ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

**ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

Logo, company name

Description automatically generated

**BÁO CÁO NGHIÊN CỨU KHOA HỌC SINH VIÊN**

**HƯỚNG TỚI KHẢ NĂNG TƯƠNG TÁC LIÊN CHUỖI SỬ DỤNG CHUỖI KHỐI NGOÀI VÀ KIỂM SOÁT TRUY CẬP DỮ LIỆU BẰNG KHOÁ CÓ THỜI HẠN**

Enhancing Blockchain Interoperability through **Sidechain** Integration and Valid-Time-KeyData Access Control

**Giáo viên hướng dẫn: Th.S Trần Tuấn Dũng**

**Sinh viên thực hiện: Võ Anh Kiệt – 20520605**

**Nguyễn Bùi Kim Ngân – 20520648**

**Nguyễn Bình Thục Trâm – 20520815**

**Lớp: ATTN.2020**

**Thành phố Hồ Chí Minh, tháng 6 năm 2023**

**MỤC LỤC**

[LỜI CẢM ƠN 3](#_Toc138365059)

[NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN 4](#_Toc138365060)

[DANH MỤC HÌNH ẢNH 6](#_Toc138365061)

[DANH MỤC BẢNG 7](#_Toc138365062)

[DANH MỤC VIẾT TẮT VÀ GIẢI NGHĨA 8](#_Toc138365063)

[CHƯƠNG I: TỔNG QUAN ĐỀ TÀI 9](#_Toc138365064)

[1.1. Ngữ cảnh 9](#_Toc138365065)

[1.2. Hướng giải quyết đề tài 10](#_Toc138365066)

[CHƯƠNG II: CƠ SỞ LÝ THUYẾT 12](#_Toc138365067)

[2.1. Tổng quan các phương pháp 12](#_Toc138365068)

[2.2. Phương pháp Notary 13](#_Toc138365069)

[2.3. Phương pháp Hash-locking 14](#_Toc138365070)

[2.4. Phương pháp Relays/Chuỗi khối ngoài 16](#_Toc138365071)

[2.5. Chuỗi khối Oracle 17](#_Toc138365072)

[CHƯƠNG III: ĐỀ XUẤT HỆ THỐNG 20](#_Toc138365073)

[3.1. Tổng quan 20](#_Toc138365074)

[3.2. Đề xuất hệ thống chuỗi khối 20](#_Toc138365075)

[3.2.1. Mô hình chung 20](#_Toc138365076)

[3.2.2. Giải pháp chuỗi khối riêng 21](#_Toc138365077)

[3.2.3. Chuỗi khối ngoài 24](#_Toc138365078)

[3.2.4. Ứng dụng phi tập trung 25](#_Toc138365079)

[3.2.5. Truyền dữ liệu 27](#_Toc138365080)

[3.3. Đề xuất các giải pháp hỗ trợ 30](#_Toc138365081)

[3.3.1. Lưu trữ EMR 30](#_Toc138365082)

[3.3.2. Khoá có thời hạn 30](#_Toc138365083)

[CHƯƠNG IV: KỊCH BẢN THỰC NGHIỆM 33](#_Toc138365084)

[4.1. Đánh giá hiệu suất 33](#_Toc138365085)

[4.2. Phân tích bảo mật 39](#_Toc138365086)

[CHƯƠNG V: KẾT LUẬN 41](#_Toc138365087)

[TÀI LIỆU THAM KHẢO 42](#_Toc138365088)

TÓM TẮT ĐỀ TÀI (ABSTRACT)

xxxxxxxxxxxxxxx

NỘI DUNG ĐỀ TÀI

1. Tóm tắt các công trình liên quan

Xxxxxxxxxx

1. Tính khoa học, tính mới

Xxxxxxxxxxxxx

MỤC TIÊU PHƯƠNG PHÁP

1. Mục tiêu công trình

xxxxxxx

1. Tổng quan giải pháp

xxxxxxxxxxxxx

1. Hệ thống liên chuỗi khối

xxxxxxxxxx

1. Hệ thống khoá có thời hạn

xxxxxxxxxxxxxxxx

KẾT QUẢ - THẢO LUẬN

1. Môi trường

Xxxxxxxxxxxxxxx

1. Kết quả

xxxxxxxxxxxx

KẾT LUẬN VÀ ĐỀ NGHỊ

xxxxxxxxxxxxx

TÀI LIỆU PHỤ LỤC

DANH MỤC HÌNH ẢNH

[Hình 1 Sự khác biệt giữa các kiến trúc chuỗi khối. 9](#_Toc138549309)

[Hình 2 Mô hình giao tiếp liên chuỗi 11](#_Toc138549310)

[Hình 3 Mô phỏng chuỗi chéo 12](#_Toc138549311)

[Hình 4 Mô phỏng phương pháp Notary Blockchain Interoperability 13](#_Toc138549312)

[Hình 5 Mô phỏng phương pháp Hash - locking 15](#_Toc138549313)

[Hình 6 Mô phỏng phương pháp Relays/Sidechain 16](#_Toc138549314)

[Hình 7 Tổng quan về framework của Polkadot 17](#_Toc138549315)

[Hình 8 Triển khai Cosmos sử dụng giao thức IBC để giao tiếp liên chuỗi 17](#_Toc138549316)

[Hình 9 Sự thiếu kết nối của dữ liệu và sự kiện với Blockchains 18](#_Toc138549317)

[Hình 10 Cách hoạt động của chuỗi khối Oracles 19](#_Toc138549318)

[Hình 11 Mô hình tổng quan của hệ thống 21](#_Toc138549319)

[Hình 12 Mạng Quorum cung cấp khả năng phần quyền các nút 22](#_Toc138549320)

[Hình 13 Vai trò các thực thể trong mạng chuỗi khối 23](#_Toc138549321)

[Hình 14 Mạng chuỗi khối Ethereum 24](#_Toc138549322)

[Hình 15 Tương tác giữa hai chuỗi khối sử dụng nút Oracle 25](#_Toc138549323)

[Hình 16 Ứng dụng phi tập trung cơ bản 26](#_Toc138549324)

[Hình 17 Các phiên bản DApp dành cho các thực thể 27](#_Toc138549325)

[Hình 18 Quy trình trao đổi dữ liệu liên chuỗi 28](#_Toc138549326)

[Hình 19 Thuật toán xác thực tính toàn vẹn dữ liệu của EMR 29](#_Toc138549327)

[Hình 20 Phương án lưu trữ sử dụng Cloud kết hợp với Blockchain 30](#_Toc138549328)

[Hình 21 Quy trình cấp quyền cho người dùng quyền thấp 31](#_Toc138549329)

[Hình 22 Thuật toán kiểm soát truy cập EMR 32](#_Toc138549330)

[Hình 23 Mạng Sepolia Ethereum 33](#_Toc138549331)

[Hình 24 Mạng Quorum 34](#_Toc138549332)

[Hình 25 Mạng Quorum 34](#_Toc138549333)

[Hình 26 Hệ thống Sidechain 35](#_Toc138549334)

[Hình 27 Smart contract 1 35](#_Toc138549335)

[Hình 28 Smart contract 2 36](#_Toc138549336)

[Hình 29 Smart contract 3 36](#_Toc138549337)

[Hình 30 Deploy smart contract 37](#_Toc138549338)

[Hình 31 Thông tin các Transaction 37](#_Toc138549339)

DANH MỤC BẢNG

Bảng 1 Môi trường thực nghiệm 33

Bảng 2 Kết quả thực nghiệm về mặt thời gian 38

Bảng 3 Kết quả thực nghiệm về mặt hiệu năng và chi phí 39

DANH MỤC VIẾT TẮT VÀ GIẢI NGHĨA

|  |  |
| --- | --- |
| EMR – Electrical medical records | Hồ sơ bệnh án điện tử |
| Blockchain | Chuỗi khối |
| Public Blockchain | Chuỗi khối ngoài |
| Private Blockchain | Chuỗi khối riêng |
| Sidechain | Hệ thống chuỗi khối ngoài |
| VTK – Valid time key | Khoá có thời hạn |
| Off-chain | Ngoài chuỗi khối |
| On-chain | Trên chuỗi khối |
| DON – Decentralized oracle networks | Các mạng phi tập trung |
| Full Node | Nút đầy đủ |
| Light Node | Nút nhẹ |

TÀI LIỆU THAM KHẢO

1. M. Rauchs, A. Blandin, K. Bear, and S. B. McKeon, “2nd global enterprise blockchain benchmarking study,” Available at SSRN 3461765, 2019.
2. Y. Pang, “A new consensus protocol for blockchain interoperability architecture,” IEEE Access, vol. 8, pp. 153 719–153 730, 2020.
3. S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, “Interoperability and synchronization management of blockchain-based decentralized e-health systems,” IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1363–1376, 2020.
4. T. Hardjono, A. Lipton, and A. Pentland, “Toward an interoperability architecture for blockchain autonomous systems,” IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1298–1309, 2019.12 T.D. Tran et al.
5. Roehrs, C. A. Da Costa, and R. da Rosa Righi, “Omniphr: A distributed architectureb model to integrate personal health records,” Journal of biomedical informatics, vol. 71, pp. 70–81, 2017.
6. N. Spence, M. Niharika Bhardwaj, and D. P. Paul III, “Ransomware in healthcare facilities: A harbinger of the future?” Perspectives in Health Information Management, pp. 1–22, 2018.
7. N. Thamer and R. Alubady, “A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,” in 2021 1st BICITS, IEEE, 2021, pp. 210–216.
8. M.-H. Kuo et al., “Opportunities and challenges of cloud computing to improve health care services,” Journal of medical Internet research, vol. 13, no. 3, e1867, 2011.
9. S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, “Towards blockchain interoperability,” in Business Process Management: BPM 2019 Blockchain and CEE Forum, Vienna, Austria, Proceedings 17, Springer, 2019, pp. 3–10.
10. R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, “A survey on blockchain interoperability: Past, present, and future trends,” ACM Computing Surveys (CSUR), vol. 54, no. 8, pp. 1–41, 2021.
11. V. Buterin, “R3 report-chain interoperability,” R3 Res, 2016.
12. Z. Wang, J. Li, X.-B. Chen, and C. Li, “A secure cross-chain transaction model based on quantum multi-signature,” Quantum Information Processing, vol. 21, no. 8, p. 279, 2022.
13. Monika, R. Bhatia, A. Jain, and B. Singh, “Hash time locked contract based asset exchange solution for probabilistic public blockchains,” Cluster Computing, vol. 25, no. 6, pp. 4189–4201, 2022.
14. R. Bhatia, A. Jain, and B. Singh, “Hash time locked contract based asset exchange solution for probabilistic public blockchains,” Cluster Computing, vol. 25, no. 6, pp. 4189–4201, 2022.
15. J. Kwon and E. Buchman, “Cosmos whitepaper,” A Netw. Distrib. Ledgers, p. 27, 2019.
16. G. Wood, “Polkadot: Vision for a heterogeneous multi-chain framework,” White paper, vol. 21, no. 2327, p. 4662, 2016.
17. M. V. Baysal, O. ¨ Ozcan-Top, and A. Betin-Can, “Blockchain technology ¨ applications in the health domain: A multivocal literature review,” The Journal of supercomputing, vol. 79, no. 3, pp. 3112–3156, 2023.
18. Chainlink Documents: <https://docs.chain.link/>
19. Foley & Lardner LLP
20. TradaFX
21. ResearchGate
22. arshbot.medium.com
23. Hyperchain Documentations: <https://www.hyperchain.cn/>
24. Cosmos Documentations: <https://docs.cosmos.network/main>
25. Polkadot Documentations: <https://polkadot.network/development/docs/>
26. Stakin: <https://stakin.com/>
27. Chainstack: <https://chainstack.com/>
28. Shiksha: <https://www.shiksha.com/>
29. Moonbeam Documentationons: <https://docs.moonbeam.network/>
30. Horizen Academy: <https://www.horizen.io/academy/sidechains/>