Issues in Information Systems
Volume 24, Issue 3, pp. 144-158, 2023

DOI: https://doi.org/10.48009/3_iis_2023_113

Quantum threat and dependability of quantum-safe blockchain-based distributed control systems and network

Jongho Seol, *Middle Georgia State University, jongho.seol@mga.edu*
Jongyeop Kim, *Georgia Southern University, jongyeopkim@georgiasouthern.edu*

Abstract

Quantum computing and blockchain technology are two rapidly advancing fields in modern computing. While blockchain provides decentralized trust and security, cryptography ensures data confidentiality and integrity. However, the vulnerability of traditional cryptographic algorithms to brute-force attacks by quantum computers poses a threat to existing blockchain security mechanisms. This research aims to construct a model and analyze Quantum-Secured Blockchain-based Distributed Control Systems and networks, specifically focusing on industrial plant applications and networked DCS. The methodology involves a comprehensive literature review to identify quantum-resistant algorithms, cryptographic primitives, and blockchain consensus mechanisms. These components form the foundation for designing a quantum-secured blockchain-based distributed control system model. The model incorporates crucial factors like network latency, node failures, and quantum attack scenarios to assess system availability under various conditions. Simulations are conducted using representative attack scenarios to evaluate the proposed model's performance and effectiveness. The research findings contribute to the emerging field of quantum-secured blockchain technology, shedding light on dependability challenges and opportunities. Additionally, the outcomes provide practical guidelines for developing and deploying secure and available distributed control systems and networks in the era of quantum computing.

Keywords: quantum computing, blockchain, quantum-safe, cryptography, dependability, availability, brute-force attacks

Introduction

Quantum computing (Steane, 1988; Gruska, 1999; Kaye, 2006) and blockchain technology (Yli-Huumo, 2016; Pilkington, 2016; Golosova, 2018) are two fields that have gained significant attention in recent years. Both have the potential to revolutionize the way we process information and establish trust in digital systems. While blockchain offers decentralized trust and security, cryptography (Forouzan, 2015) ensures the confidentiality and integrity of data. However, traditional cryptographic algorithms are susceptible to which could potentially break existing blockchain security mechanisms. Integrating quantum computing and blockchain technology has been a topic of increasing interest among researchers and practitioners in recent years. While blockchain technology provides decentralized trust and security, cryptographic algorithms ensure the confidentiality and integrity of data. However, the increasing power of quantum computers threatens the security of traditional cryptographic algorithms, making them vulnerable to brute-force attacks (Mosca, 2018; Mitra, 2017). As a result, the integration of quantum computing and blockchain technology offers a potential solution to this problem (Kiktenko, 2018).

Quantum computing provides new opportunities to enhance the security and privacy of blockchain technology. Quantum-safe cryptographic algorithms, which are resistant to attacks by quantum computers, are being developed to address the security challenges posed by the increasing computational power of quantum computers. These algorithms use different mathematical structures that are difficult to solve even with the computational power of quantum computers (Fernandez-Carames, 2020).

This research paper explores the potential of quantum computing in enhancing cryptography for blockchain applications, presenting an in-depth analysis of the most promising quantum-safe cryptographic algorithms and their feasibility in blockchain environments. It discusses the challenges and opportunities of integrating quantum computing with blockchain technology, outlining the benefits of a secure quantum blockchain for future applications (Brotsis, 2022). The paper also reviews the current state of the art in quantum-safe cryptography and its potential for use in blockchain technology. It provides a comprehensive overview of the most promising quantum-safe cryptographic algorithms, including hash-based, code-based, lattice-based, and multivariate cryptography. The feasibility of implementing these algorithms in blockchain applications is evaluated, considering their computational complexity and efficiency.

Furthermore, the paper discusses the challenges and opportunities of integrating quantum computing with blockchain technology. The potential benefits of using quantum-safe cryptographic algorithms (Kuang, 2022) in blockchain environments include enhanced security, privacy, and scalability. The challenges of implementing quantum-safe cryptography in blockchain technology are also discussed, including issues related to standardization, compatibility, and adoption. Overall, this research paper provides a comprehensive analysis of the potential of quantum computing in enhancing cryptography for blockchain applications. It highlights the importance of developing quantum-safe cryptographic algorithms to ensure the security and privacy of blockchain technology in the face of the increasing computational power of quantum computers. The paper concludes by outlining the potential of a secure quantum blockchain for future applications and the need for further research in this area.

The organization of this paper is as follows: The upcoming section will provide an overview of the background and literature review, followed by a section that introduces the research objectives. The subsequent sections will be arranged in the following order: contribution, modeling and analysis, results, and findings. Lastly, the paper will conclude by discussing the findings, limitations, and conclusions, with the final section dedicated to the references.

Background and Literature Reviews

In this research paper, the literature review takes a closer look at the current state of quantum computing and blockchain technology, exploring their potential impact on the field of cryptography and investigating the challenges and opportunities that arise from integrating these two technologies. The review begins by providing an overview of quantum computing, delving into its fundamental principles, current development stage, and potential applications in cryptography. From there, the focus shifts to blockchain technology, emphasizing its decentralized trust and security features and its current utilization of cryptographic algorithms. One of the key objectives of the literature review is to examine the limitations of existing cryptographic algorithms when faced with the threat of quantum computing, which poses significant risks to data security. This section meticulously analyzes the potential of quantum-safe cryptographic algorithms, such as lattice-based cryptography, hash-based cryptography, and code-based cryptography, in mitigating this challenge. The feasibility of implementing these algorithms within blockchain environments is thoroughly explored, considering aspects such as efficiency, scalability, and ease of implementation.

Furthermore, the review explores the challenges and opportunities of integrating quantum computing with blockchain technology. It highlights the benefits a secure quantum blockchain could bring to future applications and delves into the ethical implications of this integration, including concerns surrounding privacy and data sovereignty.

To provide robust analysis, the literature review draws upon existing research in quantum computing, blockchain technology, and cryptography. It scrutinizes the current state of research, identifying gaps in knowledge and pinpointing areas that warrant further investigation. Ultimately, the literature review concludes with a summary of the key findings and offers recommendations for future research endeavors in this dynamic study area. By following this structured approach, the research paper aims to comprehensively analyze the current landscape, challenges, and potential opportunities in integrating quantum computing and blockchain technology for cryptography.

Blockchain technology was first introduced in 2008 with the creation of Bitcoin, the first cryptocurrency. The technology enables decentralized trust by using a distributed ledger, which stores transactions securely and tamper-proof. Cryptography is a fundamental aspect of blockchain technology, as it provides confidentiality, integrity, and authentication of transactions. Cryptographic algorithms are used to encrypt the data and ensure that only authorized parties can access it. However, the current cryptographic algorithms used in blockchain technology are based on classical computing and are susceptible to attacks by quantum computers.

Quantum computing is a rapidly advancing field that promises to solve computational problems currently intractable for classical computers. Quantum computers use qubits, which can exist in superposition, to perform calculations much faster than classical computers. One of the major advantages of quantum computers is their ability to break classical cryptographic algorithms, potentially compromising blockchain technology's security.

Cryptography is the practice of securing communications in the presence of adversaries. One important application of cryptography is to secure online communications, such as those between a web server and a user’s device, when connecting via https. Transport Layer Security (TLS) is used to ensure secure communication between a web server (referred to as Alice) and a user’s computer (referred to as Bob) when accessing a website, starting with https. TLS employs a sequence of cryptographic operations that provide confidentiality, integrity, and authenticity of the messages being sent. Symmetric encryption is used where Alice and Bob share a secret value or key (referred to as kenc) to encrypt and decrypt the message (m) that Alice sends to Bob. They also share an authentication key (kauth) that is used to ensure the integrity and authenticity of the message using a message-authentication code (MAC). The symmetric encryption and MAC algorithms used by https are varied, and some of the MACs are built using hash functions. (Bernstein, 2017)

(Nejatollahi, et al., 2019) discusses the impact of quantum computing on classical cryptographic schemes and the need for post-quantum cryptography that can resist quantum computing threats. Lattice-based cryptography is highlighted as a promising post-quantum cryptography family, with applications in encryption, digital signature, key exchange, and homomorphic encryption. However, practical implementation requires careful design choices and tradeoffs to account for diverse computing platforms and changing standards. This work surveys recent trends in lattice-based cryptography, explores fundamental proposals, and highlights software and hardware implementation challenges. (Bernstein, 2017) cryptography is crucial for securing online communication, medical devices, and cars. However, the advent of large-scale quantum computers threatens to break many existing cryptosystems. Post-quantum cryptography addresses this issue by designing secure cryptosystems against quantum computing threats.

This emerging field has already achieved some success by identifying mathematical operations that are resistant to quantum algorithms and building cryptographic systems around them. The main challenge in post-quantum cryptography is to balance usability and flexibility with strong security guarantees.

Grover's algorithm (Long, 2001) is a quantum algorithm that provides a quadratic speed-up for searching an unordered database of size N. The algorithm is based on searching for roots of a function f, where $f(x) = 0$, and if one out of every N input is a root of f, then Grover's algorithm finds a root using only about N quantum evaluations of f on superpositions of inputs. In the context of cryptography, Grover's algorithm can be used to search for symmetric encryption keys that have been used to encrypt plaintexts '7' and '8' under a secret 128-bit AES key k, producing a 256-bit ciphertext $c = \left(AES_k(7), AES_k(8)\right)$ visible to the attacker, Grover's algorithm can find k using only about 2^{64} quantum evaluations of f (overall about 2^{86} quantum gates applied to about 3,000 qubits).

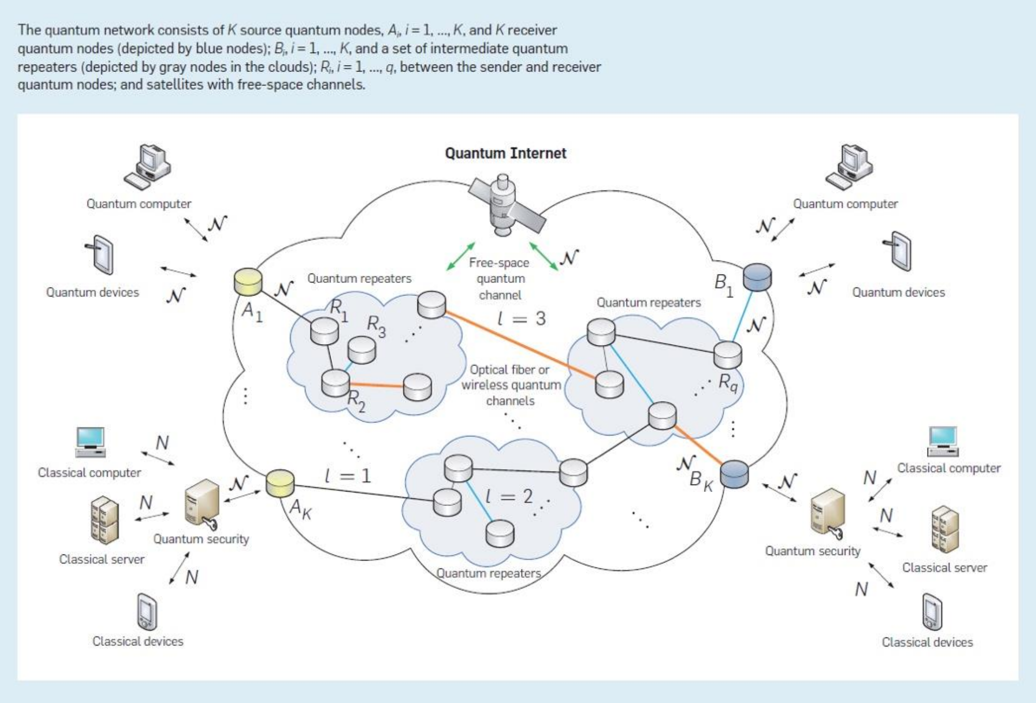
However, the physical cost of quantum database queries and the overhead of qubit operations being more expensive than bit operations may limit the practical use of Grover's algorithm. The number of serial evaluations that can be carried out in the time available is defined as T, and if N exceeds T, then Grover's algorithm cannot use fewer than $\frac{N}{T}$ evaluations spread across $\frac{N^2}{T}$ parallel quantum processors. Therefore, if qubit operations are small enough and fast enough, Grover's algorithm (Long, 2001) will threaten many cryptographic systems that aim for 2^{128} security, such as 128-bit AES keys. In this case, switching to 256-bit AES keys is recommended to ensure security. Table 1 shows examples of widely deployed cryptographic systems and their conjectured security levels. The table implies lists various public-key cryptosystems and their respective key sizes, which might make it seem like the development of quantum computers renders all public-key cryptography insecure, except for symmetric cryptography that requires larger key sizes.

Table 1: Examples of deployed cryptographic systems and their conjectured security levels (Bernstein, 2017)

Name	Function	Pre-quantum security level	Post-quantum security level
Symmetric cryptography			
$AES - 128$[8]	Symmetric encryption	128	64(Grover)
$\mathrm{AES} - 256$[8]	Symmetric encryption	256	128(Grover)
Salsa20[58]	Symmetric encryption	256	128(Grover)
GMAC[59]	MAC	128	128(no impact)
Poly1305[60]	MAC	128	128(no impact)
$\mathrm{SHA} - 256$[61]	Hash function	256	128(Grover)
$\mathrm{SHA} - 256$[62]	Hash function	256	128(Grover)
Public-key cryptography			
$\mathrm{RSA} - 3072$[1]	Encryption	128	Broken(Shor)
$\mathrm{RSA} - 3072$[1]	Signature	128	Broken(Shor)
$\mathrm{DH} - 3072$[42]	Key exchange	128	Broken(Shor)
$\mathrm{DSA} - 3072$[63,64]	Signature	128	Broken(Shor)
$256 - \mathrm{bitECDH}$[4−6]	Key exchange	128	Broken(Shor)
$256 - \mathrm{bitECDSA}$[66,67]	Signature	128	Broken(Shor)

(Al-Hazaimeh, 2013) addresses the need for (Renner & Wolf, 2023)methods due to the growing importance of information security. Although several encryption algorithms such as AES, DES, and RSA have been proposed, many encounter issues such as lack of robustness and delays in packet transmission. To enhance security goals, the paper presents a new approach for complex encrypting and decrypting data, which aims to prevent attackers from predicting patterns and improve encryption/decryption speed. The proposed approach maintains security on communication channels and makes it difficult for attackers to decipher the encrypted data.

(Renner & Wolf, 2023) explores the potential of quantum information technology to break the cycle of cryptography and cryptanalysis competition. While quantum computers have the ability to render most current public key cryptosystems insecure, the paper suggests that cryptographers will ultimately be able to prevail over cryptanalysts. The paper provides an overview of quantum cryptography, which allows for building communication schemes that rely solely on the laws of physics and minimal assumptions about cryptographic hardware, leaving little room for attack. The paper also assesses current challenges and prospects for overcoming them in the field of quantum cryptography.



The quantum network consists of K source quantum nodes, A_i, $i = 1, \ldots, K$, and K receiver quantum nodes (depicted by blue nodes); B_i, $i = 1, \ldots, K$, and a set of intermediate quantum repeaters (depicted by gray nodes in the clouds); R_i, $i = 1, \ldots, q$, between the sender and receiver quantum nodes; and satellites with free-space channels.

Figure 1: Entangled network structure of a quantum Internet. (Gyongyosi & Imre, 2022)

The network structure of Figure 1 shown below predicts future networks by complexly connecting quantum Internet to existing networks. Therefore, it can be seen as a problem how to harmonize with existing classical computers, servers, and devices with Quantum computers, devices, and network communication. As can be seen in general, the biggest problem is the possibility of quantum computing's attack on classical systems.

Diagrams and transitions shown in Figure 2 show the process of a quantum-secured blockchain, a system that can be safely protected from quantum algorithms in blockchain systems based on distributed networks that are ahead of security in existing classical systems. Therefore, to more effectively and safely protect the classical system from the quantum computing power along the quantum-secured blockchain, we will organize the most threatening algorithms and attacks in the quantum into variables and find out their reliability, safety, reliability, and dependability (Mozaffari-Kermani, 2015; Wallden, 2019) from the next section.

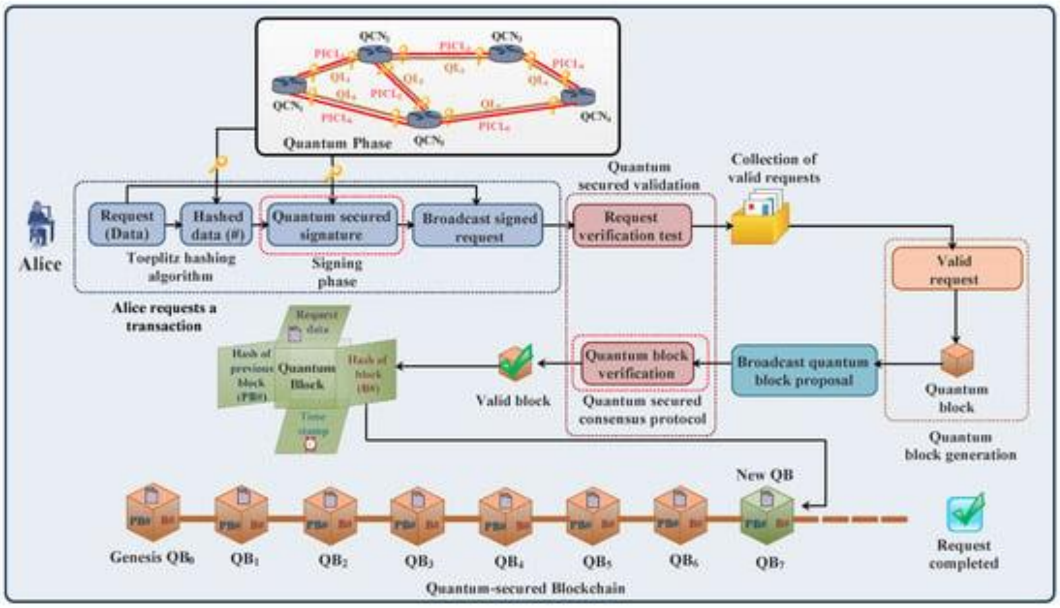

QCN
PICL
QL
Quantum Phase
Alice
Request (Data)
Hashed data (#)
Quantum secured signature
Broadcast signed request
Toeplitz hashing algorithm
Signing phase
Alice requests a transaction
Quantum secured validation
Request verification test
Collection of valid requests
Valid request
Quantum block
Quantum block generation
Broadcast quantum block proposal
Quantum block verification
Quantum secured consensus protocol
Valid block
Request data
Hash of previous block (PB#)
Quantum Block
Hash of block (B#)
Time stamp
New QB
Genesis QB₀
QB₁
QB₂
QB₃
QB₄
QB₅
QB₆
QB₇
Request completed
Quantum-secured Blockchain

Figure 2: Process of quantum-secured blockchain (Sharma, K., Balzek, Bhatia, & Prakash, 2023)

Research Objectives

The primary goal of this paper is to explore the potential impact of quantum computing on enhancing cryptography for blockchain applications. The specific objectives of this research are as follows:

1. Offer a comprehensive overview of blockchain technology, including an examination of the cryptographic mechanisms that form its foundation.
2. Investigate the limitations of classical cryptography and the potential risks posed by quantum computing to the security of blockchain systems.
3. Introduce the Quantum-Safety Blockchain-based DCS and Network (QSBDN) model and assess its feasibility within blockchain environments.
4. Analyze the challenges and opportunities related to reliability, availability, safety, and dependability in implementing the QSBDN model.
5. Highlight the advantages and benefits of a secure quantum blockchain for future applications.

By addressing these objectives, this paper aims to contribute to understanding how quantum computing can enhance cryptography in the context of blockchain technology.

Contribution

In this research, the paper explores the intersection of quantum computing and blockchain technology, which have both made significant advancements in recent years. The main focus is to investigate the potential of quantum computing in enhancing cryptography for blockchain applications. In addition, the paper recognizes the crucial role of blockchain technology in establishing decentralized trust and security, while cryptography ensures the confidentiality and integrity of data.

However, the paper sheds light on the limitations of traditional cryptographic algorithms, as they are susceptible to brute-force attacks from quantum computers. This raises concerns about the future security of existing blockchain applications and emphasizes the need for developing new cryptographic solutions. To address this, the paper extensively analyzes the most promising quantum-safe cryptographic algorithms, examining their feasibility in blockchain environments. The study compares and evaluates various quantum-safe cryptographic solutions, including lattice-based, code-based, and hash-based cryptography, to identify their strengths, weaknesses, and suitability for integration with blockchain technology. Additionally, these algorithms' performance and computational requirements are thoroughly examined, assessing their potential impact on blockchain applications.

Furthermore, the paper delves into the challenges and opportunities associated with integrating quantum computing and blockchain technology. It discusses the potential benefits of a secure quantum blockchain, such as enabling more complex smart contracts, improving consensus algorithms, and enhancing overall security and privacy. Overall, the paper's contribution to the literature lies in its comprehensive assessment of the potential of quantum computing in enhancing cryptography for blockchain applications. It emphasizes the necessity of developing quantum-safe cryptographic algorithms to ensure the long-term security of blockchain technology. Additionally, the research introduces a system/network model named QSBDN (Quantum-Secured/Safe Blockchain-based DCS and Network) as the framework used in the study.

Modeling Dependability of the QSBDN

This research employs both combinatorial modeling and Markov modeling, which involve a variety of extensive quantum attacks on blockchain technology and networks based on cryptographic algorithms and their consensus algorithms. The combinatorial model uses probabilistic techniques that calculate the smallest unit of components of the industrial plant, i.e., power plant, to evaluate the probabilistic of each power plant unit extending to a site. The site consists of several power plants or a single plant in a particular area. The Markov model uses probabilistic techniques for many complicated systems since the Markov model is easy to use in a more complex variety of systems whereas the combinatorial model is challenging to use and is suitable for expressing state transition (Johnson, 1988), it is suitable for showing the reliability/availability/safety of each site that is easy to connect with networking.

Reliability, availability, maintainability, security, safety, and testing/verification are considered to be quantified dependability (Johnson, 1988). In this research, dependability is defined as Quantum-safe/-secured/-proof/-resistant to blockchain cryptographic algorithms and systems, including traditionalism designed to remain secure even in powerful quantum computers. More fundamental countermeasures should be taken for quantum attacks, and before that, we would like to find out how to figure out the dependability through the existing quantum-safe algorithms. In order to define the success probability of a single transaction posting in a blockchain network, it is defined well-known quantum attacks e.g., the Shor's algorithm, Grover's algorithm, QKD (Quantum Key Distribution) attacks, and Quantum 51% attack. In this context, the probability of a single transaction being successfully posted into a blockchain network, P_{txn}, as shown in Equation (1) with four well-known kinds of representative quantum attack variables, P_{sa}, P_{ga}, P_{qkd}, and $P_{51\%}$. Those two variables P_{sa}, and P_{ga}, are included in the quantum algorithms.

The first one is the security broken rate by Shor's quantum computer algorithms to break the security of public-key cryptographic algorithms, such as RSA and ECC, especially to break the cryptographic signatures and encryption mechanisms used in blockchain technology and network, and the second one is the symmetric encryption algorithm, such as AES, broken rate by Grover's algorithm respectively. The rest two variables P_{qkd}, and $P_{51\%}$ are variables known as the security threat rate by Quantum Key Distribution (QKD) attacks (Lütkenhaus, 2000) ,and another one is the blockchain network attack rate by Quantum 51% attack (Kiktenko, 2018; Kearney, 2021).

The QKD itself is considered a secure protocol. Still, there are targeting vulnerable systems, and the Quantum 51% attack is a well-known threat to the blockchain network because an attacker can get the majority control power of the network's computing. An attacker with over 51% computing power in the network can manipulate transactions and create a fake fork blockchain network.

To evaluate the dependability of QSBDN, we consider a single transaction as a failure/fault to be posted into a blockchain with the representative four kinds of security threats/attacks and network attacks. The expected dependability of a single transaction is referred to as P_{txn}, can be expressed in Equation (1) as follows.

$$P_{txn} = (1 - P_{sa})^{ntc} \times \left(1 - P_{ga}\right)^{ntc} \times \left(1 - P_{qkd}\right)^{ntc} \times (1 - P_{51\%})^{ntc} \qquad (1)$$

Where,

P_{txn}: the probability of a single transaction being successfully posted into a blockchain network.
P_{sa}: the security broken rate by Shor's algorithm of quantum computing.
P_{ga}: the encryption broken rate by Grover's algorithm of quantum computing.
P_{qkd}: the security threat rate by QKD.
$P_{51\%}$: the 51% attack rate in blockchain networks by quantum 51% attack.
ntc: number of transactions being created in a blockchain network. (Approximately 15,000)

We can calculate a result of P_{txn} when each kind of quantum computing attack has a 0.0001 (0.01% each) rate with the number of transactions being created in the blockchain network. The probability of a transaction failure P_{qf} can be expressed in the following Equation (2).

$$P_{qf} = (1 - P_{txn})^{ntp} \times (1 - P_{net}) \qquad (2)$$

Where,

P_{qf}: the probability of transaction failure by any quantum attacks.
P_{txn}: the probability of a single transaction being successfully posted into a blockchain network.
P_{net}: the probability of the blockchain network being successful (not any other attacks found except 51% attack).
ntp: number of transactions being posted into a blockchain network.

The graph shown in Figure 1 shows the state that changes as the created Txn increases the failure rate of the QSBDN system linked thereto according to the value of P_{txn}. The QSBDS system failure rate remains highest than others, that is, P_{txn} is 0.0024, which is the lowest state for Txn to be successfully posted than others P_{txn} 0.003, 0.004, and 0.005, meaning that the threat of P_{sa}, P_{ga}, P_{qkd}, and $P_{51\%}$ remains relatively higher at 0.0001 (0.01% rate) respectively.

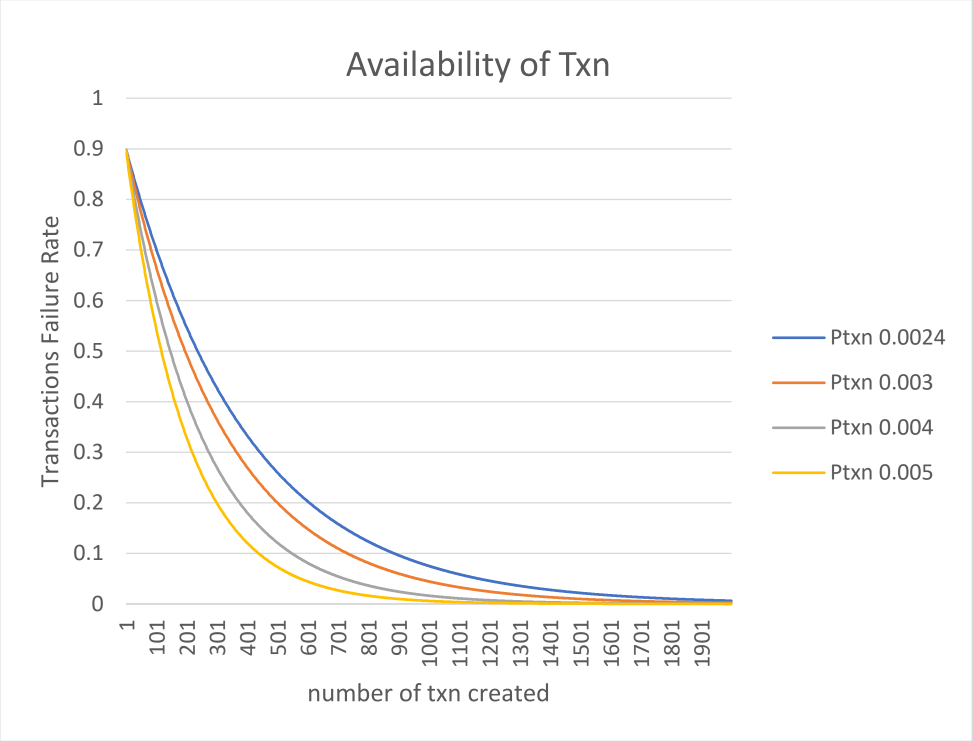


Figure 1: Availability of Txn

The following Equation (3) expresses the dependability of a QSBDN. As the number of transactions posted among the total number of transactions created into the blockchain network increases, it calculates P_{qf} the probability of transaction failure by any quantum attacks.

$$P_{d_{qsbdn}} = \sum_{i=0}^{n} C(n,i) {P_{qf}}^{i} \left(1 - P_{qf}\right)^{n-i} \tag{3}$$

Where,
$P_{d_{qsbdn}}$: dependability of a QSBDN.
n: number of transactions created in the blockchain network but not posted into the blockchain network yet.
i: number of transactions posted into the blockchain network.

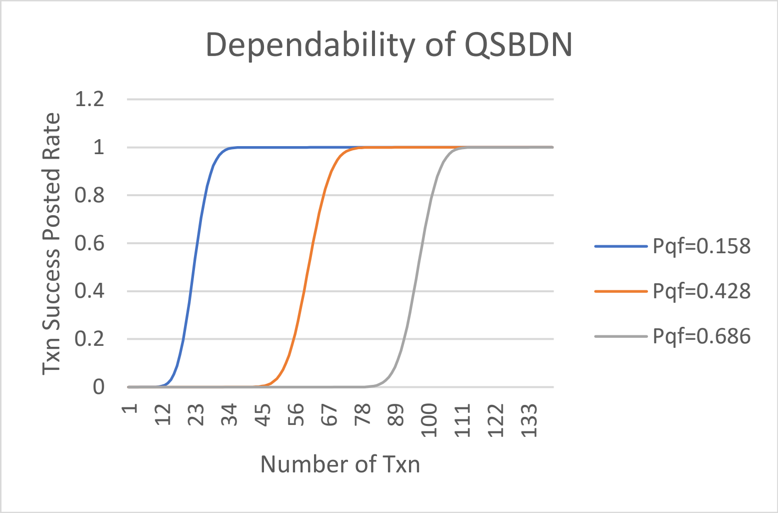


Figure 2: Dependability of QSBDN

The graph shown in Figure 2 plots three different transaction success posted rates as the number of transactions increases as P_{qf}, 0.158, 0.428, and 0.686 as lowest, medium, and highest, respectively. The lowest P_{qf} value indicates that the transaction success rate is full as earliest as the number of transactions among them. Transaction success posted rate is full at the number transaction 33 for P_{qf}, 0.158 as the fastest, whereas the transaction success posted rate comes full at the number transaction 105 for P_{qf}, 0.686 as the slowest among them.

In order to evaluate the dependability of multiple QSBDN model sites, we consider a single dependability of a QSBDN, $P_{d_{qsbdn}}$ in Equation (3). In the Markov model, whereas in the combinatorial model, two main key points are to be considered: the system state and the state transition.

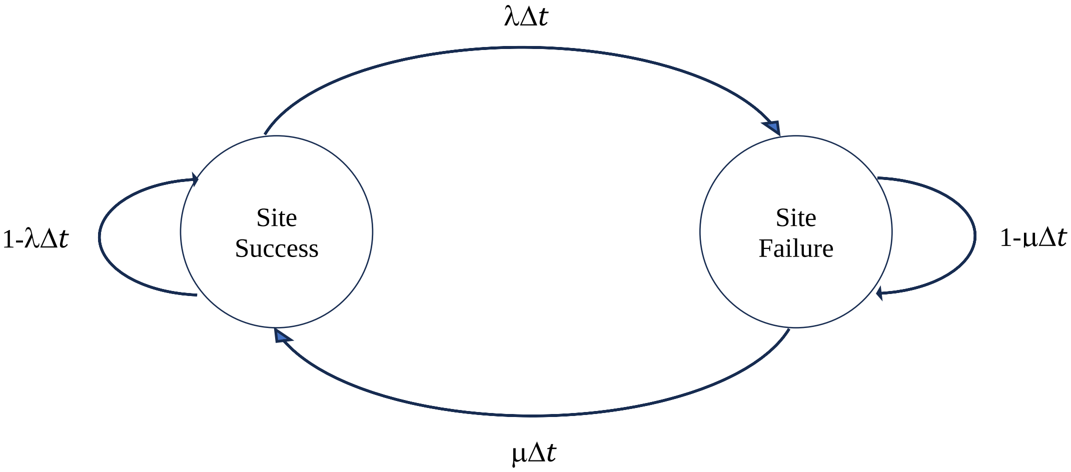


Figure 3: A State Diagram of a Site Availability

Figure 3 shows a state diagram of a site availability that is based on the QSBDN model. It assumed that a site has a failure rate (λ) and a repair rate (μ), those variables rates are followed to the quantum-secured blockchain algorithm. The equation of the site availability model can be expressed in Equation (4) and (5).

$$P_{ss}(t+\Delta t) = (1-\lambda\Delta t)P_{ss}(t) + \mu\Delta t P_{sf}(t) \tag{4}$$
$$P_{sf}(t+\Delta t) = (1-\mu\Delta t)P_{sf}(t) + \lambda\Delta t P_{ss}(t) \tag{5}$$

Where,
P_{ss}: the probability of a site's success.
P_{sf}: the probability of a site failure.
λ: the failure rate.
μ: the repair occurring rate.
Δt: time interval for a probability of failure or success

In order to express the site availability simplified Equations (6) and (7), we consider the time interval for a probability of events (success or failure) taking the limit as Δt approaches zero in the differential equations, taking Laplace transforms and inverse Laplace transform it (Johnson, 1988).

$$P_{ss}(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \tag{6}$$
$$P_{sf}(t) = \frac{\lambda}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \tag{7}$$

Where,
e: taking the approximate value 0.000023 in the simulation.
λ: the failure rate, taking the value 0.005.
μ: the repair occurring rate, taking three values 0.0001, 0.005, and 0.015.

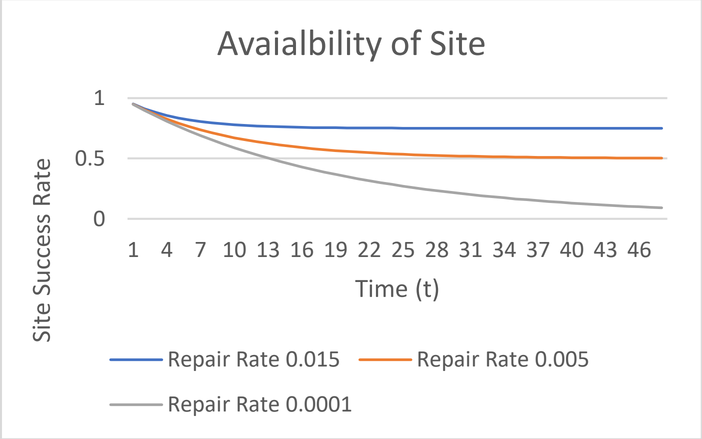


Figure 4: Availability of Site against Time with Repair Rate (μ)

As shown in Figure 4 above, the site success rate decreases over time, and when the repair rate is the highest at μ=0.015, it remains below 0.8 very gently, and when the repair rate is the lowest μ=0.0001, it shows a graph that falls very sharply.

The following Equation (8) shows the dependability of network Grid sites.

$$P_{d_{gridsite}} = \sum_{i=k}^{n} C(n,i){P_{sf}}^{i}\left(1 - P_{sf}\right)^{n-i} \tag{8}$$

Finally, the dependability of the Grid site to be checked is confirmed as the number of sites included in the Grid network increases using P_{sf} in the equation shown above. As shown in Figure 5, it shows the dependability of site-grid as increasing the number of sites with three different P_{sf} rate i.e., 0.95, 0.75, and 0.5. As an important impact variable, if the value of P_{sf}=0.95 is relatively large, the site grid success rate improves when the number of site is 90, whereas if the P_{sf}=0.5 is relatively low, the site grid success rate increases from the number site around 40.

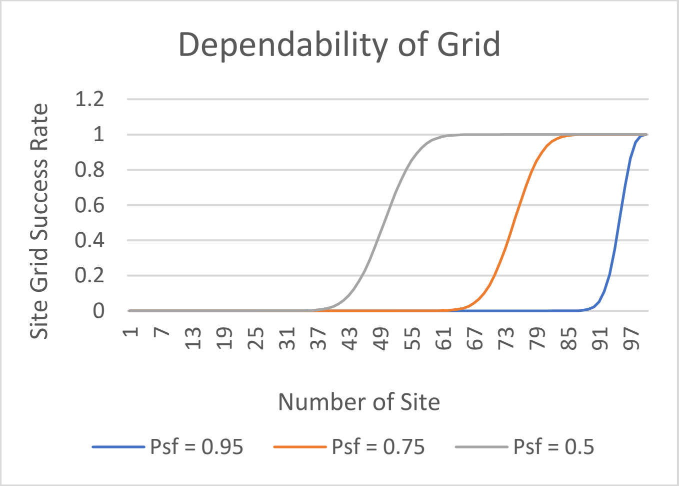


Figure 5: Dependability of Site-Grid against number of Site with $\boldsymbol{P_{sf}(t)}$

Results and Findings

The modeling simulation results demonstrate a significant threat to the security of current blockchain technology posed by quantum computing. However, a potential solution to this issue is found in the development of quantum-safe cryptographic algorithms-based modeling. The simulation reveals that quantum attacks not only disrupt individual transactions but also diminish the overall availability of the blockchain system. Moreover, these attacks possess the capability to manipulate the network and render any single site inoperable, thereby impacting dependability, even when connected to the entire network. The modeling confirms that creating a grid site through network connectivity can have severe consequences.

To address these challenges, several quantum-safe cryptographic algorithms, such as lattice-based, code-based, and hash-based cryptography, have been proposed. These algorithms are viable options for implementation in blockchain environments and offer a higher security level than traditional cryptographic algorithms. Integrating quantum computing with blockchain technology presents numerous opportunities, including improved efficiency, scalability, and privacy.

Discussion of Findings

This research paper aims to explore the intersection of quantum computing and blockchain technology, two rapidly evolving fields in computing. While blockchain offers decentralized trust and security, cryptography ensures data confidentiality and integrity. However, traditional cryptographic algorithms are vulnerable to brute-force attacks by quantum computers, which could break the security mechanisms of existing blockchains. The paper aims to address this issue by investigating the potential of quantum computing to enhance cryptography for blockchain applications. It presents an analysis of the most promising quantum-safe cryptographic algorithm-based QSBDN and their feasibility in blockchain environments. The paper also discusses the challenges and opportunities of integrating quantum computing with blockchain technology, outlining the potential benefits of a secure quantum blockchain for future applications.

The paper reviews several promising quantum-safe cryptographic algorithms, such as lattice-based cryptography, code-based cryptography, hash-based cryptography, and multivariate cryptography. The paper also explores the challenges of integrating quantum computing with blockchain technology, such as the need for secure quantum distribution and the potential impact on blockchain consensus mechanisms.
Overall, the paper provides a comprehensive overview of the potential of quantum computing in enhancing cryptography for blockchain applications. It highlights the need for further research and development in this area to address the challenges and opportunities of this emerging technology. The paper concludes by outlining the potential benefits of a secure quantum blockchain, such as enhanced privacy, scalability, and security, for future applications in fields such as finance, healthcare, and supply chain management.

Limitations

This paper serves as a foundation for anticipating the advent of quantum computing and proposing measures to prepare for its impact, even in the context of existing distributed peer-to-peer (p2p) communication security technology, such as blockchain. Given the current limitations in experimenting with quantum computing power, quantitative evaluation methods were employed to assess the system's dependability in terms of reliability, safety, and availability. Nevertheless, it is crucial to thoroughly examine all quantum attacks/threats and determine how to accurately model their characteristics and functional threats, which remains an area for future research.

Conclusions

In conclusion, this paper emphasizes the potential of quantum computing in enhancing cryptography for blockchain applications. The development of quantum-safe cryptographic algorithms provides a solution to the threat posed by quantum computing to blockchain security. Integrating quantum computing with blockchain technology also brings increased efficiency, scalability, and privacy opportunities. The rapid progress of quantum computing and blockchain technology has the capacity to revolutionize secure information storage and exchange. While blockchain offers a decentralized and secure platform, traditional cryptographic algorithms that safeguard data confidentiality and integrity are vulnerable to quantum computer attacks. Therefore, exploring the potential of quantum computing in enhancing cryptography for blockchain applications is crucial.

This paper conducts a comprehensive analysis of the most promising quantum-safe cryptographic algorithms and evaluates their feasibility in blockchain environments. We discuss the challenges and opportunities of integrating quantum computing with blockchain technology, as well as the advantages of a secure quantum blockchain for future applications. The analysis reveals that quantum computing can significantly enhance the security of blockchain technology, but integrating the two fields also presents substantial challenges.

Adapting existing blockchain networks to accommodate quantum-safe cryptographic algorithms would necessitate significant infrastructure changes. Furthermore, the scalability and efficiency of quantum computers must be improved for practical implementation in blockchain applications. Despite these challenges, the integration of quantum computing and blockchain technology offers tremendous opportunities to revolutionize data storage and exchange security.

The future of blockchain technology will rely on the integration of quantum computing, and this research underscores the need for further exploration in this exciting research area. Addressing these challenges and fully realizing the potential of a secure quantum blockchain requires additional research.

References

Al-Hazaimeh, O. (2013). A New Approach for Complex Encrypting and Decrypting Data. *International journal of Computer Networks & Communications*, 95-103.

Bernstein, D. (2017). Post-quantum cryptography. *Nature*, 188-194.

Brotsis, S., Kolokotronis, N., & Limniotis, K. (2022). Towards post-quantum blockchain platforms. *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*, 106-30.

Fernandez-Carames, T. M.-L. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, 8.

Forouzan, B. A. (2015). Cryptography and network security . *Mc Graw Hill Education (India) Private Limited.*

Golosova, J. &. (2018). The advantages and disadvantages of the blockchain technology. *IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.

Gruska, J. (1999). *Quantum computing.* London: McGraw-Hill.

Gyongyosi, L., & Imre, S. (2022). Advances in the Quantum Internet. *Communications of the ACM*, 52-63.

Johnson, B. W. (1988). *Design & analysis of fault tolerant digital systems.* Addison-Wesley Longman Publishing Co., Inc..

Kaye, P. R. (2006). *An introduction to quantum computing.* Oxford: OUP.

Kearney, J. J.-D. (2021). Vulnerability of blockchain technologies to quantum attacks. *Array*.

Kiktenko, E. O. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, 3.

Kuang, R. &. (2022). Quantum permutation pad for universal quantum-safe cryptography. *Quantum Information Processing*.

Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Physical Review A*.

Long, G. L. (2001). Grover algorithm with zero theoretical failure rate. *Physical Review A*.

Mitra, S. J. (2017). Quantum cryptography: Overview, security issues and future challenges. *4th International Conference on Opto-Electronics and Applied Optics* (pp. 1-7). IEEE.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: will we be ready? *IEEE Security & Privacy*, 38-41.

Mozaffari-Kermani, M. &. (2015). Reliable hash trees for post-quantum stateless cryptographic hash-based signatures. *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)* (pp. 103-108). IEEE.

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-Quantum Lattice-Based Cryptography Implementations: A Survey. *ACM Computing Survey*, 41.

Pilkington, M. (2016). Blockchain technology: principles and applications. *Edward Elgar Publishing*, 225-253.

Renner, R., & Wolf, R. (2023). Quantum Advantage in Cryptography. *AIAA Journal*, 1-16.

Sharma, P., K., K., Balzek, P., Bhatia, V., & Prakash, S. (2023). Securing Optical Networks Using Quantum-Secured Blockchain: An Overview. *Sensors* .

Steane, A. (1988). Quantum computing. *Reports on Progress in Physics*, 117.

Wallden, P. &. (2019). Cyber security in the quantum era. . *Communications of the ACM*, 120-120.

Yli-Huumo, J. K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, 11.