International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Quantum Computing Threats: Study the Potential Threats that Quantum Computing Poses to Blockchain Security

[1]Krutika Gadge, [2]Dr. Pradyna Borkar, [3]Shreyash Daduria, [4]Dr. Sagarkumar Badhiye, [5]Abhishek Sarodaya, [6]Dr. Roshani Raut

Submitted: 26/10/2023 **Revised**: 16/12/2023 **Accepted**: 26/12/2023

Abstract: With its amazing features like entanglement and superposition, quantum computing has the potential to completely transform industries like cybersecurity. However, it also presents a serious threat to current encryption standards, which are crucial to the security of blockchain technology, raising questions about their viability. Proactive tactics are necessary to address this dual challenge. Blockchain's resilience in the quantum era depends on embracing quantum-secure consensus techniques, maintaining scalability and decentralization, and implementing transitional plans using hybrid cryptography techniques. The future of digital security is largely dependent on how the revolutionary possibilities of quantum computing are balanced with the security imperatives. This study highlights the importance of stakeholder cooperation and quantum-resistant cryptography in achieving this goal, examining the ways in which these tactics strengthen the digital environment.

Keywords*: superposition, cybersecurity, decentralization, imperatives*

1. Introduction

Quantum computing has brought a revolutionary shift to the classical computing models due to its unique properties of quantum bits or qubits. Unlike the classical binary bits, qubits can exist in a superposition of states allowing quantum computers to process information faster exponentially. This super positioning ability enables quantum computer system to handle complex computational problems hard to control for classical machines we all know. Quantum computing goes beyond just its impressive processing power, it holds great potential across various fields, including cybersecurity and cryptography. Existing encryption standards that we have relied on for data protection till now could be rendered out-dated by quantum capabilities for code-breaking. As we analyse the potential security related threats quantum computing poses for blockchain system, it is important to first understand the fundamental difference between classical computing and the transforming application of quantum across various industries. Grasping the core contrasts and capabilities provide the minimum knowledge required to fully understand the multiple sides of the issue arising from the interaction of quantum computing and blockchain security. This background sets the stage for explaining vulnerabilities that can surface at the intersection of these two very important emerging technologies.

[1]Symbiosis Institute of Technology, Nagpur Campus Symbiosis International (Deemed University), Pune, India
krutikargadge29@gmail.com
[2]Symbiosis Institute of Technology, Nagpur Campus Symbiosis International (Deemed University), Pune, India
pradnyaborkar2@gmail.com
[3]Symbiosis Institute of Technology, Nagpur Campus Symbiosis International (Deemed University), Pune, India
shreyashd.sd@gmail.com
[4]Symbiosis Institute of Technology, Nagpur Campus Symbiosis International (Deemed University), Pune, India
sagarbadhiye@gmail.com
[5]Symbiosis Institute of Technology, Nagpur Campus Symbiosis International (Deemed University), Pune, India
abhisheksarodaya18@gmail.com
[6]Department of Information Technology, Pimpri Chinchwad College of Engineerin,Pune
rosh513@gmail.com

A. Fundamental of Quantum computing

1) Quantum Bits (Qubits)

The fundamental building block of information in quantum computing are quantum bits, also known as qubits. Unlike classical bits, which can only be either 0 or 1, qubits have the amazing property of being in a superposition of states at the same time, representing either 1 or 0. Because of this special trait, quantum computers can tackle a ton of data all at once, opening up huge possibilities for certain types of computations.

2) Quantum Entanglement

This phenomenon is defined as follows: the quantum state of two or more particles become entangled with one another so that the states of the particles are inextricably linked, regardless of physical distance separating them. This characteristic is the foundation of quantum computing because it allows quantum algorithm to perform calculation that would be impossible for classical computer to do.

B. Quantum computing algorithms

1) Shor's Factorization Algorithm

A key quantum algorithm called Shor's algorithm has the potential to factor big number quickly. For classical encryption systems, such as RSA, which depend on the complexity of factoring large number to enhance security, this possibility present serious concerns. Many cryptographic system will be able to handle this task if quantum computer can do it well.

2) Grover's Search Algorithm

Grover's algorithm is optimized for quantum computing and is designed to search lists or databases at a quadratic speed faster than its classical equivalent. This suggest that quantum computer could surpass the speed of classical computing in the deciphering of some symmetric encryption and password hashing techniques [1] [2] [3].

C. Development in Quantum Computing

1) Modern Quantum Computing System

- IBM Quantum Computer: IBM is a leader in quantum computing, allowing access to quantum processors through the IBM Quantum Experience platform. The IBM Quantum System One, unveiled in 2019, is a prime example of quantum computing. IBM is working hard to increase the number of qubits and improve the qubit assembly time in its quantum processors.
- Google Quantum Computing: Google's Quantum AI Laboratory is at the forefront of quantum research. In 2019, Google claimed quantum sovereignty with its quantum processor Sycamore, which demonstrated the ability to perform specific tasks faster than traditional supercomputers This event focused on the power of quantum computing
- Advances in qubits: One notable exception is the ever-increasing number of qubits in quantum processors. Both IBM and Google, among other companies, have been working to increase the number of qubits in their quantum systems. We need that scalability to tackle more demanding computing challenges [4] [5].

2) Advance in Quantum Technology

Examine the ongoing studies and development in quantum technology. Emphasis efforts to improve qubit coherence times, forge fault-tolerant quantum computers, and make quantum computing more practical and scalable.

- Qubit Coherence Enhancements: Extending qubit coherence times, which are essential to the stability and dependability of quantum computations, is the focus of ongoing research. Error correction and external influence isolation are two strategies that are investigated to reduce the effect of quantum decoherence and improve qubit overall coherence [4].
- Practicality and Scalability: One of the main goals is to increase the practicality and scalability of quantum computing. System integration, error correction overheads, and the integration of quantum processors with classical computing infrastructure are among the issues that researchers are tackling. Scalability and a practical quantum advantage are necessary for quantum technology to be widely adopted in a variety of applications [6].
- Quantum Algorithm Development: The usefulness of quantum computing is greatly enhanced by developments in quantum algorithms. Current research endeavors center on optimizing current algorithms and creating new strategies that capitalize on the special powers of quantum systems. This includes making an attempt to effectively solve difficult issues like cryptography and optimization tasks [7].
- Fault-Tolerant Quantum Computers:The development of fault-tolerant quantum computers is a major focus area for quantum technology. Because these systems are built to withstand noise and errors that come with quantum computations, the accuracy of the results is guaranteed. In this quest, novel error correction codes and fault-tolerant architectures play a crucial role, providing an insight into robust quantum computing in the future [10].
- Materials Science and Quantum Hardware: The development of quantum hardware is greatly aided by research in materials science. Improvements in the performance of quantum devices lead to more stable and scalable quantum computations. These advancements are facilitated by new quantum hardware architectures and materials for qubit fabrication [11] [12].
- Quantum Communication Networks: Developments in quantum communication networks go beyond quantum computation. The creation of secure quantum communication channels and quantum key distribution protocols enhances the practicality of quantum technology by supporting the ecosystem as a whole [13].

2. Threats to Quantum Computing

Although quantum computing has a lot of promise, there are a few significant issues and problems with it as well. These risks don't just affect the technical side, they have many other problem as well.

1. Risks to Quantum Security: Quantum security threats present a paradoxical challenge for quantum security. Many of the encryption algorithms in use today could be compromised by quantum computers as they grow in power. Quantum attacks can go and attack systems that keep our data safe, such as RSA and ECC in cryptography. concerns about privacy loss and the

requirement to create cryptographic solution resistant to quantum fluctuation are raised by this [1].

2. Quantum Error Correction: Quantum computing is extremely error-sensitive due to its intrinsic quantum nature. Quantum attacks can go and attack systems that keep our data safe, such as RSA and ECC in cryptography. Nevertheless, creating and putting into practice reliable error correction techniques continues to be very difficult [2].
3. Limited Hardware and Scalability: Building and maintaining hardware for quantum computing is difficult. Currently, quantum computers can only handle a limited number of computations because it has a finite number of qubits. One of the biggest obstacles to the wider application and accessibility of quantum computing is the achievement of scalability in quantum hardware [3].
4. Quantum Software Engineering: There is a dearth of quantum software developers in the challenging field of quantum software development. It's still difficult to bridge the gap between software development and hardware capabilities [6].
5. Environmental Factors: Quantum Computer operates on low temperature, which can be expensive and technically challenging to maintain [8].
6. Ethical and Regulatory Concerns: Quantum computing's amazing computational power raises question about possible abuse. It is imperative to tackle ethical and regulatory aspect in order to guarantee the conscientious advancement and application of this technology [9].
7. Countermeasure for Quantum Cryptography: Although classical encryption is in danger due to quantum computing, there is also hope foe quantum-resistant encryption. To counter this threat, efforts are being made in race to develop and implement quantum-resistant cryptography techniques [10].
8. Technological Difficulties: It can be difficult to create a pure and interference-free environment for quantum computers outside of specialized facilities [11].
9. Quantum Cryptanalysis Algorithm: The threat posed by quantum algorithms such as Shor's and Grover's to traditional cryptography system is growing. This development might jeopardize privacy and data security [6] [12].

It concludes that although quantum computing present novel opportunities, it also brings serious risks and obstacles that need to be resolved as this technology develops. Researchers and organizations must continue to be aware of these issue and collaborate to find solution to lessen these threats as they attempt to fully utilize the potential of quantum computing.

3. Importantance of Overcoming Quantum Computing Threats and Ensuring Security

With the rapid advancement of quantum computing, the field of digital security is set to undergo a profound transformation. It is crucial for these potential threats to be proactively addressed, and strong security protocols must be established for a multitude of compelling factors.

1. Preserving Data Privacy: In a time when enormous volumes of private information flow across digital networks, protecting this data's privacy is critical. The confidentiality of sensitive, private, and financial information is at risk due to the possibility of quantum attacks breaching traditional encryption techniques. Preserving data privacy requires removing this threat [1].
2. Maintaining Trust in Digital Transactions: The foundation of all digital transactions, including online banking, e-commerce, and international communication, is trust. This trust is put at risk by the security breach brought about by quantum threats. In order to preserve confidence in digital transactions, it is imperative that these threats be eliminated [2].
3. National Security: There are implications of quantum computing for national security. Secure communication and data protection are crucial for governmental agencies, military groups, and businesses linked to critical infrastructure. Security against quantum threats must be ensured to protect national interests [3].
4. Economic and Business Stability: Businesses, financial institutions, and enterprises rely on robust security measures to protect their operations, intellectual property, and private customer data in a world where digital technologies are becoming more and more important. Quantum attacks may have a negative effect on the economy and business continuity [6].
5. Preventing Critical Infrastructure Disruption: Safe digital systems support vital services like energy grids, transportation networks, and healthcare systems. The possibility of quantum threats poses a serious danger, as it could lead to a breach in security that puts public health and safety at risk and weakens crucial infrastructure. Precautionary measures for security are necessary to prevent these disruptions.[7].
6. Technological Innovation: Quantum computing has the potential to transform fields like materials science, drug development, and complex simulations, even in spite of security concerns. Security must not be compromised by these innovations. By using secure quantum technologies, it is possible to take advantage of quantum computing's benefits without sacrificing security or privacy [8].

7. Accuracy and Data Integrity: Threats from quantum computing affect data integrity and go beyond encryption. Maintaining the integrity and precision of data is paramount in industries such as science, law, and allied fields. Maintaining data integrity requires thwarting quantum threats [9].
8. Global Cooperation: International cooperation is necessary to counteract quantum threats. By implementing a set of common security standards and practices, the quantum era can be made more secure on a global scale. This framework will promote consistency and cooperation, allowing for a comprehensive and united approach to security.[10]

Overall, it is imperative to prioritize the mitigation of risks tied to quantum computing. By effectively addressing factors such as security, economic stability, resilience of critical infrastructure, technological advancement, data integrity, and international collaboration, we can work towards ensuring a safer and more stable future. Safe quantum technologies are essential to maintaining the dependability of our digital infrastructure and protecting people, businesses, and countries against possible security breaches brought on by quantum technology.

4. Blockchain Technology

Blockchain technology is an emerging technology and has become very important in the modern day and is changing how data and security works. A blockchain is a decentralized record that keeps data and transactions accurate. Blockchains are secure, trustworthy, and provides transparency. This makes them useful for all sorts of industries.

Blockchains don't need central control as they are decentralized. It's data doesn't change and stays the same because blockchains are immutable. Security and transparency are the key features because it ensures accountability and prevent unwanted changes that can be threating to the integrity of the data. A distributed digital ledger that is shared over a computer network is called a blockchain. This technology allows information to be stored electronically and essentially serves as a database. Blockchains have become widely recognized due it's essential function in cryptocurrency systems such as bitcoin, which maintains a safe and distributed ledger of transactions. Blockchain is innovative because it can guarantee the security and integrity of data records, promoting trust among network users without requiring a centralized, reliable third party.

Unique Properties of Blockchain.

1. Decentralization: Without a single central authority, blockchain function as a peer-to-peer network. Rather, they depend on a dispersed computer network, or nodes, to uphold and verify transactions.
2. Immutability: After data is recorded on a blockchain, it cannot be removed or altered. This essential quality of immutability protects the data's integrity.
3. Transparency: Every transaction carried out on a blockchain is visible to all network users and is publicly recorded. This openness guarantees that the history of the ledger is accessible for examination
4. Security: Data and transactions on blockchains are protected by cryptographic techniques, which makes it very difficult for unauthorized access or fraudulent activity to occur [8]

5. Mitigation and Countermeasur

D. Post Quantum Cryptography in Blockchain

One essential component in protecting blockchain technology against possible attacks from quantum computers is post-quantum cryptography, or PQC. Conventional cryptographic algorithms, which are the cornerstone of blockchain security, can be broken by quantum computers. The adoption, strategies and tactics for preventing Quantum threats to blockchain system is discussed as follows.

E. PQC Implementation and Adoption

Although in its early stages of development, quantum computing presents a significant risk to blockchain systems. Due to their vulnerability to quantum attacks, the cryptographic systems used by blockchains are especially at risk. Therefore, it is now essential to adopt and implement PQC in order to safeguard the security and integrity of blockchain technology.

Post-quantum cryptography uses cryptographic algorithms that are difficult for quantum computers to decipher. These algorithms give quantum computers challenging mathematical puzzles that they cannot solve in a reasonable amount of time. The fundamental component of PQC is this mathematical problem, which also serves as a strong barrier against any dangers that quantum computing may bring.

- Updating Cryptographic Protocols and Algorithms: An essential first step in implementing PQC in the context of blockchain technology is to update cryptographic algorithms and protocols at different systemic levels. Although PQC algorithms abound, some exhibit more promise than others in terms of resilience against quantum attacks. These algorithms provide a means of protecting blockchain data and transactions in a world where quantum vulnerabilities are becoming more prevalent.
- Hybrid Systems as an Transitional Measure: Even though widespread adoption of fully functional quantum computers is still some way off, the threat posed by quantum computing is real. As such, it is imperative that we consider future-proofing our

blockchain systems. Combining quantum-resistant and classical cryptography to create hybrid systems is a workable approach.

- Ongoing Research and Updates: With an eye towards the future, being proactive is essential. Blockchain technology needs to continue being flexible and open to new advances in cryptography. It is anticipated that quantum computing power will continue to increase, so our defense systems will need to change as well. This is similar to the ideas of cybersecurity, wherein a vulnerability is complacency. In a post-quantum world, regular updates to quantum-resistant cryptography will be essential to maintaining blockchain security [7].

F. Proactive Mitigation Strategies

There is no denying the existence of the quantum threat and the significant effects it will have on blockchain security. On the other hand, proactive mitigation techniques, like hybrid systems and ongoing research and development of cryptographic techniques, provide a way to maintain the reliability and robustness of blockchain technology. No computer is too powerful if the proper security measures are taken.

To sum up, post-quantum cryptography adoption and application are essential to the long-term security of blockchain systems. Blockchain technology can withstand potential quantum threats by conducting research and development, investigating hybrid systems, and improving cryptographic protocols. Although the quantum threat is real, it is not unavoidable, and blockchain technology can continue to be a dependable and safe solution for a range of uses with the correct strategy.

The potential danger of quantum computing in the context of blockchain technology makes it necessary to carefully weigh the options available for preserving functionality and security. Here, we list the most important tactics and design tenets for fending off the quantum threat while maintaining decentralization, scalability, and seamless transitions.

G. Quantum-Secure consensus Machine

The challenge for blockchain networks is to move to quantum-secure consensus methods in order to fend off quantum attacks. The author in [13] provides extensive documentation on this requirement. Their study demonstrates how multilevel and lattice-based cryptography can strengthen Proof-of-Work (PoW) and Proof-of-Stake (PoS) agreements' defense against attacks using quantum computing. These methods maintain the security of blockchain networks by using hash functions and digital signatures that are resistant to quantum attacks.

H. reserving Scalability and Decentralization

For blockchain systems, scalability and decentralization are essential design concepts. While switching to quantum-resistant protocols is imperative, it's also critical to make sure that these fundamental ideas are not compromised in the process. For decentralized consensus protocols such as PoS and PoW to remain functional, they need to maintain their scalability and decentralized characteristics.

An invaluable resource for understanding how to navigate the quantum threat landscape is discussed by author in [1]. This discussion provides direction for modifying blockchain systems to meet quantum challenges while maintaining scalability and decentralization.

I. Transitional Plans and Hybrid Methodologies

Using hybrid approaches and transitional plans is a big part of getting ready for the quantum threat. As blockchain systems progress toward complete quantum safety, hybrid strategies combining both classical and quantum-resistant cryptography techniques are likely to be required. This strategy preserves security while enabling a seamless transition.

This transition can be supported by implementing quantum-resistant digital signatures and hashes gradually with ongoing projects. It is imperative that we approach this evolution with caution and a proactive mindset. As part of their proactive approach, blockchain systems should start experimenting with and implementing quantum-resistant protocols. To ensure a smooth transition, any disruptions to current networks must be minimized at the same time.

As discussed above,blockchain technology is facing the quantum threat head on at this critical juncture in its evolution. To overcome this challenge, the blockchain community must take a versatile approach that includes hybrid strategies for a smooth transition, protects decentralization and scalability, and embraces quantum-resistant consensus mechanisms. Blockchain systems can survive the threats posed by quantum computing by adhering to these guidelines and consulting pertinent research, as discussed above. This will ensure the security and resilience of decentralized networks [6] [7] [11] [13].

6. Techniques for Overcome Quantum Computing Threats and Ensuring Security

As quantum computing advances, different methods and approaches must be used to protect digital security and counter the threats it presents. In order to reduce quantum threats and improve the security of digital systems, these strategies are crucial:

1. Cryptography Resistant to Quantum Elements: Employing quantum-resistant cryptographic algorithms is a cornerstone in defending against quantum threats,

as these algorithms are designed to withstand attacks such as Shor's algorithm. The goal of current post-quantum cryptography research is to create encryption techniques that are resistant to powerful quantum computers.

2. Quantum Key Distribution (QKD): By utilizing the ideas of quantum mechanics, QKD makes it easier to create safe channels of communication. This enables secure distribution of encryption keys while also ensuring that any eavesdropping efforts are rapidly detected. Putting QKD into practice provides a strong defense against quantum threats.
3. Lattice-Based Cryptography: A class of quantum-resistant cryptographic algorithms is known as lattice-based cryptography. It depends on how difficult some lattice-related mathematical problems are. Adopting lattice-based encryption methods is a viable way to strengthen data security in a world where quantum threats exist.
4. Code-Based Cryptography: This method of encrypting data depends on how difficult it is to decode linear codes. This approach is know as post-quantum cryptography which is protected from quantum attacks Using code-based cryptography increases the level of security for online communications.
5. Multi-Party Computation: Methods for multi-party computation allow participants' privacy to be maintained while safe data processing and computation are performed. These methods guarantee the security of computations and sensitive data even in the face of quantum threats.
6. Quantum-Safe Blockchain Solutions: In the field of blockchain technology the creation of quantum-safe consensus mechanisms and creation of cryptographic algorithms is crucial. By defending blockchain networks from quantum attacks, these solutions hope to maintain the security and immutability of blockchain records in the quantum era [13].
7. Continuous Research and Standardization: It is vitally important to continue research and establish standards for quantum-resistant methods. Adoption of secure techniques to counter quantum threats is greatly aided by international cooperation and the creation of standardized security practices.
8. Quantum Error Correction: Reliable quantum computing requires the development of strong quantum error correction codes. By reducing the effects of quantum noise, these methods preserve data integrity and guarantee the accuracy of quantum computations.
9. Awareness and Education: It is essential to raise awareness and spread information about security precautions and quantum threats. The first line of defense against quantum vulnerabilities is to recognize the risks and implement best practices.
10. Cooperative Attempts: Governments, businesses, and research organizations must work together. Developing of quantum-resistant technologies and building a complete security framework that protects digital systems, privacy and data from all the possible threats that will come with quantum computing we need to have collaboration and cooperation [7] [10] [11] [12].

In order to mitigate the risks posed by quantum computing and ensure security in the quantum era, a comprehensive and collaborative approach is required. This strategy combines strong cryptography, quantum-resistant cryptography, quantum key distribution, ongoing research, international collaboration, and education. These efforts, when combined, fortify data, privacy, and digital systems against the rapidly changing quantum technology environment.

7. Conclusion

The emergence of quantum computing poses a twofold challenge to the field of digital security. This study has clarified the numerous risks that quantum computing presents and highlighted it's broad ramifications. It is crucial to ensure security in the face of quantum threats. Proactive steps are necessary due to the potential consequences for data privacy, trust in digital transactions, and national security, as well as the ability of quantum computing to compromise traditional encryption methods.

There is a repertoire of techniques being developed to counter these threats. Securing digital communication requires the use of quantum-resistant cryptography, quantum key distribution, and error correction techniques. Establishing standard security practices requires cooperation between governments, businesses, and academic institutions. Information is spread via education and awareness campaigns, enabling people and organizations to defend against quantum vulnerabilities.

Finding a balance between protecting digital landscapes and utilizing the potential of quantum computing is a key challenge in navigating the quantum era. The future of digital security will be shaped by cooperative efforts and quantum-resistant strategies that maintain data, privacy, and the integrity of digital systems in the quantum era.

References

[1] Sharma, R., Kumar, R., & Singh, S. (2023). Navigating the quantum computing threat landscape for blockchains: A comprehensive survey. IEEE Access, 11, 10022-10041.

[2] Shor, P. W. (1994). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 23(5), 1010-1036.

[3] Sathya, B. S., Kumar, R., & Srinivasan, D. (2023). A review of quantum computing threats to blockchain security and mitigation strategies. Computer Science Review, 49, 100580.

[4] Kawase, K., & Gambetta, J. (2022, May 31). Building Japan's quantum future with IBM Quantum System one. IBM Reseach-https://research.ibm.com/blog/japan-quantum-system-one?mhsrc=ibmsearch%_%a\&mhq=IBM+Quantum+System+One\%26period\%3B (referred on 10/2023)

[5] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandão, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., . . . Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

[6] Chen, Z., He, D., & Zhang, Y. (2022). Quantum computing: A threat to blockchain security? IEEE Transactions on Emerging Topics in Computational Intelligence, 7(1), 134-142.

[7] He, D., Chen, Z., Zhang, Y., & Wang, X. (2022). Post-quantum cryptography for blockchain security. IEEE Transactions on Reliability, 71(4), 1693-1704.

[8] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder,S.(2016).Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.

[9] Kerenidis, I., & Prakash, A. (2018). Quantum attacks on Bitcoin, and how to protect against them. arXiv preprint arXiv:1803.08220.

[10] Moody, D., Chen, L., & Perlner, R. (2021). Post-quantum cryptography: A NIST perspective. NIST Interagency Report (NISTIR), 8309.

[11] Chailloux, A., Plosker, S., & Winter, A. W. (2022). The impact of quantum computing on present cryptography. arXiv preprint arXiv:2202.07077.

[12] Lipton, R. J., & Stark, E. S. (2019). Quantum attacks on public-key cryptosystems. Annual Reviews of Computer Science, 4(1), 343-368.k

[13] Camenisch, J., & Neven, G. (2022). Quantum-resistant cryptography for blockchain. Nature, 601(7893), 470-477