Acta of Turin Polytechnic University in Tashkent, 2023, 30, 56-61
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

ADVANCING BLOCKCHAIN SECURITY: POST-QUANTUM CRYPTOGRAPHY IN THE QUANTUM ERA

Bakhtiyor Yokubov
Turin Polytechnic University in Tashkent
Email: b.yokubov@polito.uz

Abstract– The emergence of quantum computing presents significant challenges for the security of blockchain technology, traditionally reliant on cryptographic methods now vulnerable to quantum capabilities. This article examines how current blockchain cryptography is at risk due to advancements in quantum computing and emphasizes the urgent need to shift towards more secure, quantum-resistant cryptographic methods. It explores various advanced cryptographic approaches, including lattice-based, code-based, multivariate polynomial, hash-based, and isogeny-based cryptography, highlighting their potential to enhance blockchain security against quantum threats. The focus then shifts to strategies for incorporating these advanced methods into existing blockchain systems, detailing a step-by-step transition process, the importance of comprehensive testing, ensuring compatibility across different systems, and adhering to new global standards. The discussion also covers the potential difficulties and opportunities in this integration, such as performance considerations, maintaining the ability to handle an increasing number of transactions, and the importance of ongoing innovation and research. Finally, the article emphasizes the need for collaborative efforts in research and development to successfully adapt blockchain technology to this new era of quantum computing, ensuring the future security of digital transactions.

Key words– blockchain, quantum computing, post-quantum cryptography, quantum-resistant algorithms

I Introduction

The advent of Bitcoin heralded a pivotal moment in the digital era, thrusting blockchain technology into prominence within digital currencies. This association between blockchain and digital currency is justified, considering that a blockchain serves as a continually updated transaction database across an extensive network of computers [1]. The allure of digital currencies and their valuation underpins the endurance of this network.

Blockchain technology's evolution has seen Ethereum (ETH) attain a level of computational universality known as Turing completeness [2]. This advancement signifies that computational capabilities on ETH are as extensive as those on any contemporary computer, effectively transforming the blockchain into a vast, globally connected computational entity [1].

Money, as a universal medium of exchange, embodies value. The macroeconomic circulation of money reflects the collective intentions of society. Extending this analogy to blockchain, a Turing-complete system like ETH may be viewed as an immense, networked computer utilising digital currency to manifest computational desires.

This understanding naturally posits an open currency system as the foremost and most intuitive application of blockchain when envisaged as a networked computer. Nevertheless, alternative blockchain forms exist, such as permissioned and private blockchains, which operate independently of digital currency generation and consumption for their operational security and reliability. However, when integrated with the internet, these blockchains still face the paramount challenge of authentication.

Authentication remains critical across all types of blockchains—public, permissioned, or private. A verifiable identity for each node within the network is imperative. While many blockchain solutions endeavour to fully virtualize currency and transactions, and despite the deployment of smart contracts like ERC725 to address digital identity fraud, challenges persist [3]. Presently, digital signatures, based on cutting-edge cryptography, are the primary authentication method.

The stability of blockchain technology is deeply rooted in its cryptographic foundation. A compromise in this area could lead to severe disruptions, enabling malicious actors to rapidly access numerous user credentials and jeopardising the blockchain's very essence. Such a breach's consequences could be far-reaching, potentially causing divisions within the blockchain community, as previously observed in the DAO attack [4].

Quantum computing poses a significant risk with its potential to disrupt conventional cryptographic principles. Particularly, Shor's algorithm poses a formidable threat by enabling the factorization of large integers, a fundamental aspect of many cryptographic protocols. This would directly undermine the integrity of digital signatures [5].

Furthermore, quantum algorithms like Grover's could expedite hash computations, quicken block generation, and facilitate potential modifications to the blockchain, thus compromising its integrity. While Grover's algorithm's limitations suggest that increasing hash lengths could mitigate these risks, incorporating quantum-resistant algorithms into the blockchain's security framework is essential for safeguarding against such quantum computational advancements.

II BACKGROUND

Blockchain technology aims to digitise all transactional processes, with the digital signature as the sole authentication mechanism. In a decentralised architecture, this signature essentially represents the user's identity. A compromise of the digital signature by an unauthorised entity poses significant challenges for the legitimate user in rectifying the situation.

Digital signatures, integral to asymmetric cryptography, employ a dual-key system: the public key, which is openly available for identification, and the private key, which is kept confidential. These keys are created so that deriving the private key from the public key is unfeasible. The user utilises the private key to sign messages. A message encrypted with the private key can only be decrypted with its corresponding public key, confirming the message's origin from the private key holder and validating its identity.

The public and private keys exhibit several key properties:

- It is computationally challenging to infer the private key from the public key.
- A message encrypted with a public key is decryptable solely by its corresponding private key, and vice versa.
- The strength of these keys relies on complex mathematical challenges, such as prime factorisation and elliptic curve cryptography, which, with current computing power, require impractical amounts of time to resolve [6].

Thus, deducing the private key from the public key should be prohibitively time-intensive, while verifying a message signed with a private key should be rapid. Underlying mathematical principles maintain this balance. After rigorous mathematical evaluation, encryption methods like RSA and those based on elliptic curves are considered secure for asymmetric encryption.

However, the advent of quantum computing poses a significant threat to this equilibrium. Quantum computers have the potential to solve specific mathematical problems much more efficiently than classical computers, undermining the efficacy of existing cryptographic algorithms. Specifically, quantum computation could simplify extracting a private key from a public key, thereby challenging the security assured by current algorithms.

The rise of quantum computing endangers widely used cryptographic systems, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). Quantum computers, utilising algorithms like Shor's, could feasibly break RSA and ECDSA (Elliptic Curve Digital Signature Algorithm) in polynomial time, an achievement beyond the reach of classical computing [5]. In response, post-quantum cryptography is being developed to create cryptographic systems resistant to the capabilities of large-scale quantum computers [7].

Blockchain platforms, including Bitcoin, rely on elliptic curve cryptography to safeguard token ownership, ensuring that only the rightful owner can engage in transactions [8]. Without a shift to quantum-resistant cryptographic systems, the ownership of tokens could be jeopardised by anyone with access to a powerful quantum computer. This scenario could severely compromise the foundational trust and security underpinning blockchain technology.

III LIMITATIONS OF CLASSICAL CRYPTOGRAPHY IN BLOCKCHAIN

Blockchain technology, central to establishing a secure and decentralized transaction ledger, fundamentally depends on two cryptographic protocols:

1. Asymmetric digital signatures, such as ECDSA and RSA, are integral to public-key cryptography.
2. Hashing functions like SHA-256, essential for implementing consensus mechanisms.

Though challenging for classical algorithms, these protocols are not intrinsically secure against advancements in quantum computing. Shor's algorithm, in particular, poses a significant threat to the integrity of classical asymmetric digital signatures by undermining their trapdoor functions [9]. Additionally, Grover's algorithm can substantially accelerate the Proof of Work (PoW) algorithm, increasing the likelihood of a quantum node dominating the consensus process [10].

The emergence of quantum computing presents a formidable challenge to traditional cryptographic protocols such as RSA and ECDSA. These protocols rely on the computational complexity of the Integer Factorization (IF) problem and the Elliptic Curve Discrete Logarithm Problem (ECDLP), which quantum computers can resolve much more rapidly [9]. The prevalent use of ECDSA in blockchain digital signature schemes makes them particularly susceptible to quantum attacks.

Shor's algorithm can solve problems like integer factorization and ECDLP in polynomial time [9], a critical risk for public-key cryptography systems depending on RSA or ECDSA. Classical computers require exponentially more time to solve these problems. Furthermore, quantum computers using Grover's algorithm could hasten hash generation, potentially enabling the reconstitution of an entire blockchain. Grover's algorithm might also be adapted to identify hash collisions, permitting the substitution of blockchain blocks without compromising the system's integrity [10].

Consider Bitcoin as a case in point: its network transactions are vulnerable to quantum attacks. Bitcoin addresses are initially just hashed values of the user's public key, concealing both the private and public keys. However, when a transaction is broadcast on the network, the user's public key is exposed for verification [11]. With quantum adversaries capable of easily breaking ECDSA, they could infer the user's private key from the public key. This would enable an adversary to forge the user's digital signature, authorizing unauthorized transactions. They could impersonate the user, initiating transactions to transfer funds, acting without the user's consent or knowledge. If such unauthorized transactions are confirmed and added to the blockchain before the legitimate ones, they would be erroneously accepted, hijacking genuine transactions [12].

As quantum computers become more accessible, advancing cryptographic systems and digital signature schemes to be quantum-resistant is crucial, ensuring blockchain-based systems' continued security and integrity.

IV POST-QUANTUM CRYPTOGRAPHY IN BLOCKCHAIN

The emergence of quantum computing necessitates a fundamental shift in the cryptographic foundations of blockchain technology. To fortify blockchain systems against quantum threats, a thorough reassessment and evolution of cryptographic primitives are essential. This section delves into signature methods devised to counteract vulnerabilities inherent in public-key cryptography in the quantum age. These methods are based on various mathematical principles, each providing a distinct strategy for securing blockchain against quantum computing challenges.

1 Lattice-Based Cryptography

Lattice-based cryptography is notable for its resilience to quantum computing attacks. It is predicated on the complexity of solving problems in n-dimensional lattice spaces, which are presumed to be unsolvable by quantum computers. This type of cryptography underlies several proposed quantum-resistant algorithms, including New Hope, NTRU, and LWE (Learning with Errors), each promising robust security against quantum threats.

2 Code-Based Cryptography

Originating from the McEliece cryptosystem, code-based cryptography depends on the difficulty of decoding random linear codes. The security principle of this method is anchored in the complexity of solving the Generalized Syndrome Decoding (GSD) problem, a task that quantum algorithms have yet to solve efficiently. This approach is known for its rapid encryption and decryption processes, albeit often resulting in larger key sizes than other cryptographic methods.

3 Multivariate Polynomial Cryptography

Cryptography employs multivariate polynomials over finite fields to create public keys. Its security is contingent upon the difficulty of solving systems of multivariate quadratic equations, known as the MQ problem, which remains an arduous task for quantum computers. This method is especially efficient in generating and verifying signatures.

4 Hash-Based Signatures

Hash-based signatures are among the earliest examples of post-quantum cryptography. Their security is derived entirely from cryptographic hash functions currently considered quantum-resistant. While they provide strong security assurances, hash-based signatures typically face limitations regarding key usage and have larger signature sizes.

5 Isogeny-Based Cryptography

A recent development, isogeny-based cryptography, concentrates on the computational challenge of identifying isogenies between elliptic curves. The security of this method relies on the difficulty of certain problems in elliptic curve theory, which quantum algorithms have not effectively addressed yet.

6 Quantum Key Distribution

Quantum Key Distribution (QKD) utilizes quantum mechanics to secure communication channels. It facilitates the secure exchange of cryptographic keys, making any eavesdropping detectable. While not a direct application in blockchain, QKD exemplifies a broader spectrum of quantum-resistant cryptographic practices.

In conclusion, post-quantum cryptography is varied, with each approach offering unique advantages and facing distinct challenges. Integrating these cryptographic techniques into blockchain technology is vital for ensuring its durability and security in the forthcoming quantum computing era. As research continues, selecting and adopting these post-quantum cryptographic methods will be critical in protecting blockchain against quantum computing threats.

V ADAPTING BLOCKCHAIN TECHNOLOGY FOR QUANTUM RESILIENCE

The advent of quantum computing necessitates a critical reassessment of the cryptographic infrastructure currently employed in blockchain technology, which is adept at countering conventional computational attacks. This reassessment involves re-evaluating the bit security level metric, a measure traditionally used to gauge the effort required by classical computers to mount a brute-force attack. For example, a 1024-bit RSA key implies a security level equivalent to brute-forcing a key of the same bit length. However, the introduction of quantum computing significantly alters this security paradigm.

Quantum computers fundamentally transform the security landscape. While a classical brute-force attack on an 80-bit security cryptosystem might incur costs ranging from tens of thousands to hundreds of millions of dollars, quantum computers pose a more severe threat. A quantum computer with 1000 qubits could potentially compromise 160-bit elliptic curves, and a 2000-qubit quantum computer might breach a 1024-bit RSA key. This vulnerability extends to systems based on integer factorization and elliptic curves and those reliant on discrete logarithm problems, which Shor's algorithm can efficiently solve.

Conversely, hash functions generally exhibit greater resilience to quantum attacks due to the challenges in developing quantum algorithms for NP-hard problems. Nevertheless, to counter quantum threats, especially from Grover's algorithm, which enhances brute-force capabilities quadratically, the output lengths of hash functions may need to be extended. For instance, a hash function ensuring an n-bit security level in a quantum environment should yield outputs of at least 3*n bits.

Furthermore, Grover's algorithm could potentially hasten mining processes in blockchains like Bitcoin, resulting in faster block generation and potential integrity concerns. Shor's algorithm presents an additional risk by enabling quantum adversaries to forge digital signatures, thus jeopardizing user identities and assets.

In response to these quantum developments, the National Institute of Standards and Technology (NIST) initiated a project in 2016 to establish future post-quantum cryptography standards. By 2017, 59 encryption schemes were submitted, leading to the selection of three digital signature algorithms: Falcon, Dilithium, and SPHINCS+.

Post-quantum cryptosystems intended for blockchain frameworks must exhibit certain characteristics for optimal functionality: small key sizes to ensure efficient storage and management; concise signatures and hashes to prevent blockchain bloat; fast execution speeds to support high transaction volumes; low computational complexity for compatibility across a wide range of hardware; and minimal energy consumption to be environmentally sustainable.

Transitioning to quantum-resistant blockchains is not just a technical challenge but a pivotal step in safeguarding the future of digital transactions in the era of quantum computing.

VI Challenges and Opportunities in Implementing Post-Quantum Cryptography in Blockchain

Integrating post-quantum cryptographic algorithms into established blockchain systems presents significant challenges and opportunities. Successfully navigating these challenges and leveraging the opportunities is crucial for strengthening blockchain systems against the looming quantum computing threat. This section explores the key challenges and opportunities associated with the integration of post-quantum cryptography in blockchain technology.

Integration with Existing Systems: A primary challenge is integrating post-quantum cryptography into blockchain systems that currently rely on classical cryptographic principles. Selecting suitable post-quantum schemes is essential for a smooth transition without compromising security or disrupting ongoing operations. Assessing performance and compatibility with existing systems is imperative. Furthermore, developing new protocols and software tools that support post-quantum cryptography is vital for its efficient integration into blockchain architectures.

Performance Trade-offs: Post-quantum cryptographic algorithms often entail larger key sizes, extended signature lengths, and increased computational demands compared to their classical counterparts. These factors can influence the efficiency, latency, and scalability of blockchain systems. Addressing these issues requires continuous research to refine post-quantum algorithms, exploring hybrid cryptographic solutions, and investigating innovative implementation techniques that maintain security in blockchain systems.

Scalability and Network Efficiency: Blockchain networks need to manage growing transaction volumes and participant numbers efficiently. The larger key and signature sizes inherent in post-quantum cryptographic schemes could exacerbate scalability challenges by increasing storage and bandwidth requirements. Research into key and signature compression, reducing storage overhead, and minimizing the impact of post-quantum cryptography on network performance is essential to mitigate these challenges.

Standardization Efforts and Regulatory Considerations: Standardizing post-quantum cryptographic algorithms is a critical aspect of their adoption in blockchain systems. Organizations such as NIST are instrumental in evaluating and endorsing post-quantum schemes for widespread use. Developers and organizations must adapt to these new standards and modify their systems accordingly as standardisation progresses. Additionally, evolving regulations regarding data protection, privacy, and cybersecurity must be considered in implementing post-quantum cryptography, as these regulations can influence the adoption of new cryptographic technologies in blockchain systems.

In summary, the shift to post-quantum cryptography in blockchain systems entails various challenges and opportunities that require careful consideration and strategic action. Collaborative efforts among researchers and developers are crucial to ensure blockchain technology's long-term security and resilience in the era of post-quantum computing, focusing on effective integration, performance optimization, scalability, and compliance with emerging standards.

VII STRATEGIES FOR POST-QUANTUM INTEGRATION IN BLOCKCHAIN SYSTEMS

Integrating post-quantum cryptographic algorithms into existing blockchain systems is a crucial and complex task that demands a strategic and systematic approach. This section outlines various strategies to facilitate the seamless incorporation of post-quantum cryptography into blockchain technology, thus protecting these systems from potential quantum computing threats.

Gradual Transition to Post-Quantum Cryptography: A phased transition from classical cryptographic protocols to post-quantum alternatives is recommended to minimize disruptions. This step-by-step approach entails updating cryptographic primitives and protocols in stages, maintaining backward compatibility with existing systems. Hybrid cryptographic schemes, which merge classical and post-quantum algorithms during this transitional phase, can provide enhanced security and flexibility.

Thorough Testing and Validation: Rigorous testing and validation of post-quantum cryptographic algorithms are imperative before integrating them into blockchain infrastructures. Assessments should focus on the algorithms' resilience to quantum attacks, their computational and communication efficiency, and compliance with established standards. Additionally, the potential impact of these new algorithms on overall system performance and user experience should be meticulously evaluated and mitigated.

Ensuring Interoperability and Standardization: Effective integration of post-quantum cryptography in blockchain systems necessitates ensuring interoperability across various implementations and platforms. Embracing standardized post-quantum cryptographic algorithms and protocols facilitates smooth interactions and communication between diverse blockchain networks. Collaboration with standardizing bodies, like NIST, is vital for adhering to international guidelines and promoting the adoption of secure and reliable post-quantum solutions.

Education and Awareness: Increasing awareness among developers, users, and stakeholders about quantum computing's implications and the need for quantum-resistant solutions is fundamental to successful integration. Initiatives aimed at education, training, and disseminating research findings are key in accentuating the benefits and challenges of implementing post-quantum cryptography in blockchain systems. A well-informed community is better prepared to make decisions regarding adopting and integrating these advanced technologies.

Ongoing Research and Development: The landscape of post-quantum cryptography is continuously evolving, introducing new algorithms and methods to address emerging challenges and improve existing solutions. Persistent research and development are vital to keep pace with advancements in quantum computing and post-quantum cryptography. Staying informed about the latest developments and actively participating in research endeavours ensures that blockchain systems remain secure and updated in the face of evolving quantum threats.

In summary, integrating post-quantum cryptographic algorithms into blockchain systems necessitates a comprehensive strategic approach encompassing gradual transition, rigorous testing, a focus on interoperability, educational initiatives, and ongoing research. By embracing these strategies, the blockchain community can collaboratively ensure blockchain technology's long-term security and viability in the quantum computing era.

VIII CONCLUSION AND FUTURE DIRECTIONS

In conclusion, integrating post-quantum cryptography into blockchain technology is a precautionary measure and a necessary evolution to safeguard against the impending quantum computing era. This paper has outlined the vulnerabilities of current cryptographic methods in blockchain systems to quantum computing threats and emphasized the importance of transitioning to post-quantum cryptography. Strategies for implementing this transition have been discussed, focusing on the gradual integration of new cryptographic methods, rigorous testing and validation, ensuring interoperability and standardization, raising awareness and education, and the need for continuous research and development.

As we look to the future, several key directions emerge:

Advancements in Quantum-Resistant Algorithms: Ongoing research into developing more efficient and robust quantum-resistant algorithms is paramount. This includes improving the performance of existing algorithms and discovering new cryptographic approaches that may offer enhanced security and efficiency.

Collaborative Standardization Efforts: The role of international standardization bodies like NIST will become increasingly crucial as they set the benchmarks for post-quantum cryptographic methods. Collaboration among academia, industry, and regulatory bodies will be essential to establish and adopt these standards globally.

Blockchain Infrastructure Evolution: Blockchain technology itself must evolve to accommodate new cryptographic standards. This evolution involves both software and hardware aspects, ensuring that blockchain platforms can implement and run post-quantum cryptographic algorithms efficiently.

Education and Training: As the blockchain and quantum computing fields rapidly evolve, the need for specialized knowledge and skills in these areas will grow. Educational institutions and industry leaders should focus on developing curricula and training programs that equip the next generation of professionals with the necessary expertise.

Monitoring Quantum Computing Developments: The blockchain community must stay vigilant regarding the progress in quantum computing. Understanding the advancements in quantum technologies will be crucial for timely responses and updates to cryptographic practices.

Exploring Hybrid Solutions: Investigating and developing hybrid solutions that combine the strengths of classical and quantum-resistant cryptographic methods could provide an effective interim solution while fully quantum-resistant technologies are perfected.

The journey towards quantum-resistant blockchain systems is both challenging and exciting. It presents opportunities for innovation, collaboration, and the development of technologies that could redefine the security landscape in the digital world. The blockchain community, therefore, must remain proactive, adaptive, and collaborative in addressing these challenges and embracing the opportunities that lie ahead in the quantum computing era.

IX References

[1] “What is ethereum?” [Online]. Available: https://ethereum.org

[2] V. Buterin, “A next-generation smart contract and decentralized application platform,” white paper, vol. 3, no. 37, pp. 2–1, 2014.

[3] “Erc725 alliance.” [Online]. Available: https://erc725alliance.org/

[4] M.I. Mehar, C.L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, and M. Laskowski, “Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack,” Journal of Cases on Information Technology (JCIT), vol. 21, no. 1, pp. 19–32, 2019.

[5] T.M. Fern´andez-Caram‘es and P. Fraga-Lamas, “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks,” IEEE Access, vol. 8, pp. 21 091–21 116, 2020.

[6] J.-S. Coron, “What is cryptography?” IEEE Security & Privacy, vol. 4, no. 1, pp. 70–73, 2006.

[7] D.J. Bernstein and T. Lange, “Post-quantum cryptography,” Nature, vol. 549, no. 7671, pp. 188–194, 2017.

[8] “Transactions — bitcoin.” [Online]. Available: https://developer.bitcoin.org/devguide/transactions.html

[9] P.W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.

[10] L.K. Grover, “Quantum mechanics helps in searching for a needle in a haystack,” Physical Review Letters, vol. 79, no. 2, pp. 325–328, 1997.

[11] A.M. Antonopoulos, Mastering Bitcoin, 2nd Edition. O’Reilly Media, Inc., 2017.

[12] J.J. Kearney and C. A. Perez-Delgado, “Vulnerability of blockchain technologies to quantum attacks,” Array, vol. 10, no. November 2020, p. 100065, 2021. [Online]. Available: https://doi.org/10.1016/j.array.2021.100065