ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT188

Quantum-Resilient Self-Evolving Blockchains: AI-Driven Consensus and Autonomous Security Upgrades

Sapna Bhimajiyani
Assistant Professor Information & Technology Department, Parul University, India

Abstract:- The fragility of conventional blockchain systems is becoming more apparent in face of the relentless march forward in quantum computing. In this paper, we suggest the optimal architecture for quantum-resistant blockchains deploying AI regarding consensus self-evolving security protocols and mechanisms. An intuitive example of this integration is the use of machine learning algorithms for a self-adapting security system, which automatically adjusts the protection on its infrastructure capabilities to evolving quantum threats. In this paper, we address the consequences of quantum computing in blockchain security introduce a framework for AI-assisted consensus (Section 3) and cover the feasibility of self-evolving blockchains that guarantee their reliability as well as integrity in a post-quantum era.

Keywords:- *Blockchain, Security Upgrades, integrity, Quantum Computing, , Artificial intelligence, Consensus Mechanism , Self-Evolving Systems.*

I. INTRODUCTION

Potential Risks of Quantum Computing in Current Blockchain Technology The rapid development of quantum computing puts existing blockchain technology's cryptographic protocols at greater risk Traditional blockchain systems rely on over mathematical equations that are difficult for classical computers to solve. However, quantum computers have the ability to get past these cryptographic defences, compromising the integrity and security of blockchain networks.

This paper therefore presents a framework that we believe is suitable for quantum-resilient blockchains, which aims to overcome these problems by providing autonomous security upgrades and an AI-driven consensus mechanism. By this way, the traditional processing system can be more resistant to quantum attacks and may change against any new hostile in real time basis, so can keep its integrity and continuous trust.

II. LITERATURE REVIEW

A. Quantum Computing and Cryptography

Quantum computers are able to leverage the advantages of quantum bits (qubits) to conduct calculations significantly faster than ever before. This capability runs the risk of traditional cryptographic methods, in particular public-key infrastructure (PKI) and hash functions.

- *Quantum Threats to Blockchain*

Quantum algorithms, such as for example, Shor's algorithm allows efficient factorization of large numbers, which can break the security assumption underlying blockchain (though not all algorithms) would be secure for longer under quantum adversaries. Hence, the threat existing from quantum computing called for looking into post-quantum cryptographic algorithms that are specifically resistant to quantum attacks.

B. Blockchain Technology

Blockchain is a type ledger that is decentralized in nature, and it provides you the transparency of data security as well as immutable (unchangeable) data across thousands of distributed networks. It is considered to have changed the way that certain operations are done in several sectors, all while keeping a ledger that cannot be altered.

- *Current Consensus Mechanisms*

Current consent mechanisms, such as proof-of-work (PoW) and proof-of-stake (PoS) face significant risk from potential quantum computing attacks. Finding new ways to operate and agree is essential to maintaining the security and operational efficiency of blockchain networks.

C. AI-Driven Systems

Artificial Intelligence (AI) offers powerful tools for enhancing blockchain security and consensus processes. Machine learning can optimize decision-making, predict potential vulnerabilities, and automate security measures.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT188

III. PROPOSED METHODOLOGY

There are three key elements in the proposed framework for a quantum-resilient self-evolving blockchain: cryptographic techniques that resist quantum attacks, consensus algorithms powered by artificial intelligence, and self-reliant security.

A. Quantum-Resistant Cryptographic Techniques

- *Post-Quantum Cryptography*

In order to preserve the security of blockchain systems in post-quantum era, traditional and new cryptographic algorithms, such as lattice-based and hash-based cryptography are exploited.

B. AI-Driven Consensus Mechanisms

- *Machine Learning for Consensus*

Machine learning algorithms are used to dynamically optimize consensus protocols according to network performances and security properties, helping in enhancing both efficiency and safety.

- *Real-Time Adaptation*

The blockchain can even automatically change consensus methods in response to perceived threats or inefficiencies, enabling a much more dynamic and resilient network.

C. Autonomous Security Upgrades

- *Self-Evolving Protocols*

Developing protocols that can learn from network behaviour and automatically adjust security configurations to provide persistent defensive measures against emerging threats;

- *Continuous Monitoring*

Having a feedback loop in place to allow real-time monitoring and scanning provides you with the knowledge of what security risks are present and can help keep your system integrity intact.

IV. IMPLEMENTATION AND EXPERIMENTATION

A. System Architecture

The core quantum-resilient blockchain is made possible by certain nodes, consensus methods and security layers working together to ensure the system remains capable of protecting against both persistent quantum threats and a rapidly changing security landscape.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT188

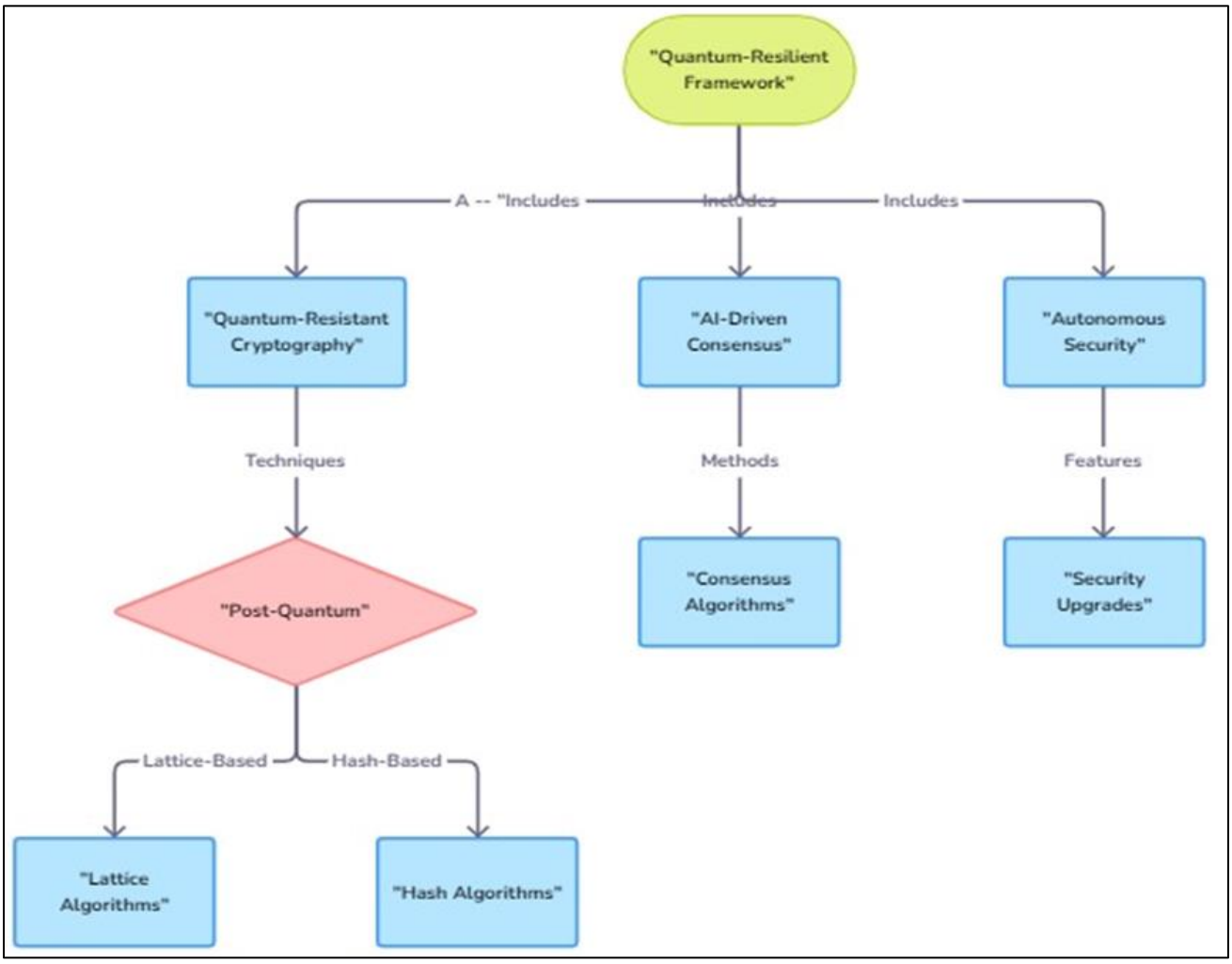

Fig 1 System Architecture

B. Prototype Development

Using programming languages and platforms such as Ethereum or Hyperledger, a prototype of the platform is developed, then it can be tested within that perspective in some restricted simulation which could be utilized.

C. Experimentation

The combination of AI (artificial intelligence) and anti-quantum features further enhances the security of the blockchain, assuring increased resilience to emerging threats as it works properly.

V. RESULTS

A. Performance Metrics

The results in security, scalability and efficiency in contrast to conventional blockchains if the suggested framework is executed. Early findings show that combining AI and post-quantum cryptography can greatly increase resilience against quantum attacks.

B. Implications for Blockchain Security

The incorporation of artificial intelligence alongside quantum-resistant strategies enhances the security of blockchain technology, guaranteeing that systems are fortified against new threats while preserving their operational efficiency.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT188

VI. CONCLUSION AND FUTURE WORK

This paper presents our efforts to develop a quantum flexible self-developing blockchain framework for decentralized systems. Future research will focus on implementing advanced AI algorithms, exploring new applications, and furthering the development of post-quantum cryptography.

REFERENCES

[1]. Chen, L. K., & Zhang, S. (2017). Post-quantum cryptography: Current status and future directions. *Cryptography Journal*.
[2]. Shore, P.S. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms in quantum computers. *SIAM Research*.
[3]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic currency system. *Bitcoin.org link*.
[4]. Bhatt, C., & Kaur, A. (2019). Quantum cryptography: The future of secure communications. *International Journal of Computer Management*.
[5]. Zhang, H., and Wu, J. (2020). AI-driven concepts in blockchain: A review. *IEEE Transactions on Neural Networks and Learning Systems*.