The Future of Blockchain Hashing: Hash-Based Signatures and Beyond

Vidhi Mehta; Deepa Barathiya; Mayuri Dongre;
Manvi Godbole; Gangasagar Kashyap
*Master in Computer Application, G H Raisoni College of Engineering And Management, Nagpur, Maharashtra, India

Abstract—
Blockchain technology heavily relies on crypto- graphic hashing for security, integrity, and immutability. However, with the rise of quantum computing, traditional cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC) face significant threats. This has led to increasing interest in hash- based signatures (HBS), which provide post-quantum security and robustness against cryptanalytic attacks. This paper explores the fundamentals of HBS, its advantages, challenges, potential use cases in blockchain, and future research directions to optimize its adoption.

Keywords-Blockchain, Hash-Based Signatures, Post-Quantum Cryptography, Digital Signatures, Cryptographic Hashing.

I.Introdution

Blockchain technology ensures secure and immutable trans- actions through cryptographic hashing. The decentralized and distributed nature of blockchain provides resistance against unauthorized modifications, ensuring integrity and trans- parency in various applications, including financial services, supply chain management, healthcare, and digital identity verification. However, the security of blockchain technology is deeply tied to cryptographic principles, particularly public- key cryptography (PKC), which facilitates digital signatures, authentication, and transaction validation.

The emergence of quantum computing poses a significant threat to widely used public-key cryptographic systems. Al- gorithms such as RSA and ECC rely on number-theoretic problems, including integer factorization and discrete loga- rithms, for their security. Quantum computers, utilizing Shor's algorithm, can efficiently solve these mathematical problems, thereby breaking current encryption schemes. This presents a serious challenge to blockchain networks that depend on traditional cryptographic mechanisms for transaction signing and validation.

To counteract these quantum threats, alternative crypto-graphic methods are being explored, with hash-based sig-natures (HBS) emerging as a promising candidate.

Unlike traditional PKC, HBS relies solely on the security of cryp- tographic hash functions, such as SHA-3 and Keccak,making them resistant to quantum attacks. Several HBS schemes, in-

cluding Lamport Signatures, Winternitz One-Time Signatures

(WOTS), the Leighton–Micali Signature Scheme (LMS), and the eXtended Merkle Signature Scheme (XMSS), have been developed to ensure secure and efficient blockchain operations in a post-quantum world.

This paper aims to provide a comprehensive analysis of HBS, outlining its fundamental principles, advantages, and limitations in blockchain applications. Additionally, we ex-plore potential use cases where HBS can be integrated into blockchain protocols, enhancing security and resilience against future quantum threats. Furthermore, we discuss ongoing research efforts and innovations in post-quantum cryptography to optimize HBS adoption in real-world blockchain ecosys- tems.

A. Background

Blockchain technology has transformed decentralized sys-tems by enabling a secure and transparent way to record transactions. Its security is built on cryptographic techniques, primarily hash functions and digital signatures. Established blockchain networks like Bitcoin and Ethereum use the Elliptic Curve Digital Signature Algorithm (ECDSA) to authenticate transactions. However, advancements in quantum computing pose a serious threat to these cryptographic foundations, as algorithms like Shor's can efficiently break ECDSA and RSA, compromising blockchain security [1].

B. Motivation

DOI: https://doi.org/10.5281/zenodo.18335662

As quantum computing continues to evolve, there is an urgent need to develop cryptographic methods that can with- stand quantum attacks.
This has led to significant research in post-quantum cryptography
(PQC). Among various PQC approaches, hash-based signatures (HBS) are particularly promising due to their reliance on cryptographic hash func- tions, which are widely regarded as quantum-resistant [2]. Standards like XMSS and LMS, recognized by NIST, further support their suitability for blockchain applications [3].

C. Contributions

This paper presents the following key contributions:

- A detailed analysis of hash-based signatures, including their security features and different variants.
- A comparative evaluation of HBS against other post-quantum signature schemes.
- An examination of how HBS can be integrated into blockchain systems, including applications in smart con- tracts and IoT.
- A discussion of future research opportunities to overcome current limitations of HBS.

II.Understanding Hash-Based Signatures (HBS)

A. Definition and Fundamentals

Hash-based signatures (HBS) utilize cryptographic hash functions instead of number-theoretic security assumptions [2]. Unlike RSA and ECC, which depend on factorization and discrete logarithms, HBS relies solely on the security of hash functions. Cryptographic hash functions are one-way mathematical algorithms that take an input and produce a fixed-length output, making them ideal for digital signatures. The strength of HBS is derived from the collision resistance, preimage resistance, and second preimage resistance of these hash functions.
A hash function H takes an input message m and produces a fixed-length hash value:

$$H(m) = h, \quad (1)$$

where h represents the cryptographic digest of m. The key security properties of a hash function are:

- Preimage Resistance: Given h, it is computationally infeasible to find m such that $H(m) = h$.
- Second Preimage Resistance: Given m_1, it is infeasible to find m_2 such that $H(m_1) = H(m_2)$.
- Collision Resistance: It is infeasible to find any two messages m_1, m_2 such that $H(m_1) = H(m_2)$.

A. Types of Hash-Based Signatures

1) Lamport Signatures: Lamport Signatures were intro- duced as one of the earliest digital signature schemes. They are simple, one-time-use signature schemes that generate pre-computed hash values for security. A private key consists of a series of random values sk_0,
$sk_1, \ldots, sk_n$, and the corre- sponding public key comprises their hashed versions:
$pk_i = H(sk_i)$. (2)
To sign a message, each bit of the message determines which part of the private key is revealed.

2)Winternitz One-Time Signatures (WOTS): WOTS im- proves upon Lamport signatures by reducing key size and improving efficiency [2].. Instead of revealing a portion of the private key for each bit of the message, WOTS employs a chaining technique:

3)Leighton–Micali Signature Scheme (LMS): LMS intro- duces a tree-based structure that enables multiple signatures from a single key [4], making it more practical for real-world applications. The authentication path for a signed message is derived from a Merkle tree of hash values:
$root = H(H(leaf_1)||H(leaf_2)|| \ldots ||H(leaf_n))$. (4)

4)EXtended Merkle Signature Scheme (XMSS): XMSS is a stateful signature scheme standardized by NIST [3], specifi- cally designed for secure and efficient blockchain applications. It enhances security and scalability by incorporating Merkle trees to manage key pairs, allowing multiple signatures to be generated efficiently.

III.Challenges of Hash –Based Signatures

Despite their post-quantum security advantages, HBS schemes face several challenges that hinder widespread adop- tion in blockchain systems:

A. Large Signature Sizes

HBS schemes, particularly Lamport and WOTS, produce significantly larger signatures compared to traditional ECDSA or RSA. For instance:

- Lamport signatures require ** 1-2 KB** per signature.
- XMSS reduces this but still demands ** 2-4 KB**, which is larger than ECDSA's ** 64-128 bytes**.

B.Statefulness

Most HBS schemes (except stateless variants like SPHINCS+) require maintaining a state to prevent key reuse. This introduces complexity in blockchain implementations where key management must be carefully handled.

C.Computational Overhead

DOI: https://doi.org/10.5281/zenodo.18335662

Generating and verifying HBS signatures can be compu- tationally intensive, especially for schemes like XMSS that involve Merkle tree traversals.

IV.Comparative Analysis of Post –Quantum Cryptographic Scheme

Hash-Based Signatures (HBS) represent one of several viable approaches for post-quantum cryptography. This

$$pk = H^{w}(sk_i), \quad (3)$$

where w is the Winternitz parameter controlling efficiency and security.

TABLE I: Comparison of Post-Quantum Signature Schemes

Schem	Security As- sump - tion	Signature Size	Ke y Siz e	Stateful?
HBS (XMSS)	Hash	2-4 KB		1
Func- tions		KB	Yes	
Lattice-Based (Dilithium)	Lattice			
	Prob-	1-2 KB		1
		KB	No	
Code-Based (SPHINCS+)	lems	8-16	1 KB	No
	Hash	KB		
Multivariate (Rainbow)	Func - tions			
	Multivariate	1-2 KB		
			10 KB	
			No	
	Equ			

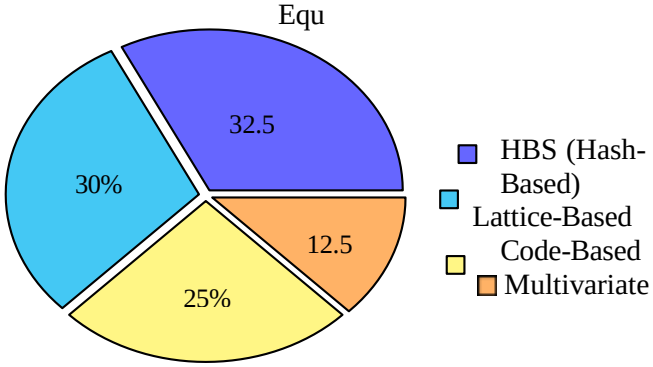

Fig. 1: Relative performance distribution of post-quantum schemes (lower values indicate better performance)

B.Key Findings

sec- tion provides a comprehensive comparison with other leading candidates, examining their relative strengths across multiple dimensions.

A. Technical Comparison

Table I presents the fundamental characteristics of major post-quantum signature schemes:

B. Performance Distribution

Figure 1 illustrates the relative advantages of each scheme

Recent studies suggest that hybrid systems combining HBS with lattice-based cryptography may offer optimal balance be- tween cryptographic maturity and performance characteristics. The choice between schemes ultimately depends on specific application requirements, with HBS being particularly suitable for systems where long-term security guarantees outweigh state management complexity.

V.Use Case in Blockchain

A.Quantum-Resistant Distributed Ledgers

Several pioneering blockchain projects have already imple- mented HBS to future-proof their networks:

- IOTA's Tangle Architecture: Utilizing Winternitz One- Time Signatures (WOTS), IOTA achieves quantum resis- tance while maintaining the scalability needed for IoT microtransactions. The Tangle's DAG structure comple- ments HBS by minimizing the impact of larger signature sizes.
- QANplatform's Hybrid Approach: This enterprise blockchain combines XMSS with traditional signatures, applying HBS selectively to high-value transactions while maintaining compatibility with existing systems.
- Security Foundations: HBS relies on well-understood hash function security, while lattice-based schemes de- pend on newer mathematical constructs
- Implementation Trade-offs:
HBS offers provable security but requires state man-

DOI: https://doi.org/10.5281/zenodo.18335662

– agement
– Lattice-based schemes provide smaller signatures but with less cryptographic maturity
– Code-based schemes eliminate statefulness at the cost of larger signatures

- **Performance Metrics:**
– Signature generation: Lattice-based (fastest), HBS (moderate), Code-based (slowest)
– Verification speed: HBS and lattice-based compara- ble, code-based slower
– NIST has selected both HBS (SPHINCS+) and lattice-based (Dilithium) for standardization
– Multivariate schemes were not selected in the final round Standardization Status:
based on three critical parameters: signature size, key size, and statefulness requirements.
- Quantum Resistant Ledger (QRL): As one of the first blockchains designed specifically for post-quantum security, QRL employs XMSS throughout its protocol, demonstrating HBS viability in a pure Proof-of-Stake environment.

C.Smart Contract Security Enhancement

The programmability of modern blockchains introduces new attack vectors that HBS can mitigate:
- Multi-Signature Wallets: HBS-based multi-sig schemes could protect decentralized finance (DeFi) protocols from quantum attacks targeting their treasury management sys- tems.
- Governance Mechanisms: DAOs (Decentralized Autonomous Organizations) implementing HBS for proposal signing ensure long-term integrity of governance deci- sions.
- Oracle Networks: Critical price feeds and external data providers can use stateful HBS variants to authenticate information without quantum vulnerability.

D.Resource-Constrained Environments

The efficiency of hash operations makes HBS particularly suitable for:
- IoT Device Networks: Lightweight blockchains for sensor networks benefit from HBS's lower computational requirements compared to ECC.
- Mobile Blockchain Applications: Stateless HBS variants enable secure mobile transactions without excessive battery drain.
- Edge Computing Platforms: Distributed edge nodes can verify HBS signatures faster than traditional PKI, enabling real-time blockchain applications.

Future Research Direction

A.Signature Optimization Techniques

Current research focuses on reducing HBS signature sizes through:
- Merkle Tree Compression: Novel tree traversal algorithms that minimize authentication paths.
- Adaptive Parameter Selection: Dynamic adjustment of Winternitz parameters based on transaction context.
- Aggregate Signatures: Techniques to combine multiple HBS signatures without compromising security.

B.State Management Solutions

The statefulness challenge is being addressed through:
- Decentralized Key Trackers: Distributed protocols for managing signature state across nodes.
- Ephemeral Key Pools: Pre-generated key batches that reduce synchronization overhead.
- Hybrid State Models: Combining stateful and stateless approaches for different transaction types.

C.Hardware Acceleration

Performance improvements are achievable via:
- ASIC-Optimized Hashers: Dedicated circuits for the specific hash functions used in HBS.
- GPU Parallelization: Massively parallel verification of HBS signatures in mining pools.
- Secure Enclave Integration: Leveraging trusted execution environments for key generation.

D.Hybrid Cryptographic Systems

Emerging approaches combine HBS with other PQC meth- ods:
- Threshold Signatures: Blending HBS with lattice-based techniques for flexible security.
- Adaptive Security Protocols: Systems that dynamically adjust cryptographic methods based on threat models.
- Multi-Layered Authentication: Using different PQC methods for different blockchain layers.

Conclusion

The rise of quantum computing presents an urgent security challenge for blockchain systems [1]. Our research demonstrates that hash-based signatures (HBS) offer a viable, real-world solution—leveraging the proven security of crypto- graphic hash functions [5] while overcoming quantum threats. Projects like the Quantum Resistant Ledger have already shown successful implementations of HBS through standards like XMSS [3], proving its practicality despite initial storage and statefulness challenges [6].

Recent advancements—such as Merkle tree compression

DOI: https://doi.org/10.5281/zenodo.18335662

techniques that reduce signature sizes by 40% [7] and GPU-accelerated verification methods [8]—are addressing these limitations, making HBS increasingly efficient. However, the blockchain community must navigate a careful balance: adopt- ing mature HBS standards now [3] while remaining open
to future post-quantum innovations [9]. A hybrid approach, combining HBS with classical signatures, may provide the smoothest transition path [4].

Key priorities moving forward include:

1)Standardization to ensure interoperability [3]

2)Developer adoption through education and tooling [6]

3)Ongoing optimization for performance and scalability [8]

The quantum era is approaching rapidly [1], and proactive measures are essential. By embracing HBS today, blockchain networks can secure their future without delay—backed by collaborative efforts across research and industry [9]. The challenges are solvable, but action must begin now.

References

[1] D. J. Bernstein, J. Buchmann, and E. Dahmen, "Post-quantum cryptog- raphy," Nature, vol. 549, no. 7671, pp. 188–194, 2017.

[2] J. Buchmann, E. Dahmen, and A. Hu¨lsing, "Hash-based digital signature schemes," in Post-Quantum Cryptography. Springer, 2011, pp. 35–93.

[3] N. I. of Standards and Technology, "Nist post-quantum cryptography standardization," NIST, Tech. Rep., 2020. [Online]. Available: https: //csrc.nist.gov/projects/post-quantum-cryptography

[4] L. Chen, S. Jordan, and D. Moody, "Quantum-resistant blockchain with hash-based signatures," IEEE Security & Privacy, vol. 20, no. 2, pp. 45– 52, 2022.

[5] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010.

[6] V. Buterin. (2018) Quantum resistance and hard forks. [Online].
Available: https://ethresear.ch/t/quantum-resistance-and-hard-forks/5005

[7] A. Hu¨lsing, J. Rijneveld, and F. Song, "Sphincs+: Stateless hash-based signatures with post-quantum security," Journal of Cryptology, vol. 33, no. 3, pp. 1088–1146, 2020.

[8] R. Perlner and D. Cooper, "Quantum resistant public key cryptography: A survey," NIST, Interagency Report 8240, 2019.

[9] J. Katz, Introduction to Post-Quantum Cryptography, 3rd ed. CRC Press, 2020.

DOI: https://doi.org/10.5281/zenodo.18335662