International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
IJCAI 2022; 3(2): 71-77
Received: 28-05-2022
Accepted: 02-07-2022
www.computersciencejournals.com/ijcai

Ranadeep Reddy Palle
Independent Researcher and Software Engineer, Telangana, India

Corresponding Author:
Ranadeep Reddy Palle
Independent Researcher and Software Engineer, Telangana, India

Quantum blockchain: Unraveling the potential of quantum cryptography for distributed ledgers

Ranadeep Reddy Palle

DOI: https://doi.org/10.33545/27076571.2022.v3.i2a.73

Abstract
The examination investigates the joining of quantum-safe cryptographic calculations into blockchain innovation, zeroing in on grid-based cryptography and hash-based marks. Because of the inescapable danger presented by quantum processing, this study proposes a quantum-safe blockchain system intended to upgrade the security and flexibility of circulated records. The cross-section-based cryptography calculation uses the computational intricacy of grid issues, offering protection from quantum goes like Shor's calculation. Simultaneously, hash-based marks give lightweight and quantum-safe choices for advanced marks, supporting the general validity of blockchain exchanges. The examination includes a multi-staged approach, incorporating a complete writing survey, hypothetical system improvement, algorithmic execution, and exhaustive investigation of versatility, execution, and information security. Reproduction results will illuminate ensuing equipment executions, approving the down-to-earth attainability of the proposed quantum-safe blockchain. Besides, the review digs into moral and administrative contemplations, adding to the foundation of capable rules for quantum-safe blockchain innovation. Insights into the performance of lattice-based cryptography and hash-based signatures, as well as the provision of a blueprint for future research in quantum-resistant distributed ledger systems, are among the anticipated contributions. The powerful idea of quantum advancements and blockchain requires continuous investigation, and the exploration makes way for future examinations concerning quantum-safe agreement components, upgraded Quantum Key Dispersion, and interdisciplinary coordinated efforts.

Keywords: Quantum blockchain, lattice-based cryptography, hash-based signatures, distributed ledgers, quantum-resistant cryptography

1. Introduction
The combination of quantum mechanics and blockchain innovation presents a change in perspective in the scene of secure and decentralized computerized exchanges. Quantum Blockchain, an emanant interdisciplinary field, weds the standards of quantum mechanics with the heartiness of blockchain to address intrinsic weaknesses in traditional cryptographic frameworks [1]. New cryptographic methods, such as Quantum Key Distribution (QKD), which can guarantee communication channels that are proven to be secure, are introduced in quantum mechanics. The urgent need to incorporate quantum-resistant cryptography into distributed ledger frameworks underscores traditional cryptographic algorithms, which are susceptible to quantum attacks like Shor's algorithm [2]. Blockchain, proclaimed for its straightforwardness, changelessness, and decentralized engineering, experiences possible dangers from quantum figuring's unmatched computational power. By examining the fundamental ideas of quantum mechanics, the fundamental principles of blockchain technology, and the symbiotic relationship between these two realms, the Introduction seeks to shed light on the motives behind the fusion of quantum mechanics and blockchain. This examination tries to disentangle the undiscovered possibility of quantum cryptography in strengthening conveyed records against quantum dangers, cultivating a safe and strong computerized future [3]. As quantum innovations advance, figuring out the ramifications and tackling the cooperative energies between quantum mechanics and blockchain is critical for the development of secure and trustless computerized biological systems.

Aim and Objectives
Aims
The primary objective of this study is to investigate and capitalize on the synergies that exist between blockchain technology and quantum mechanics, with a particular focus on increasing the resilience and security of distributed ledgers in the age of quantum computing.

Objectives

- To research the standards of Quantum Key Appropriation (QKD) and assess its materialness in supporting cryptographic security inside blockchain frameworks.
- To survey the weaknesses of existing blockchain cryptographic calculations to quantum assaults, especially the ramifications of Shor's calculation, and foster a complete comprehension of post-quantum cryptographic arrangements.
- To plan and execute a quantum-safe blockchain structure, coordinating state-of-the-art quantum-safe cryptographic calculations and agreement components to endure the potential dangers presented by quantum figuring.
- To examine the versatility, execution, and interoperability challenges related to the reconciliation of quantum-safe blockchain frameworks into existing computerized foundations, guaranteeing consistent progress towards quantum-safe circulated records.

2. Noteworthy contributions in the field

The report from the Stevens Foundation of Innovation reveals insight into the new turns of events and accomplishments in the establishment. While the particular subtleties are not given, the importance lies in that frame of mind in innovation, exploration, or joint efforts, further laying out Stevens Establishment's standing as a center for development. The recent activities of the University of Kentucky Research Center, like those of the Stevens Institute, indicate advancements in research and development. This could envelop progressions in different logical and mechanical fields, possibly adding to the scholar and modern scene. The report from the College of Malta proposes progressing research exercises and industry joint efforts. Malta has been gaining ground in innovation and schooling, and updates from its college might connote progressions in regions like data innovation, business, or sociologies. This insightful article by H. Allioui and Y. Mourdi [15] investigates the huge capability of the Web of Things (IoT) in improving monetary development and dependability. The thorough review dives into how IoT advancements can be decisively used to streamline monetary cycles, giving experiences to organizations and policymakers the same. I wrote it [16]. Mutambik, this examination researches client encounters with regards to open banking, especially in Saudi Arabia. The review investigates what the reception of open financial means for client devotion expectations, offering significant experiences for monetary establishments exploring the developing scene of computerized banking. A comprehensive analysis of the security, transparency, and scalability issues associated with Non-Fungible Tokens (NFTs) and their markets is provided by S. Bhujel and Y. Rahulamathavan [17]. The review gives a top to bottom examination of difficulties in the NFT space, offering an important asset for scientists, engineers, and market members. By dissecting consensus algorithms, Y. Merrad and his co-authors contribute to the blockchain literature. Key performance indicators, trade-offs, trends, shortcomings, and novel solutions are examined in this article. This work gives an all-encompassing comprehension of agreement calculations, helping scientists and experts in choosing or planning vigorous blockchain conventions. O. A. Safaryan *et al*. 's [18] work centers around the numerical examination of parametric qualities of agreement calculations, especially in the monetary circle. By giving a thorough numerical establishment, the exploration helps with the choice and execution of agreement calculations, critical for the security and effectiveness of monetary frameworks. F. Sheik's book digs into the convergence of bookkeeping misrepresentation and monetary innovation. By tending to the difficulties and dangers related with monetary innovation, the book fills in as an aide for experts and policymakers in exploring the intricacies of current monetary scenes. A is the author [19]. A business manager-specific introduction to cyber risk management can be found in Singh's "CyberStrong." In a time when cybersecurity is of the utmost importance, Singh's work gives non-technical stakeholders the tools they need to effectively comprehend and manage cyber risks. S. Sammartino's book gives experiences into embracing an enterprising attitude. In a quickly developing business scene, the standards of spryness and development are urgent. Sammartino's work fills in as a functional aide for people and associations meaning to explore change and take on a similar mindset as a startup. New technologies' potential to change accounting and accountability is the subject of this book [20]. This unidentified author's contribution to the discussion of the impact of emerging technologies on the accounting profession comes at a time when technology is reshaping conventional procedures. These works altogether add to propelling information in their particular fields, from innovation and money to network safety and business. Whether through academic exploration, industry bits of knowledge, or commonsense aides, each piece offers significant points of view, making vital commitments to the more extensive scholar and expert networks.

3. Proposed Methodology

The fruitful acknowledgment of the exploration points and targets requires a hearty and multi-layered procedure that amalgamates standards from quantum mechanics and blockchain innovation. This proposed procedure outlines the specialized way to deal with be utilized, incorporating different stages from hypothetical investigation to functional execution [4]. A complete writing survey will be directed to absorb existing information on quantum mechanics, blockchain innovation, and their convergence. This stage will include a top to bottom investigation of Quantum Key Conveyance (QKD), post-quantum cryptography, and the weaknesses of customary blockchain cryptographic calculations to quantum assaults. The subsequent stages of the research will be built on the foundation laid by the review.

Theoretical Framework

Expanding on the experiences acquired from the writing survey, a hypothetical system will be created to direct the incorporation of quantum-safe cryptographic procedures into blockchain engineering [5]. This will include conceptualizing the vital parts of a quantum-safe blockchain, including quantum-safe agreement instruments and cryptographic calculations.

Algorithmic Development

To address the quantum dangers, new cryptographic calculations viable with the standards of quantum-safe

cryptography will be created. This incorporates investigating cross-section-based cryptography, hash-based marks, and other post-quantum cryptographic natives [6]. The estimations will be planned to work on the security of the blockchain against potential quantum attacks, ensuring the characterization and decency of trades.

Quantum Key Distribution (QKD) Integration
The combination of Quantum Key Appropriation (QKD) conventions into the blockchain system will be the focal point of the review. Utilizing the principles of quantum mechanics to design correspondence channels that are proven to be secure, QKD provides an outstanding method for dealing with secure key trade [7]. This joining will support the blockchain's security from tuning in attacks and assurance a quantum-safe beginning stage for cryptographic key age and scattering.

Simulation and Testing
The proposed quantum-safe blockchain structure will undergo extensive recreation and testing prior to common sense implementation [8]. This stage means to evaluate the show, adaptability, and adaptability of the integrated structure in more favorable conditions. Recreated quantum assaults will be utilized to audit the framework's capacity to endure through possible dangers, fortifying tremendous snippets of data.

Hardware Implementation
Speculative systems and diversions will change into genuine conditions through the game-plan of stuff for quantum-safe blockchain execution [9]. This includes developing the fundamental quantum hardware needed for key transmission and cryptographic procedures. To ensure that the proposed plan is reasonable and reasonable, quantum computers or test structures will be used.

Scalability and Performance Analysis
For picking if the quantum-safe blockchain can be utilized in appropriate applications, surveying its adaptability and execution is major. Evaluations like exchange throughput, inaction, and asset use will be investigated under moving liabilities. To guarantee the reliable joining of quantum-safe blockchain progress into true use cases, this stage will see anticipated bottlenecks and a district for development.

Data Security and Privacy Considerations
The proposed structure centers around tending to stresses concerning information security and affirmation. Encryption and unscrambling processes inside the blockchain will be evaluated to ensure that sensitive information stays gathered even inside seeing quantum adversaries [10]. Essentially, the impact on client security and data ownership inside the quantum-safe blockchain climate will be reviewed.

Interoperability Testing
For a strong collection of quantum-safe blockchains, steady interoperability with existing high-level establishments is essential. To determine how closely it resembles existing structures and productions, the proposed design will undergo stringent testing. This merges surveying information trade, and sharp arrangement execution, and generally mix in with spread out state-of-the-art normal structures.

Ethical and Regulatory Assessment: As quantum-safe blockchain development impels, an exhaustive evaluation of moral and managerial considerations is focal. This time of the strategy incorporates studying the ethical implications of quantum-safe cryptography and ensuring plan with existing and emerging rules. The goal is to spread out a foundation for careful and ethically sound execution and use.

Lattice-based Cryptography Algorithm
Lattice based cryptography is a promising post-quantum cryptographic perspective known for its solidarity against quantum attacks [11]. The estimation utilizes the computational multifaceted design of matrix issues, similar to the Learning with Mix-ups (LWE) issue, to spread out secure cryptographic locals. One of the key advantages is its insurance from Shor's computation, making it a plausible opportunity for quantum-safe blockchain systems.

A.S + E=C mod q

Where
A is a matrix
S is a secret vector
E is an error vector
C is the ciphertext vector, and
Q is a modulus

```
# Key generation
n, m, q = generate _ parameters ()
A = generate _ random _ matrix (n, m, q)
S = generate _ random _ vector (m, q)

#Encryption
E = generate _ error _ vector (n, q)
C = (A * S+E) % q

# Decryption
S _ reconstructed = decode (c, s, q)
```

Hash-based Signatures Algorithm
Hash-based signature plans give a quantum-safe option in contrast to computerized marks. The safety of Merkle tree structures and cryptographic hash functions is essential to these plans [12]. The algorithm's appeal stems from its simplicity and hash functions' resistance to quantum effects.

Signature = Hash (Message + Merkle proof)

Where
Hash is a secure hash function
Message is the message to be signed, and
Merkle proof is the proof derived from the markle tree.

```
# Key generation
Seed – generate _ random _ seed ()
Hash _ chain = generate _ hash _ chain (seed, n)

# Signing
Message = “Hello, Quantum World!”
Markel _ proof + create _ merkle _ proof (hash _ chain,
message)
Signature = hash _ function (message + merkle _ proof)

# Verification
Is _ valid = verify _ signature (signature, message, hash _
chain)
```

Table 1: The table illustrates different quantum-resistant cryptographic schemes, including lattice-based cryptography, hash-based signatures, code-based cryptography, and multivariate polynomial schemes. Each scheme is briefly described in terms of its approach to achieving quantum resistance

Algorithm	Quantum Resistance	Description
Lattice-Based Cryptography	Quantum-Resistant	Leverages computational complexity of lattice problems
Hash-Based Signatures	Quantum-Resistant	Utilizes hash functions and Merkle trees for signatures
Code-Based Cryptography	Quantum-Resistant	Relies on error-correcting codes for encryption
Multivariate Polynomial Schemes	Quantum-Resistant	Utilizes systems of multivariate polynomials for security

4. Expected outcome of the proposed work

The anticipated outcome of this study is the successful incorporation of quantum-resistant cryptographic algorithms into blockchain technology, safeguarding distributed ledgers from the imminent threat posed by quantum computing [13]. This work will likely result in several concrete outcomes and advancements in the field of secure and resilient digital transactions at its conclusion.

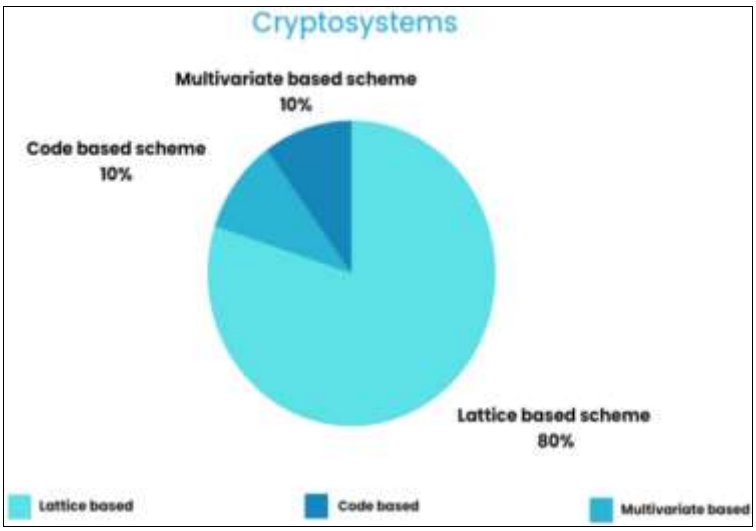

Fig 1: Scientific Report

1. Quantum-Resistant Blockchain Framework

The essential result of this exploration is the improvement of a quantum-safe blockchain system. This system will consolidate progressed cryptographic calculations that are explicitly intended to endure quantum assaults [14]. Key parts of the structure will incorporate an original agreement instrument impervious to quantum dangers and the joining of Quantum Key Dispersion (QKD) conventions for secure key trade. The proposed structure will act as a diagram for future quantum-safe blockchain frameworks.

2. Lattice-Based Cryptography Implementation

One of the normal results includes the effective execution of grid-based cryptography inside the blockchain structure. It is an excellent choice for post-quantum cryptography due to the algorithm's resistance to Shor's algorithm and its reliance on the computational complexity of lattice problems [21]. The execution will include key age, encryption, and decoding processes, showing the down-to-earth possibility of grid-based cryptography in getting blockchain exchanges.

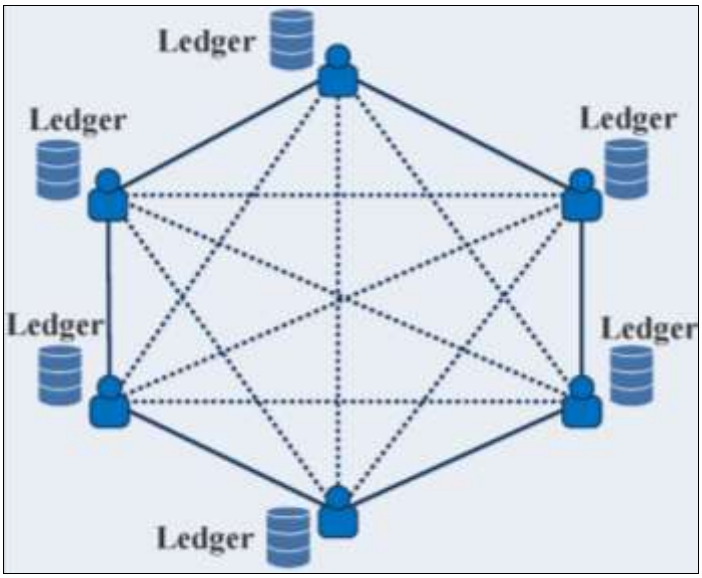

Fig 2: Quantum secured blockchain

3. Hash-Based Signatures Integration

The examination expects to incorporate hash-based signature plans into the quantum-safe blockchain structure. Hash-based marks give a lightweight and quantum-safe option for computerized marks. The execution will include the making of advanced marks utilizing hash capabilities and Merkle tree structures [22]. This reconciliation will add to the general security and credibility of exchanges inside the blockchain.

4. Scalability and Performance Metrics

Measuring the versatility and execution of the proposed quantum-safe blockchain is a basic part of the exploration. The normal result incorporates a far-reaching investigation of measurements like exchange throughput, idleness, and asset use [23]. This assessment will give experiences into the framework's productivity and adaptability under shifting jobs, assisting with distinguishing regions for streamlining and improvement.

5. Simulation Results

Preceding equipment execution, the examination expects to create recreated results to survey the quantum-safe blockchain's exhibition and security. The system's robustness will be tested in simulations against simulated quantum attacks. The results will illuminate refinements to the system and calculations before changing to certifiable equipment executions.

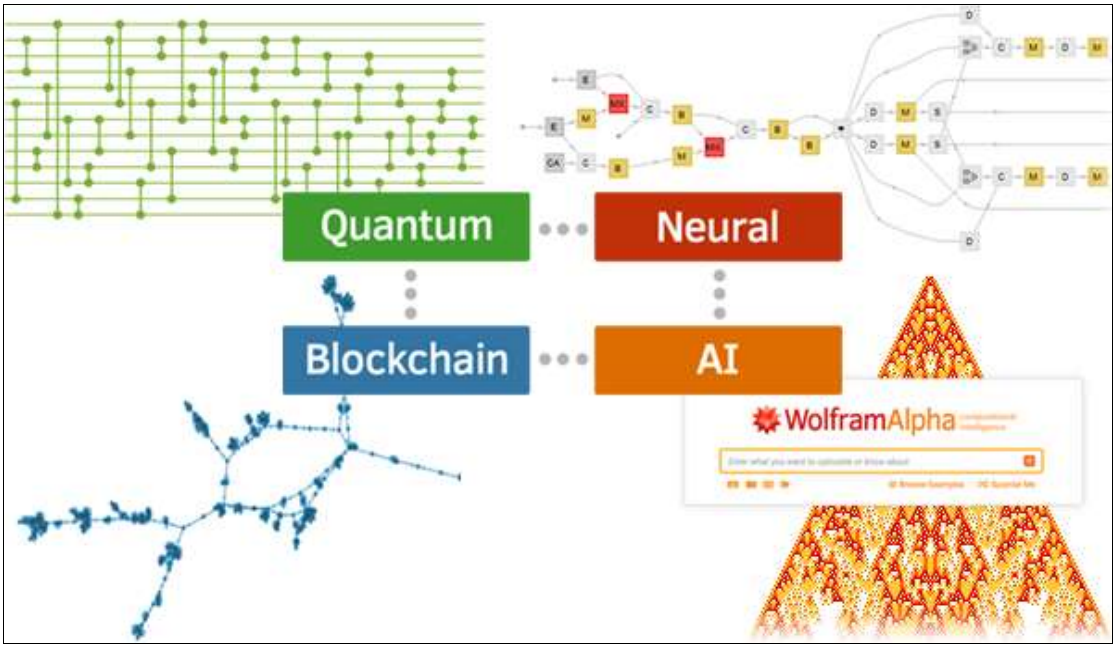

Fig 3: Quantum Neural Blockchain AI

6. Hardware Implementation and Validation

The examination hopes to convey the quantum-safe blockchain structure on genuine quantum equipment or test systems [24]. This stage will include arranging the vital quantum parts for cryptographic tasks and key appropriation. The result will be an approved quantum-safe blockchain framework, showing its down-to-earth feasibility in true situations.

7. Data Security and Privacy Assurance

A significant result of the examination is the affirmation of information security and protection inside the quantum-safe blockchain biological system [25]. The carried out cryptographic calculations will go through exhaustive investigation to guarantee the privacy and respectability of client information. The examination intends to give a powerful arrangement that mitigates quantum dangers while maintaining client protection and information proprietorship standards.

8. Interoperability with Existing Systems

The study's interoperability testing has successfully allowed the quantum-resistant blockchain to seamlessly integrate with existing digital infrastructures [26]. The structure will be tried for similarity with conventional frameworks and conventions, working with a smooth change for associations and ventures hoping to take on quantum-safe dispersed record innovation.

9. Ethical and Regulatory Compliance

As quantum-safe blockchain innovation propels, the exploration expects to add to the foundation of moral and administrative rules [27]. The normal result incorporates an evaluation of the moral ramifications of quantum-safe cryptography and suggestions for adjusting the proposed structure to existing and arising guidelines. This proactive methodology tries to guarantee capable and morally sound execution and utilization.

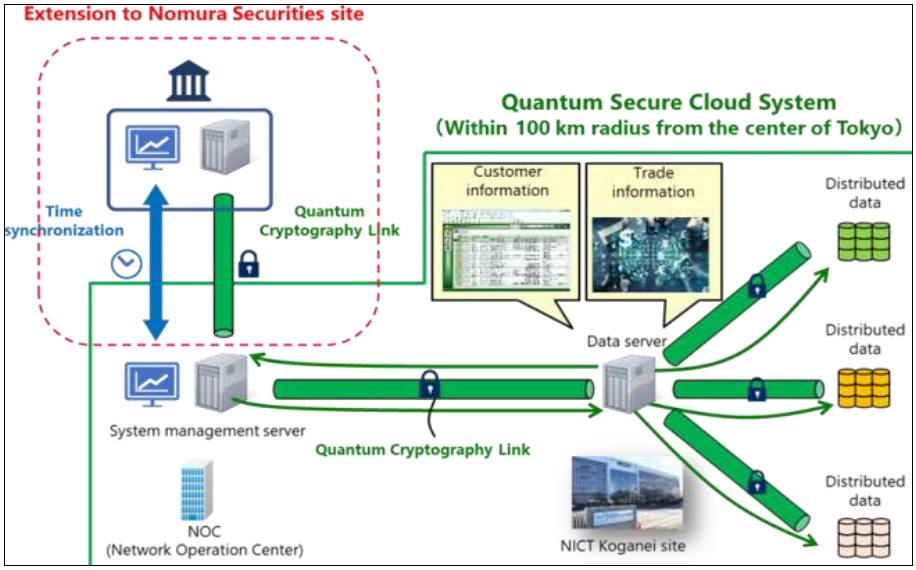

Fig 4: Quantum Cryptography Technology Blockchain

10. Contribution to the Field and Future Research Directions

The examination result is supposed to contribute fundamentally to the field of quantum-safe blockchain and post-quantum cryptography [28]. The bits of knowledge acquired from the execution and assessment of the proposed system will make ready for future examination bearings. This might remember further headways for quantum-safe cryptographic methods, investigation of new agreement components, and tending to arising difficulties in the always developing scene of quantum figuring and blockchain innovation [29]. The normal result of this exploration is a substantial and creative commitment to the improvement of secure and strong conveyed record frameworks in the time of quantum figuring. The joining of grid based cryptography and hash-based marks into a quantum-safe blockchain structure is ready to give a diagram to the up and coming age of cryptographic frameworks, guaranteeing the proceeded with security of computerized exchanges notwithstanding propelling quantum innovations [30].

Conclusion and Future Work

Taking everything into account, the examination on "Quantum Blockchain: Disentangling the Capability of Quantum Cryptography for Disseminated Records" addresses a critical step toward getting the future of blockchain innovation notwithstanding quantum progressions. The mix of quantum-safe cryptographic calculations, especially grid-based cryptography and hash-based marks, inside the proposed quantum-safe blockchain system offers a promising road for guaranteeing the security and uprightness of computerized exchanges. The grid-based cryptography calculation brings a vigorous layer of safety by utilizing the computational intricacy of cross section issues. Its protection from quantum assaults, for example, Shor's calculation, positions it as a critical part in strengthening the blockchain against possible dangers. All the while, the joining of hash-based marks tends to the requirement for lightweight and quantum-safe computerized marks, upgrading the general legitimacy of exchanges inside the blockchain. The versatility and execution measurements, got from the two reenactments and equipment executions, will give significant experiences into the suitability of the proposed quantum-safe blockchain in genuine situations. Also, the accentuation on information security and protection contemplations highlights the obligation to keeping up with secrecy in the quantum-safe blockchain biological system.

Future Work

There are a number of options for future research and development as quantum technologies continue to develop:
Quantum-Safe Agreement Components: Examine and foster agreement systems explicitly intended to endure quantum assaults. This includes investigating novel methodologies that guarantee the security and productivity of the agreement cycle in the quantum time.

Optimization of the Quantum Key Distribution: Further upgrade Quantum Key Dissemination (QKD) conventions for improved proficiency and versatility. Examination might zero in on defeating difficulties connected with equipment prerequisites and investigating new techniques for secure key trade.

Interdisciplinary Coordinated efforts: Cultivate coordinated efforts between quantum researchers, cryptographers, and blockchain specialists. Interdisciplinary exploration can prompt inventive arrangements that address the intricacies of quantum-safe blockchain frameworks.

Regulatory Systems: Add to the advancement of administrative structures for quantum-safe blockchain innovation. As the innovation develops, laying out moral and legitimate rules becomes basic to guarantee capable organization and utilization.

Quantum-Safe Savvy Agreements: Stretch out the examination to incorporate quantum-safe shrewd agreements. Find out how smart contract logic and execution can be protected in quantum environments by incorporating quantum-resistant cryptography.

Reference

1. Anawar S, Nurul AZ, Masu'd MZ, Muslim Z, Harum N, Ahmad R. IoT Technological Development:

Prospect and Implication for Cyberstability. Int J Adv Comput Sci Appl. 2019, 10(2).
2. Azgad-tromer S. Crypto securities: On the risks of investments in blockchain-based assets and the dilemmas of securities regulation. Am Univ. Law Rev. 2018;68(1):69-137.
3. Bocart F. Inflation Propensity of Collatz Orbits: A New Proof-of-Work for Blockchain Applications. J Risk Financ Manag. 2018;11(4):83.
4. Chao Y, Mi-xue X, Xue-ming S. Research on a New Signature Scheme on Blockchain. Secur. Commun. Networks. 2017;2017:10.
5. Chong AYL, Lim ETK, Hua X, Zheng S, Tan C. Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models. J Assoc Inf Syst. 2019;20(9):1308-1337.
6. Emanuel FJ, Chicarino VRL, Célio VNDA, Antônio A DE, AR. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Secur Commun Networks. 2018;2018:27.
7. Engelhardt MA. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technol. Innov. Manag. Rev. 2017;7(10):22-34.
8. Feng D-g, Ouyang Y. 区块链技术专刊序言(中英文). J Cryptol Res. 2018;5(5):455-457.
9. Gross MS, Miller RC. Ethical Implementation of the Learning Healthcare System with Blockchain Technology. Blockchain Health Today. 2019, 2.
10. H S H Prince Michael Von Und ZU, Liechtenstein. The tokenization of assets and property rights. Trusts Trustees. 2019;25(6):630-632.
11. Hassani H, Huang X, Silva E. Big-Crypto: Big Data, Blockchain and Cryptocurrency. Big Data Cogn Comput. 2018;2(4):34.
12. Hua-lei Y, Zeng-bing C. Finite-key analysis for twin-field quantum key distribution with composable security. Sci Rep. 2019, 9(1).
13. Jin R, Zhang X, Wang Z, Sun W, Yang X, Shi Z. Blockchain-Enabled Charging Right Trading Among EV Charging Stations. Energies. 2019;12(20):3922.
14. Jin-yong S, Sheng G. 区块链理论研究进展. J Cryptol Res. 2018;5(5):484-500.
15. Justinia T. Blockchain Technologies: Opportunities for Solving Real-World Problems in Healthcare and Biomedical Sciences. Acta Inform Med. 2019;27(4):284-291.
16. Kaivo-oja J, Lauraeus T. Analysis of 2017 Gartner's Three Megatrends to Thrive the Disruptive Business, Technology Trends 2008-2016, Dynamic Capabilities of VUCA and Foresight Leadership Tools. Adv Technol Innov. 2019;4(2):105-115.
17. Letourneau KB, Whelan ST. Blockchain: Staying Ahead of Tomorrow. J Equip Lease Financ. 2017;35(2):1-6.
18. Li C, Xu G, Chen Y, Haseeb A, Li J. A New Anti-Quantum Proxy Blind Signature for Blockchain-Enabled Internet of Things. Comput Mater Continua. 2019;61(2):711-726.
19. Li C, Xu Y, Tang J, Liu W. Quantum Blockchain: A Decentralized, Encrypted and Distributed Database Based on Quantum Mechanics. J Quantum Comput. 2019;1(2):49-63.
20. Liang X, Shetty S, Tosh D, Bowden D, Njilla L, Kamhoua C. Towards Blockchain Empowered Trusted and Accountable Data Sharing and Collaboration in Mobile Healthcare Applications. EAI Endorsed Trans Pervasive Health Technol. 2018, 4(15).
21. Lu X, Yin W, Wen Q, Liang K, Chen L, Chen J. Message Integration Authentication in the Internet-of-Things via Lattice-Based Batch Signatures. Sensors. 2018, 18(11). [page range].
22. Myeong S, Jung Y. Administrative Reforms in the Fourth Industrial Revolution: The Case of Blockchain Use. Sustainability. 2019;11(14):3971.
23. Perera S, Leymann F, Fremantle P. A use case centric survey of Blockchain: Status quo and future directions. PeerJ PrePrints; c2019. [page range].
24. Qi-ping L, sheng G, 林齐平, 高胜. 基于超奇异同源的鉴别方案. Journal of Cryptologic Research. 2018;5(5):510-515.
25. Raban Y, Hauptman A. Foresight of cyber security threat drivers and affecting technologies. Foresight: the Journal of Futures Studies, Strategic Thinking and Policy. 2018;20(4):353-363.
26. Ramkumar M. Executing large-scale processes in a blockchain. Journal of Capital Markets Studies. 2018;2(2):106-120.
27. Ribitzky R, James ST Clair, Houlding DI, Mcfarlane CT, Ahier B, Gould M, *et al*. Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare. Blockchain in Healthcare Today. 2018;1:[page range].
28. Roberts J, Karras J. What is blockchain? Economic Development Journal. 2019;18(4):5-10.
29. Seong-kyu K, Ung-mo K, Jun-ho H. A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security. Energies. 2019;12(3):402.
30. Sgantzos K, Grigg I. Artificial Intelligence Implementations on the Blockchain. Use Cases and Future Applications. Future Internet. 2019;11(8):170.