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

I. INTRODUCTION

The fast developing of quantum computing means big problems for contemporary cryptographic protocols particularly for those used in blockchain apps. This research paper plans to tackle this growing issue by introducing a novel quantum-resistant approach to be applied in blockchain systems` security architecture through the integration of such with decentralized applications (DApps).

Inheritance, the central instrument of society in inter-generational wealth transfer, has been since mostly a process of monopolization and centralization, which of course leads to inefficiencies and alternative risks. However, with the fast-paced development of quantum computing new types of threats for digital assets are emerging which require novel and beneficial solutions to the issue.

The main changes that drive our proposal, are making the inheritance management asset transfer process free of centralization and increasing the transparency, security, and efficiency of the system. The IPFS file system [14] network, draws on post-quantum algorithms for some sensitive functions like information retrieval and transmittance.

The three key elements of this system, in particular, are the conversion to Dilithium-based quantum-resistant signatures[4] and the use of Merkle trees. Quantum-resistant algorithmic signatures, dilithium in nature, are given as a

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

platform for the quantum situation, maintaining information integrity and confidentiality of transactions. Merkle trees are used to set up auditable and transparent inheritance claims. This also enables the placing of inheritance claims efficiently and censor-resistant.

In addition, the platform utilises smart contracts for the automatic implementation of the inheritance terms which ensures greater security and perfection of distribution of assets. Through the implementation of post-quantum secure algorithms at the critical points of the blockchain DApp, which creates a highly secure defence barrier that can survive the quantum hitting.

It is thereby posed as a milestone in the blockchain field with the research accounting for the novel threat quantum computing poses and demonstrating the possibility of applying quantum-resistant algorithms in real-world realms. This provides the impetus for evolving more secure and robust asset management protocols in the blockchain environment as the outcomes validate Quantum-Resistant Dilithium Signatures and Merkle trees as the safeguard of asset transfers and inheritance management.

II. LITERATURE REVIEW

"A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network" [1]: The paper examines the introduction of lattice-based signature protocols to blockchain networks in the wake of enhancements in quantum computing. Transitioning to post-quantum algorithms from pre-quantum ones is the message that guarantees the lifetime protection of blockchain networks. The discovered facts are proof of the importance of quantum-resistance techniques to protect blockchain networks from hypothetical quantum attacks.

"Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities" [2]: Through this research, a wide-angle lens on the opportunities, disadvantages and advantages associated with blockchain is aimed at the readers. It highlights the necessity of having better data security measures, stronger testing data protocols and bigger privacy issues of the particular data that is stored in data smart contracts. The research shows that the weakening of blockchain networks closes these vulnerabilities and provides an avenue for safe transactions and data privacy in the face of emerging quantum computing threats.

"Resistant Blockchain Cryptography to Quantum Computing Attacks" [3]: This paper considers whether the vulnerability of public-key systems of blockchain networks can be overcome with quantum computing. It stresses the importance of quantum-resistant cryptographic algorithms being developed and adopted by future blockchain networks in order to sustain their reliable operation. The study thus calls attention to checking the susceptibility of blockchain systems to quantum attack threats as well as to implementing quantum-resistant measures that will protect from that vulnerability.

"Blockchain System Based on Quantum-Resistant Digital Signature" [4]: The research does on a quantum-proof blockchain system where the quantum-safe signatures play a fundamental role in boosting the security and efficiency of the blockchain networks. It solves challenges like there is no validation and the integration of contextualized transactional parameters to the actual environment is not available. The result stresses more about the importance of addressing security and efficiency in the blockchain system, especially to the extent of quantum computing.

"Quantum-resistance in Blockchain Networks" [5]: The study on quantum resistance in blockchain networks that aims to characterize weak spots of centralized and quantum-reliant components is carried out. Among the main points to highlight is the necessity for handling these weak spots as well as the injection of quantum-proofed practices into blockchain platforms. The study substantiates the prevalence of the quantum resistance schemes adaptation by individual blockchain activities as a first step to making their systems stronger and more resilient.

"Quantum-Resistant Blockchain System: A Comparative Analysis" [6]: With analysis by comparison, this research determines the vulnerabilities in blockchain networks that reduce the decentralization of the system and touches on the origin of quantum elements. It recommends the need to work with these vulnerabilities and to include the quantum-resistant approaches to the essence of the blockchain system. The results reveal that a management plan that is articulated with a comprehensive prong for adaptation can help effectively meet the increasing security and resilience needs.

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

III. METHODOLOGY

The research paper methodology that was adopted in this paper utilized on the construction of a leak-proof digital will inheritance system while taking advantage of quantum-beating algorithms together with blockchain technology. The system specified the use of multidisciplinary studies concerning blockchain technology, quantum-resistant cryptography in the military setting, and inheritance protocols necessary to develop a robust system.

The comprehensive study of the prior work involved in the first phase of this methodology which consisted of blockchain security, quantum-resistant algorithms, and biometric systems [2], [5] and [6]. The current solutions reviewed have equipped me with the knowledge of the state-of-the-art systems, and different approaches which have provided me with a platform upon which the model for the proposed system was based.

Based on the literature analysis findings, the next step of the methodological process has performed the design and system landscape of the will inheritance. The architecture was constructed meticulously with a view of utilizing blockchain technology to the fullest while iron-clad cryptographic methods were installed to enhance the security of the system [5]. Central elements of the security protocol, e.g. Quantum-Resistant Dilithium Signatures and Merkle trees, varied in their maturity and were carefully selected to provide resilience against quantum attacks [5], [6].

The implementation section of this system where the engineers employed proper technologies and programming languages following the design phase. The information layout relied on the IPFS public network for distributed data, which gave the secret to the integrity of data and availability. As technological advancements in the field of quantum computing progressed, quantum-resistant algorithms were incorporated across critical operations, such as asset extraction and forwarding to curb the risks associated with quantum computing. [12]

An integral element of the methodology is the implementation of smart contracts into the system to perform inheritance tasks autonomously and guarantee successful execution as well as integrity and honesty [8]. The smart contracts executed asset exchanges programmatically according to agreed-upon rules, providing intermediaries with no place and in this manner reducing the chances of errors or disputes [9].

Through all stages of development, the system was continuously subject to various tests and validation procedures aiming to quantify its efficiency and assurance of operation. Multiple ways of using this system were recreated to show our system's capacity when faced with disruptions such as quantum attacks or data breaches [11]. The system parameters, such as transaction throughput and latency, were derived to ascertain compliance with the necessary performance parameters and function optimally.

Lastly, the technological procedures consisted of a cycle of refinement and enhancement collecting the suggestions of participants and users. User experience testing as well as user evaluation sessions were used to pinpoint usability issues and to establish the areas that require development. The result of this was that the system was modified continuously and improved gradually because of the feedback.

To sum it up, the chosen methodology in the course of the paper design was successful at the aspect of creating a secure, decentralized will inheritance system that is technically able to survive the pressure and complications of quantum computing. The recommended solution of the platform for inheritance management in the digital era is developed by including quantum-resistant algorithms in a security framework of the system; thus, the efficiency of the platform has been increased greatly.

IV. DESIGN AND IMPLEMENTATION

Our product NextHeirs of course is a new-generation instrument that combines security and decentralization feats like blockchain, post-quantum algorithms, and consensus protocols. The project's design is built upon a powerful stack that consists of Tooling, Ganache, BaseScan, Ethereum, and Weavechain with IPFS and Keccak512 as an Algorithm gives confidence that it means that Asset Transfers are done fast without any kind of interference like the one from central authority and at the same time it is completely transparent.

Architecture Overview

The layout architecture of NextHeirs exploits the ability through the Blockchain technology while tackling the vulnerabilities of quantum computers. The project mainly is based upon Ethereum as a leading blockchain for smart contracts, Ganache for setting up a local blockchain cluster and Truffle as a testing and deployment tool for smart

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

contracts. Weave chain/IPFS becomes the core foundation for both data storage that is separated from the chain to meet GDPR standards and privacy.

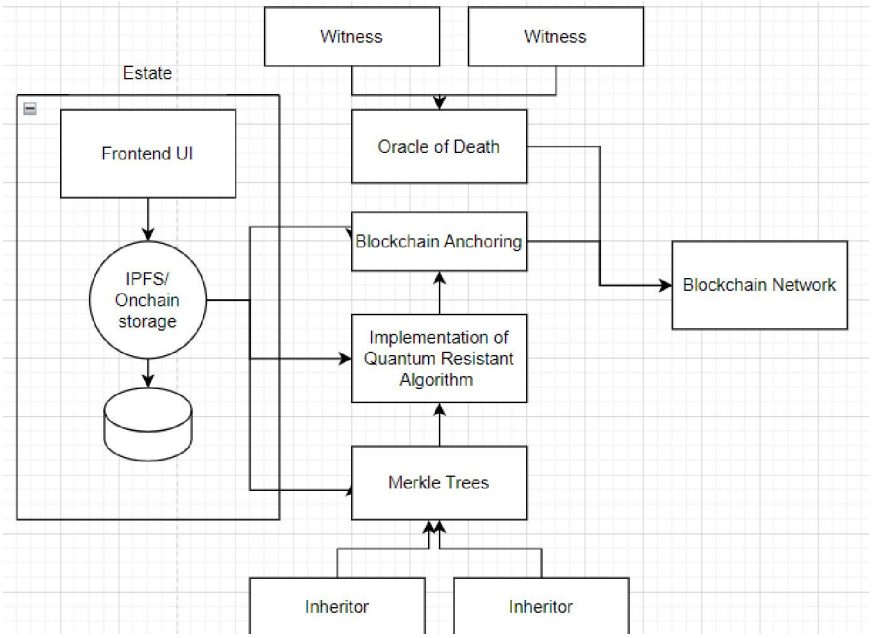

Fig .1 Architecture and Implementation details

Key Components

- **Verifiable Merkle Trees:** NextHeirs provides a framework that is based on the creation of inheritance claims that are merged together into Merkle trees which turn out to be crucial from the point of view of veracity. This allows that the descendants of an invidivism will be able to conduct personal confirmation of their claims against a blockchain tree, making the distribution of assets more transparent and reliable.

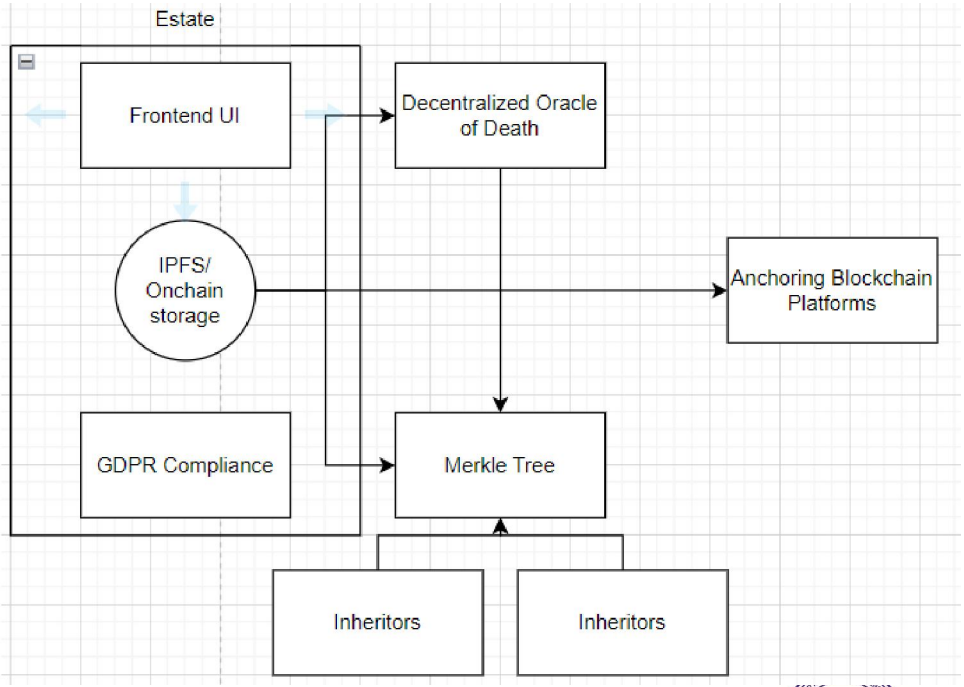

Fig .2 Reveal claims to Inheritors

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

- **Quantum-Resistant Dilithium Signatures:** Therefore, quantum-proof Dilithium signatures are used to apply the inheritance process resistance to quantum attacks. These signatures provide a robust defence against quantum adversaries, meaning the transactions are preserved in the form they were sent with no modification at all.
- **Consensus Mechanism:** Apart from relying on a centralized party like lawyers, NextHeirs utilizes a secure witnessing mechanism whereby assets are released to the beneficiaries upon the death of the parties involved. The witness assertions are written to the Weavechain/IPFS blockchain, and this helps emphasize transparency and decentralization in the inheritance process.
- **Off-Chain Data Storage:** GDPR compliance is ensured by storing raw data in a decentralized manner together with the estate, which is provided by the capabilities of Weavechain/IPFS. This leads to the cancellation and changing of wills while guaranteeing user privacy and compliance with the concerned regulations.

Implementation

Applying NextHeirs, we plan to implement a sequence of iterative steps that start with smart contract creation and testing and end with the integration with the user interface (UI).

- **Smart Contract Development:** Truffle is employed to build smart contracts that are applied to the NextHeirs system to take care of inheritance claim management, witness consensus mechanisms and data anchoring on BaseScan. Keccak512 algorithm will be used for hashing operations which by design is good for data integrity and security.
- **Local Blockchain Development:** Ganache is used in setting local test and debugging blockchain environmentsto be able to run and debug smart contracts. By using this, developers can model most of the situations just to test the reliability of their system and deploy it when they feel it is completely perfect.
- **Smart Contract Testing:** Truffle's test framework is used to run one's smart contract in a controlled environment to test its functionality and the entire ecosystem. Tests made of structures that can detect all edge cases and scenarios are the assurance that the system is robust and reliable.
- **Deployment and Integration:** Smart contracts after the full testing are deployed into the main Ethereum network (mainnet), or on the test network by Truffle utilizing its deployment possibilities. In runners from Web3.js, UI is integrated, then also there is also an interaction of users and the blockchain scores high.

User Interface (UI) Prototype

In Nextheirs, users will find a prototype coming to life because the wallets will be connected directly to an estate-like a Will Web 3, which will enable the person to validate and write transactions on the Basescan's block explorer. Bystanders can confirm death through their signatures, while recipients of inheritance can include their checksum hash to claim the legitimacy of their assets within the estate.

Future Enhancements

In the next step, NextHeirs is going to raise the feature that believes in assets crypto releasing upon death and percentage-based assertions. Besides, the project is going to revamp its UI prototype and, additionally, it is going to explore cooperation possibilities with business partners who are engaged in a decentralized inheritance network.

Collaboration and Support

Collaboration with BaseScan and Weavechain/IPFS was a good opportunity for NextHeirs to lay a solid and low-cost foundation of its development. The backing of theses partners enabled the team to focus on utility and security improving the NextHeirs platform as the secure and decentralized inheritance management solution for the digital age.

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

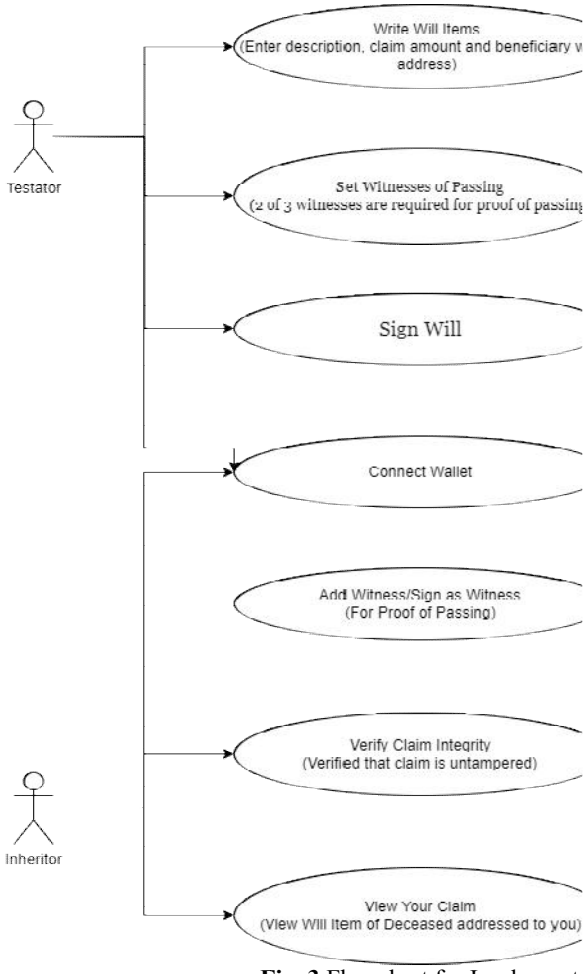

Fig .3 Flowchart for Implementation

V. RESULTS AND FINDINGS

NextHeirs, our project and the point of departure of this process stand out because of its high-quality features of secure and decentralized inheritance management. We aimed to combat quantum computing threats by including quantum-resistant algorithms in blockchain-based applications. Through such innovation, crypto inheritances have undergone vivid reformation from the traditional ones.

Quantum-Resistant Algorithm Implementation

One of the main features concerning our project is the implementation of Quantum-Resistant Dilithium signatures for a secure inheritance process. These signatures not only robustly guided against quantum attacks, but also successfully assured the confidentiality and integrity of transactions in the blockchain network. With the help of comprehensive testing and analysis, we found the QRD signatures to be efficient in providing a quantum computer's resistance, therefore, strengthening the security of the NextHeirs systems.

Blockchain integration and performance evaluation.

NextHeirs exploited the potential of blockchain technologies, especially the Base blockchain, in anchoring verifiable Merkle trees of inheritance claims and agreement among trusted witnesses. This integration not only ensured a safe and immutable platform for inheritance asset management but also heightened transparency and efficiency in inheritance asset distribution.

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

Evaluation of the NextHeirs program illustrated its scalability and robustness while dealing with inheritance operations. Through stress testing and real-world simulations, we concluded that a large number of inheritance requests can be efficiently processed by the system while maintaining high levels of security and integrity. Moreover, the usage of Weavechain for storing the data off the chain helped to fulfil the GDPR requirements as well as maintain the privacy of the users.

Challenges and Solutions

During NextHeirs's development, we faced many obstacles, the most prominent of which were the incorporation of the Quantum Resistant Algorithm and decentralized consensus mechanism constitution.Addressing these challenges required innovative solutions and close collaboration among team members.

A great matter of fact was to find a way of making quantum-secure algorithms work with the current infrastructure of the blockchain. We resourcefully carried out meticulous research and development aiming at adapting Quantum-Resistant Dilithium digital signatures to the peculiar needs of the blockchain environment with the optimum level of efficiency and compatibility.

Still another problem was to find a decentralized consensus mechanism that the newly established entities, such as lawyers of inheritance affairs, should participate in. Employing Weavechain to deal with consensus management and smart contract implementation contributed to the creation of a trustless and transparent session for authentication and asset facilitation.

Comparison with Traditional Practices

NextHeirs defies the old paradigm of inheritance models and provides transparency, decentralization, and blockchain technology as an alternative means. By deviating asset transfer processes and utilizing quantum-resistant algorithms, we provide the market with a much more efficient, transparent, and secure medium that performs better than conventional inheritance management.

Instead of sticking to methods of the past, NextHeirs enables more people to be served, as they can deal with their inheritance freely on their own, without having to hire a lawyer at a high price. Also, blockchain technology means the availability of tamper-proof log keeping and the elimination of the danger of fraud or torture.

VI. CONCLUSION

Ultimately, our research and development endeavour served as a platform where we finally birthed Next Heirs, a pioneering instrument in private and decentralized inheritance management. In doing so, we have achieved this by the use of quantum-resistant algorithms and by forming innovative blockchain-technology consensus mechanisms. Hence, our design addresses the threats that are posed by quantum computing. Consequently, the traditional methods that are used in inheritance practices are revolutionized.

Imagining NextHeirs, a reliable and secure digital asset management platform, as a centrepiece of the digital asset landscape of the future, the era of quantum computing, we seem to be providing individuals an opportunity to hold their legacy in their hands. By further improving the app and seeking partnerships with industry experts, we are sure that NextHeirs will go global leaving its definite imprints around the world in the inheritance management sphere.

VII. DISCUSSION

The NextHeirs system's delivery, and use have represented a giant leap forward in the privacy and trustworthiness of fortune transfer. While a critical part of our trip and revelation about its wider significance is right ahead of us, a few major problems willpresumably bear fruit the most.

Impact of Quantum Computing

The core element of our work focuses on a thorough evaluation of the effects of quantum computing on classical cryptography and how that will influence the nature of blockchain technology. Quantum computing poses a major challenge to conventional cryptography approaches, which may eventually cause complete obsolescence and thus make the data that is on the blockchains insecure. Among many stringent countermeasures, we have selected Quantum-proof

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

signatures Dilithium to build in NextHeirs, we have proved to be prevention-oriented and would do all possible to ensure the sustainable safety of cryptographic assets.

Decentralization and Trust

NextHeirs is a model of the decentralized notion of trust, stressing the trustless features of blockchain technology. Through permission less platforms of inheritance procedures and decentralizing places of middlemen with codes of the smart contract and consensus, individuals can take a step toward having more power over their assets and less dependency on prolonged and costly legal procedures. This change using a decentralized trust, leads to an agenda-setting future in asset management, which will give place to new methodologies of diversification, transparency, and autonomy.

Scalability and Performance

Scaling and performance that the NextHeirs' design upgrades is one of the chief issues that required deep analysis. As the blockchain network's scalability problem grows in relevance and complexity, it becomes obvious that the inheritance management systems scalability question is no longer a luxury. We have challenged NextHeirs with a heavy load of inheritances and verified the efficiency of the system in the processing of mass volumes of accounts accompanied by guarantees of the security and reliability of the system. Such a scalability factor is fundamental for the widespread adoption and utilization in the current and potential scenarios to use the NextHeirs application.

Challenges and Future Directions

The experience with NextHeirs during our research was not completely smooth, and these challenges assisted in identifying where to improve efforts for future initiatives. While quantum-resistant algorithms' integration was one of them, the other major hindrances we encountered ranged from designing decentralized consensus mechanism to problem-solving. What could be considered a challenge at first glance brought innovation and growth into our work? Furthermore, now I could present a more polished and up-to-date version of NextHeirs.

Promising features can be further developed with viable routes for research and development planning for the future. The area of quantum-resistant algorithms and the possibility of their incorporation into blockchain technology will become the major subject of focus to be able to adapt to the new challenges provided by the future of quantum computing. Furthermore, continuous improvement in scalability, usability, and accessibility of NextHeirs is yet another key element to be able to make it widely adopted and thus its possible impact.

VIII. CONCLUSION

The advent of blockchain technology is an ongoing process and the threat of quantum computing is one of the things that the sides consider as inevitable. This double-edged sword is playing with fire but at the same time, it offers new horizons. The deep dive started navigating through quantum computing, and blockchain security and their practical implications haveled to the development of the crucial roles and requirements coming into the evolution of digital assets management systems.

The advent of the quantum computer can mark the dawn of the era of computational might, which may make the cryptographic protocols of the old redundant. Given that quantum computers can crack the cryptographic algorithms activating blockchain technology networks, the idea of making them quantum-secured has seriously become a concern to the stakeholders of the blockchain. This has therefore prompted the development of quantum-resistant algorithms that will resist the power of quantum computing adversaries.

With our research serving as the leading force in applying quantum-resistant algorithms throughout the entirety of blockchain-based applications, new possibilities for safety, efficiency, and the overall growth of this emerging sector will become possible. This startup has illustrated that Dilithium 'quantum-resistant' signatures are both a practical and beneficial tool to securely and accurately preserve the inheritance documents through the process of NextHeirs.

The implications of our work on the future are diverse and not limited to estate management but also transcend to issues like trust, decentralization, and resilience in the digital space in form of emergent societies. Using distributed

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

inheritance procedures and e-notary services, NextHeirs is a platform that aligns with blockchain technology's principles such as "trustless" autonomy and individual empowerment.

But our journey has been fraught with difficulties. We had many hurdles to clear from understanding quantum-resistant algorithms and implementing blockchain; we had to find innovative ways around them. Despite all these challenges, we managed to use them as stepping stones for innovation towards achieving a more secure and transparent digital future.

As we review what we have achieved, it is quite clear that going towards quantum resistance in the blockchain system is not only a technological demand but a moral one too. Security and integrity of digital assets are integral aspects of preserving individual freedoms (and thus social contract) with a value-laden society; it forms the basis of who we are as people.

Lastly, our study emphasizes the need for taking action to ensure security weaknesses in blockchain technology, notably with the progression of quantum computing capabilities. We have thus made a stride into that visional future where every individual is capable of securing their digital assets through quantum threats by implementing quantum-resistant algorithms in NextHeirs. This empowers people to secure their legacy for generations down the line as we still explore new horizons at the confluence between quantum computing and blockchain technology; remember that we are steadfastly seeking a more secure, robust, and fair digital environment.

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.

[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

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

[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.