IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, April 2024

Implementing Quantum Resistant Algorithm in Blockchain-Based Applications

Dr. Sonali Ridhorkar[1] and Mr. Setu Sagar Mishra[2]
Associate Professor, G H Raisoni Institute of Engineering & Technology, Nagpur, India[1]
Student, G H Raisoni Institute of Engineering & Technology, Nagpur, India[2]

Abstract: *With quantum computing evolving very fast as we speak, the security and integrity of blockchain-based applications will become the most crucial aspect. A proposal is raised to use blockchain technology as a platform for writing and probating 'wills'. Blockchain technology in drafting and probating wills makes them safe from manipulations, highly secure, and transparent. It also dramatically decreases the time required without catering for the challenges created by the current system. [9] This paper presents a new method for will transfer and inheritance management by implementing quantum-resistant algorithms in the security architecture of a blockchain decentralized application (DApp). The system uses IPFS Network for data storage and quantum-safe algorithms as retrieval and sending algorithms. The system includes Quantum-Resistant Dilithium Signatures and Merkle trees as the fundamental components for safeguarding the transfers of assets and claims for inheritance. Quantum-Resistant Dilithium Signatures offer an unbreakable shield against quantum attacks that are expected to happen, which in turn safeguards the privacy and authenticity of transactions. While Merkle trees are responsible for the organization of inheritance claims in an effective and tamper-proof manner, the introduced system incorporates smart contracts to address the execution of an inheritance case, adding more security and automation to the asset distribution process. The system ensures a robust security framework by integrating quantum-resistant algorithms at the very core of the blockchain DApp for instance, retrieval and sending. This research is of great significance to blockchain technology which is the emerging technology of the future because it addresses the existing threat of quantum computing by showing the feasibility of using quantum-resistant algorithms in practical applications. As established by the findings, besides Quantum-Resistant Dilithium Signatures and Merkle trees, the systems of asset transfers and inheritance management within blockchain networks are enhanced in terms of safety and reliability. Hence, paving the road to the creation of more secure and trustworthy digital asset management systems.*

Keywords: Blockchain, quantum computers, quantum-resistant algorithms, decentralized inheritance systems, Merkle trees, InterPlanetary File System (IPFS), Dilithium Signatures, blockchain DApps

REFERENCES

[1]. C. -Y. Li, X. -B. Chen, Y. -L. Chen, Y. -Y. Hou and J. Li, "A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network," in IEEE Access, vol. 7, pp. 2026-2033, 2019, doi: 10.1109/ACCESS.2018.2886554.

[2]. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[3]. Zhwan Mohammed Khalid & Shavan Askar, 2021. "Resistant Blockchain Cryptography to Quantum Computing Attacks" International Journal of Science and Business, IJSAB International, vol. 5(3), pages 116-125.

[4]. Peijun Zhang, Lianhai Wang, Wei Wang, Kunlun Fu, Jinpeng Wang, "A Blockchain System Based on Quantum-Resistant Digital Signature", Security and Communication Networks, vol. 2021, Article ID 6671648, 13 pages, 2021.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, April 2024

[5]. Allende, M., León, D.L., Creon, S. et al. "Quantum-resistance in blockchain networks." Sci Rep 13, 5664 (2023).

[6]. Thanalakshmi, P.; Rishikhesh, A.; Marion Marceline, J.; Joshi, G.P.; Cho, W. "A Quantum-Resistant Blockchain System: A Comparative Analysis. " Mathematics 2023, 11, 3947.

[7]. Izuhara, M., & Köppe, S. (2019). Inheritance and family conflicts: exploring asset transfers shaping intergenerational relations. *Families, Relationships and Societies*, *8*(1), 53-72. Retrieved Apr 29, 2024, from https://doi.org/10.1332/204674317X14908575604683

[8]. Chen, C.-L.; Lin, C.-Y.; Chiang, M.-L.; Deng, Y.-Y.; Chen, P.; Chiu, Y.-J. A Traceable Online Will System Based on Blockchain and Smart Contract Technology. *Symmetry* **2021**, *13*, 466. https://doi.org/10.3390/sym13030466

[9]. P. Sreehari, M. Nandakishore, G. Krishna, J. Jacob and V. S. Shibu, "Smart will converting the legal testament into a smart contract," 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvananthapuram, India, 2017, pp. 203-207, doi: 10.1109/NETACT.2017.8076767.

[10]. Dondjio, I., Kazamias, A. (2024). A Blockchain Framework for Digital Asset Ownership and Transfer in Succession. In: Papadaki, M., Themistocleous, M., Al Marri, K., Al Zarouni, M. (eds) Information Systems. EMCIS 2023. Lecture Notes in Business Information Processing, vol 501. Springer, Cham. https://doi.org/10.1007/978-3-031-56478-9_7

[11]. Yang, L. Tan, N. Shi, B. Xu, Y. Cao and K. Yu, "AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud," in IEEE Access, vol. 8, pp. 70604-70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[12]. Truc Nguyen & Tre' R. Jeter & My T. Thai, 2022. "Advances in Blockchain Security," Springer Optimization and Its Applications, in: Duc A. Tran & My T. Thai & Bhaskar Krishnamachari (ed.), Handbook on Blockchain, pages 363-387, Springer.

[13]. Yihang Fu & Zesen Zhuang & Luyao Zhang, 2022. "AI Ethics on Blockchain: Topic Analysis on Twitter Data for Blockchain Security," Papers 2212.06951, arXiv.org, revised Jul 2023.

[14]. Manoj Athreya, A., et al. "Peer-to-peer distributed storage using InterPlanetary file system." *International Conference on Artificial Intelligence and Data Engineering*. Singapore: Springer Nature Singapore, 2019.

[15]. Lu Meng & Zeyao Liu, 2023. "Blockchain Security Mechanism Design Based on Chinese Cryptosystem SM2 Algorithm," Mathematics, MDPI, vol. 11(14), pages 1-13, July.