# Analytical Exploration of the Effects and Implications of Quantum Computing on Cryptocurrency Systems

Yuanyi Zhang

Rensselaer Polytechnic Institute, Troy, 12180, USA

zhangy85@rpi.edu

**Abstract.** Cryptocurrencies have gained significant importance in the financial market, and the emergence of quantum computers has raised concerns about their impact on cryptocurrency systems. This article aims to analyze these impacts, focusing primarily on the effects on the mining process, threats to blockchain security, and potential solutions to mitigate these effects. Through an extensive review of articles and theoretical research, this article uncovers significant potential effects on cryptocurrency systems resulting from quantum computing. The article highlights that the advent of quantum computing could lead to a drastic acceleration of the mining process, operating in quadratic time. Additionally, it raises concerns about the security vulnerabilities that quantum attacks pose to blockchain systems, as Shor's algorithm poses a considerable threat to the cryptographic mechanisms upon which cryptocurrencies rely. Grover's algorithm, on the other hand, has the potential to significantly reduce the time and energy consumption involved in mining. Although new cryptographic methods, such as Post-Quantum Cryptography, have been proposed to withstand quantum attacks, their effectiveness can only be theoretically evaluated until practical quantum computers become available. At present, the impact of quantum computing on the real world remains limited due to the nascent state of quantum technology. However, with IBM's plan to develop a 100,000-qubit system by 2033, the potential threats to cryptocurrency systems cannot be disregarded.

**Keywords:** Cryptocurrency, Mining, Blockchain, Quantum algorithms, Quantum security

## 1 Introduction

Cryptocurrencies, emerging with the launch of Bitcoin in 2009 by the enigmatic developer Satoshi Nakamoto [1], have become a substantial part of the financial market. Cryptocurrency, as a virtual currency system, enables users to make virtual payments for products and services without a centralized controlling authority. Underpinned by blockchain technology, cryptocurrencies provide a decentralized, peer-to-peer electronic cash system heavily reliant on cryptographic protocols for security and functionality. Over a relatively short span of ten years, the cryptocurrency market has evolved rapidly. As of the time of this writing, more than


P. Kar et al. (eds.), *Proceedings of the 2023 International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2023)*, Advances in Computer Science Research 108,
https://doi.org/10.2991/978-94-6463-300-9_8

10,000 different cryptocurrencies are in use with a total global market value of the circulating supply exceeding $1.17 trillion [2].

Quantum computing and quantum computers have recently become highly significant in technology discussions. Despite the foundation of quantum mechanics being theoretical for more than a century, numerous companies are now investing in the field. Notable names such as Quera, Google, Xanadu, Microsoft, and Amazon are currently advancing quantum computing techniques. Leveraging the concept of quantum superpositions, quantum computers can solve complex computational problems faster than classical computers, posing significant implications for cryptocurrency systems.

Two potentially transformative impacts of quantum computing on cryptocurrency systems involve the mining process and the security of the blockchain. The mining process is crucial in the cryptocurrency system as it adds transaction records and new cryptocurrency units to the blockchain. Many major cryptocurrencies, including Bitcoin, Dogecoin, and Litecoin, rely on a mining mechanism known as Proof-of-Work (PoW) [3]. PoW problems, which involve complex computations, have a unique property: the time complexity to solve the problem is considerably less than the time complexity to verify, and the problem's difficulty can be adjusted with parameters. Quantum computers, using Grover's algorithm and having sufficient qubits, can provide a quadratic advantage in time complexity for PoW [4]. This time advantage applies to both current and future PoW protocols that use computational problems as the primary mechanism [4]. Classical mining algorithms based on PoW will eventually be supplanted by quantum algorithms.

Another facet of the cryptocurrency system potentially impacted by quantum computing relates to blockchain security. Many cryptocurrencies use blockchain technology to securely record all transaction information. Blockchain is protected by cryptographic techniques that secure the data stored in the blocks. Commonly used cryptographic methods include asymmetric encryption techniques such as RSA encryption or Elliptic Curve Cryptography (ECC), which generate public and private key pairs. Rivest-Shamir-Adleman (RSA) relies on the difficulty of factoring the product of two large prime numbers, and ECC is based on the elliptic curve discrete logarithm problem. Both of these cryptosystems are nearly impossible for classical computers to solve but can be easily tackled using Shor's algorithm in quantum computers. Therefore, the security of resources in blockchains is inherently tied to the cryptosystem used, making blockchains particularly susceptible to quantum attacks [5].

The aim of this paper is to offer a succinct yet comprehensive examination of the impacts and consequences of quantum computing on cryptocurrency systems, and potential solutions to these impacts. The subsequent section provides an overview of cryptocurrency systems and the role of quantum computing therein. A brief elucidation of the components of cryptocurrency systems is presented in section 2.1. Section 2.2 discusses the significance of quantum computing in cryptocurrency systems. Section 3 delves deeper into each significant aspect of cryptocurrency systems that could be influenced by quantum computing. Section 3.1 discusses how quantum computing could speed up the mining process in cryptocurrency, primarily

focusing on the implications for the PoW mechanism used in many cryptocurrencies. Section 3.2 addresses the security threats posed by quantum computing to cryptocurrency systems. Section 4 proposes potential solutions to the impacts of quantum computing on cryptocurrency systems. The paper concludes in section 5.

# 2 Conceptual Framework

## 2.1 Cryptocurrency Systems: An Overview

Cryptocurrency operates on a decentralized structure, free from any central authority that manages or controls transactions. This decentralization relies heavily on blockchain technology, which draws on advanced cryptography. Blockchain not only safeguards information but also serves as a ledger recording all transaction data of a cryptocurrency, thereby becoming an asset in itself. The entirety of transaction information resides in the blockchain. Each block within the blockchain encompasses transaction data and information from preceding blocks, maintaining the chronological chain of blocks. Blockchain relies mainly on public key cryptography to secure information. The majority of blockchain systems utilize RSA or ECC to generate their public and private key pairs.

An individual possessing cryptocurrency also has a pair of keys. One is a private key, known only to the holder, and the other is a public key, which is accessible to others. This private key functions as a digital signature, enabling the holder to verify ownership and initiate transactions. All the transaction data inside the blockchain is encrypted and associated with these cryptographic keys to safeguard the information. Without the private keys, outsiders cannot access the transaction information inside the public blockchain.

The term "mining" refers to the process of processing transactions and appending a new block to the end of the blockchain. This action is akin to adding transaction information into the ledger, otherwise known as the blockchain. The act of mining also introduces new units of cryptocurrency into the system. For instance, in the Bitcoin mining process, each time a miner successfully adds a new block to the blockchain, a reward of 6.25 Bitcoin is received. For Bitcoin, mining is the sole method of introducing new Bitcoin into the market, which is true for certain types of cryptocurrencies as well. Some notable cryptocurrencies employ consensus mechanisms like Proof-of-Work, Proof-of-Stake, or a hybrid of these two. Proof-of-Work requires miners to solve complex computational problems that are time-consuming but can be verified swiftly. Proof-of-Work relies on hash functions, a type of one-way function that takes any input to produce a fixed-length output. For hash functions, it is straightforward to determine the output given the input, but it is computationally challenging to ascertain the input from the output. Proof-of-Stake, on the other hand, allows cryptocurrency holders to lock a certain number of tokens within the cryptocurrency system in a process known as staking. Through random selection algorithms and taking into account the total amount held by each holder, a validator is chosen. This validator is responsible for creating a new block in the

blockchain and verifying the transactions within that block. Upon successful completion of this process, the validator is rewarded with cryptocurrency.

## 2.2 The Role and Relevance of Quantum Computing in Cryptocurrency

With the advancements in quantum computing over recent years, practical quantum computers have seen remarkable progress. Major players including Quera, boasting 256 qubits, IBM with 433 qubits, Google with 72 qubits, and Xanadu with 216 qubits, are testament to the strides made in quantum computing. Moreover, IBM's ambitious plan aims at developing a 100,000-qubit system quantum computer by 2033. The emergence of such a quantum computer could potentially solve the world's most complex computational problems and even break existing cryptography. This development could fundamentally disrupt cryptographic systems, which form the bedrock of cryptocurrencies. Two main aspects of cryptocurrencies that quantum computers might impact significantly are the mining process and blockchain technology.

The mining process, especially Proof of Work (PoW), typically demands enormous amounts of electricity to solve intricate computational problems. Bitcoin alone is estimated to consume an astounding 161 terawatt-hours of electricity each year - a consumption higher than many countries. Deploying quantum computers for mining could lead to a potential energy saving of approximately 126.7 terawatt-hours of electricity per year. Research into quantum Bitcoin mining algorithms is underway, and with the development of suitable quantum computers (expected at around 1000 qubits), these quantum algorithms could replace traditional mining algorithms, leading to a quadratic speed-up in time complexity. Other cryptocurrencies that rely on PoW for mining, such as Litecoin, Dashcoin, Dogecoin, Peercoin, Monero, Bytecoin, Namecoin, Paycoin, and Monacoin, could also benefit from the speed-up offered by quantum algorithms. Considering that PoW requires a solution that is time-consuming to find but easy to verify, quantum search algorithms like Grover's algorithm could provide significant advantages.

Blockchain technology could be vulnerable to attack by quantum computing as the current cryptographic systems could be susceptible to Shor's algorithm. Each layer in a blockchain could be attacked by quantum computers, implying that not just one, but all layers need enhancements to ward off quantum attacks. Most critically, due to the decentralized nature of blockchain, if a private key is stolen during quantum attacks, there would be no central authority to address the problem, leading to a loss of all the information controlled by that private key. Post-Quantum Cryptography is considered the most effective method to protect blockchain technology against quantum attacks. However, similar to quantum computers, Post-Quantum Cryptography still requires further research and isn't fully ready for implementation in blockchain yet.

# 3 Quantum Computing's Impact on Cryptocurrency Systems

## 3.1 Influence of Quantum Computing on Cryptocurrency Mining

In the mining process, PoW mechanism will be mostly affected by quantum computing compared to PoS mechanism. Most PoW mechanisms require finding a nonce value for the new block in which the hash value of the new block meets the requirement. Using Bitcoin as an illustration, it needs to find a nonce value that combines with other information can make the block's hash value less than the target hash value. Since the hash functions are designed as one-way functions, it's not practical to find the correct input according to the output. Thus the only way is to go through the enumeration to try all possible input values.

**Table 1.** Quantum Bitcoin mining

**Algorithm 1** Quantum Bitcoin mining

**Input:** Hash Value of Previous Block, Hash Value of Merkle Root, Nonce $o$, Target Value $v$, Transaction $T_1, T_2, ...T_n$

**Output:** Block B such that $\mathrm{HASH(B)} \leq v$ or 'no valid block found'

**Steps 1.** Set states for all possible nonce values to $|0^l\rangle$ which $l$ is the length of Nonce $o$ and apply $H^{\otimes n}$ to each state.

**Steps 2.** Apply Grover's iteration $\sqrt{\frac{N}{t}}$ times where $t \geq 1$ is the total number of solutions.

**Steps 3.** Measure the result, if there are states with significantly higher probability, then these nonce values are valid and we can return the block with any valid nonce value, if all the result probability are about the same, then return 'no valid block found'.

To gain quantum advantages for PoW problems, the most common algorithm is quantum search algorithm based on Grover's algorithm. Grover's algorithm mostly relies on Grover's iteration, which is $H^{\otimes n}R_0H^{\otimes n}O_f$ to find solution for searching length of $N = 2^n$. $O_f$ is the oracle that sets an ancilla qubit to 1 if the input is a solution and 0 otherwise. $R_0$ is conditional phase shift that puts -1 in front of all states except state $|0^i\rangle$ for any $i \in N$. For classical algorithms, the average iterations to find the solutions for inputs with length $N$ is $\frac{N}{t}$, where $t \geq 1$ is the total number of solutions. For Grover's algorithm, the number of Grover's iteration will be approximately $\sqrt{\frac{N}{t}}$, as proved this is the optimal number of iterations for Grover's algorithm to maximize the probability to measure the solutions. Therefore, by using Grover's algorithm, solving PoW problem can gain quadratic advantage in time

consumption. Take SHA-256 hash algorithm, which used in several large cryptocurrencies such as Bitcoin, Peercoin, and Namecoin [6,7], as an example. The output of SHA-256 is always $2^{256}$ bits, therefore, to find one solution under SHA-256, the number of iterations for classical computer will be $3.402 \times 10^{38}$ more than quantum computers [8,9]. Even though previous studies have argued that quantum mining algorithms cannot make large impacts to Bitcoin [10], it's only because current quantum computers are not advanced enough. As quantum computers evolved these years, it can short be strong enough to fundamentally threaten cryptocurrencies, including Bitcoin.

Since Bitcoin is the largest cryptocurrency using the PoW mechanism, Algorithm 1 shows the pseudo-code of quantum Bitcoin mining to demonstrate the quantum PoW algorithm. The goal for Bitcoin miners is to find a nonce value for the new block such that the hash value of the block is less than the target value. As Bitcoin mining is based on SHA-256 hash function, the search space for the nonce will be $2^{256}$. To find the nonce that meets the requirements, miners need to apply Grover's algorithm. As shown in Table 1.

On the other hand, impacts of quantum computing on PoS mechanism itself is not significant as PoS does not rely on computation problem but the amount of cryptocurrency that miner holed. But quantum computing can threaten the security of PoS which may cause holders to lose their cryptocurrencies during the staking process due to quantum attack [11].

### 3.2 Security Concerns: Quantum Computing Threats to Cryptocurrency Systems

As cryptocurrency systems are mainly based on blockchain technology, the threat of quantum attack is also to blockchain. Blockchain usually uses public-key cryptosystem to secure transaction information. Public-key cryptography will generate public and private keys in which the private key acts as digital signature. Whoever has the private key to a wallet that holders cryptocurrencies can access and use these cryptocurrencies. Currently, ECC or RSA are commonly used public-key cryptosystem in blockchain. ECC is based on the intractability of elliptic curve discrete logarithm problem and RSA is based on the intractability of factoring the product of two large prime numbers.

Current cryptographic algorithms such as RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Diffie Hellman (ECDH), Decentralized Stable Asset (DSA), are no longer secure to large-scale quantum computers [12]. With advanced enough quantum computers, Shor's algorithm can find prime factors of large number and solve complex discrete logarithm can in polylogarithmic time, which means Shor's algorithm can break such as public-key cryptosystem ECC and RSA [13]. In particular, the time complexity for Shor's algorithm to find prime factors of integer $N$ will be $\mathrm{O}((\log \mathrm{N})^2(\log \log \mathrm{N})(\log \log \log \mathrm{N}))$.

If quantum computer cracks these cryptographic algorithms, the private key can be easily stolen. Take Bitcoin for instance, the most at risk of quantum attack is when a transaction hasn't been added to the blockchain, but it has been broadcast in the

network [14]. The attacker can then find the private key from the broadcast public key before the transaction is done. With the private key, the attacker can easily get all the Bitcoin from the original address. Due to the insecurity of current blockchain technology to quantum computers, quantum blockchain and Post-Quantum Cryptography are considered potential ways to resist quantum attacks.

# 4 Challenges and Potential Countermeasures

## 4.1 Post-Quantum Cryptography and the Advent of Post-Quantum Cryptography

Post-Quantum Cryptography are cryptographic algorithms that designed to be effective against in quantum attacks, which mostly defend against Shor's algorithm. Post-Quantum Cryptography relies on complex mathematical problem which is hard to solve even for quantum computers. Some of the current major Post-Quantum Cryptography includes Hash-based Cryptography, which is based on the security of certain hash functions, Lattice-based cryptography, which is based on the difficulty of lattice problems such as shortest vector problem, Multivariate Polynomial Cryptography, which is based on the difficulty of solving systems of multivariate polynomials over finite field, and Code-based Cryptography, which is based on the difficulty of decoding generic linear code.

Some current researches have proposed possible ways to secure cryptocurrency under quantum attack using Post-Quantum Cryptography. One way is to use secure cryptocurrency scheme rely on lattice short integer solution (SIS) to protect private key [15]. This solution doesn't need to modify blockchain, and its correctness have been analyzed [15]. Other possible ways to protect the security of cryptocurrency is to use quantum blockchain instead of currently using blockchain. Article [16] have showed quantum blockchain identity framework (QBIF), which is concept for possibility in quantum decentralized blockchain. Also, article [17] shows solution that based on post-quantum X.509 certificates to establish TLS tunnels to secure blockchain and proved its effectiveness by using it in a real blockchain network. More effective and efficient post-quantum algorithms are currently in researching, which can stop the quantum attack when quantum computers are ready.

As the impacts of quantum computing to mining process is mostly on PoW mechanism, a possible way to avoid quantum attack is to change the mining mechanism. Ethereum have switched to PoS mechanism in 2022 and it was using PoW before than, which made it become less risky. Other mining mechanism such as Proof-of-Space are also less affected by quantum algorithms. Since Grover's algorithm only provides quadratic improvement in time, another possible solution to resist quantum algorithm is to extend the search size to maintain the original time that should spend on mining process.

## 5 Conclusion

This manuscript provides an exhaustive literature review on the repercussions of quantum computing on the mining process and blockchain security in cryptocurrency systems, alongside possible countermeasures. It has been found that despite the susceptibility of the cryptocurrency systems' mining process and blockchain to quantum algorithm attacks, a plethora of defense mechanisms exist. The mining process can be safeguarded by shifting from the Proof of Work mechanism to alternative methods and by extending the search size to resist Grover's algorithm. As for blockchain security, potential countermeasures include the implementation of Post-Quantum Cryptography, utilizing secure cryptocurrency schemes such as the Short Integer Solution, and transitioning from classical blockchain to quantum blockchain.

While quantum computers possess numerous advantages over classical computers, there are viable methods to constrain quantum attacks. By incorporating Post-Quantum Cryptography into current cryptocurrency systems, it is possible to maintain market stability without succumbing to quantum threats. Given that advanced quantum computers are estimated to emerge in the next decade, there is ample time to discover robust Post-Quantum Cryptography to thwart Shor's and Grover's algorithms. The aim of this manuscript is to offer an all-encompassing analysis of the implications of quantum attacks on cryptocurrency systems and the potential solutions. Future work should include a deeper analysis of each major type of cryptocurrency, such as Bitcoin, Ethereum, and Tether. An examination of each cryptocurrency's mining mechanism, hash function, and blockchain public-key cryptosystem will yield valuable insights into the impacts of quantum attacks and the strategies to defend against them.

## References

1. Ali A. A Pragmatic Analysis of Pre-and Post-Quantum Cyber Security Scenarios[C]//2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST). IEEE, 2021: 686-692.
2. Shuaib M, Hassan N H, Usman S, et al. Effect of quantum computing on blockchain-based electronic health record systems[C]//2022 4th International Conference on Smart Sensors and Application (ICSSA). IEEE, 2022: 179-184.
3. Treiblmaier H. Exploring the next wave of blockchain and distributed ledger technology: The overlooked potential of scenario analysis[J]. Future Internet, 2021, 13(7): 183.
4. Yue Y, Li X, Zhang D, et al. How cryptocurrency affects economy? A network analysis using bibliometric methods[J]. International Review of Financial Analysis, 2021, 77: 101869.
5. Godoy-Descazeaux I, Avital M, Gleasure R. Images of Quantum Computing: Taking Stock and Moving Forward[J]. 2023.
6. Volya D, Zhang T, Alam N, et al. Towards Secure Classical-Quantum Systems[C]//2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2023: 283-292.

7. Masys A J. Digitizing Policing: From Disruption to Innovation Through Futures Thinking and Anticipatory Innovation[M]//Digital Transformation in Policing: The Promise, Perils and Solutions. Cham: Springer International Publishing, 2023: 1-14.
8. Chatterjee S, Chaudhuri R, Kamble S, et al. Adoption of artificial intelligence and cutting-edge technologies for production system sustainability: A moderator-mediation analysis[J]. Information Systems Frontiers, 2022: 1-16.
9. Solitario R S. Research Outlook of Crypto Systems in the Quantum Computing Era[J]. 2023.
10. Jhanwar A, Nene M J. Enhanced machine learning using quantum computing[C]//2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2021: 1407-1413.
11. Sajimon P C, Jain K, Krishnan P. Analysis of post-quantum cryptography for internet of things[C]//2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2022: 387-394.
12. Rohde P P, Mohan V, Davidson S, et al. Quantum crypto-economics: Blockchain prediction markets for the evolution of quantum technology[J]. arXiv preprint arXiv:2102.00659, 2021.
13. Agarwal A, Kedia A, Yadav K. Quantum computing and its threats to blockchain[J]. J. Anal. Comput, 2022, 16: 1-5.
14. Kaushik K, Kumar A. Demystifying quantum blockchain for healthcare[J]. Security and Privacy, 2023, 6(3): e284.
15. Golestan S, Habibi M R, Mousavi S Y M, et al. Quantum computation in power systems: An overview of recent advances[J]. Energy Reports, 2023, 9: 584-596.
16. Dwivedi A, Saini G K, Musa U I. Cybersecurity and Prevention in the Quantum Era[C]//2023 2nd International Conference for Innovation in Technology (INOCON). IEEE, 2023: 1-6.
17. Lu C, Cui Y, Khalid A, et al. A novel combined correlation power analysis (CPA) attack on schoolbook polynomial multiplication in lattice-based cryptosystems[C]//2022 IEEE 35th International System-on-Chip Conference (SOCC). IEEE, 2022: 1-6.