers more convenient encapsulation possibilities, as well as a well-adopted UML-based graphical accompaniment of the hierarchy and links between modeled blockchain nodes. Finally, the agent-oriented approach provides possibly the best overall approach to modeling blockchain technology by offering an object capable of representing the flexible behavioral nature of blockchain nodes, an agent, while continuing to allow a visual depiction of the modeled entity.

This article aims to explore the main methods of modeling blockchain technology and to determine the most promising one for further in-depth research into the possibilities of modeling all aspects of blockchain technology in the most efficient manner. As part of it, it was confirmed that agent-oriented approach to blockchain modeling is the most suitable one. Even more specifically, the organization-oriented approach, as a subdivision of the agent-oriented approach, is advised for experimentation to potentially provide a new perspective on blockchain technology representation with the help of multi-agent systems.

Keywords: blockchain, multi-agent systems, modeling.

Матеріал надійшов 22.07.2024