applied sciences

IMPACT FACTOR 2.5

CITESCORE 5.5

Article

Asynchronous Quantum-Resistant Blockchain for Secure Intelligence Sharing

Yun-Yi Fan, Chit-Jie Chew and Jung-San Lee

Special Issue
Advances in Quantum-Enabled Cybersecurity

Edited by
Prof. Dr. Nuno Silva and Dr. Mariana Ferreira Ramos

MDPI

https://doi.org/10.3390/app15115921

applied sciences

MDPI

Article

Asynchronous Quantum-Resistant Blockchain for Secure Intelligence Sharing

Yun-Yi Fan [1], Chit-Jie Chew [1,2] and Jung-San Lee [1,3,*]

[1] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407102, Taiwan; a19990101152@gmail.com (Y.-Y.F.); cjie723@gmail.com (C.-J.C.)
[2] AAA Security Technology Co., Ltd., Taichung 407037, Taiwan
[3] Cybersecurity Technology Institute, Institute for Information Industry, Taipei 106214, Taiwan
* Correspondence: leejs@fcu.edu.tw

Abstract: By aggregating intelligence on emerging threats, attack techniques, and vulnerabilities, organizations can establish a more comprehensive threat landscape awareness and proactively identify potential risks. However, in the process of sharing threat intelligence, companies often hesitate due to concerns over information leakage, which reduces their willingness to collaborate. Furthermore, the lack of transparency and credibility in intelligence sources has negatively impacted the quality and trustworthiness of shared data. To address these issues, authors aim to leverage blockchain technology, utilizing its decentralized and tamper-proof properties to ensure corporate privacy and the reliability of intelligence sources. Additionally, a dual blockchain architecture is implemented to enhance operational efficiency and reduce storage burdens. However, with the advent of large-scale quantum computing, traditional cryptographic mechanisms used in blockchain systems face potential vulnerabilities due to Shor's algorithm, which threatens widely adopted public key cryptographic schemes. To ensure long-term security and resilience in a quantum-enabled threat landscape, quantum-resistant cryptographic technologies, including SPHINCS+ and CRYSTALS-KYBER, are integrated to facilitate quantum-safe migration in blockchain applications, ensuring system security and resilience in future environments of quantum computing.

Keywords: post-quantum migration; threat intelligence; asynchronous blockchain

Academic Editors: Nuno Silva and Mariana Ferreira Ramos

Received: 16 April 2025
Revised: 16 May 2025
Accepted: 19 May 2025
Published: 24 May 2025

Citation: Fan, Y.-Y.; Chew, C.-J.; Lee, J.-S. Asynchronous Quantum-Resistant Blockchain for Secure Intelligence Sharing. *Appl. Sci.* **2025**, *15*, 5921. https://doi.org/10.3390/app15115921

1. Introduction

Sharing threat intelligence data is essential in a contemporary, interconnected digital landscape where cyber threats evolve rapidly and pose significant risks to organizations and individuals alike. By pooling together data on emerging threats, attack techniques, and vulnerabilities, organizations can gain a comprehensive understanding of the threat landscape and identify potential risks early on.

According to a Ponemon Institute report [1], high-performing companies are often willing to share intelligence than other companies. The report highlights the collaborative benefits of shared threat intelligence in enhancing cybersecurity posture and reducing risk. Moreover, government agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) in the United States, actively promote threat intelligence sharing among public and private sector organizations. Through programs like the Automated Indicator Sharing (AIS) [2], participating organizations can exchange actionable threat indicators in real time, enabling them to strengthen their cyber defenses and respond to emerging threats more effectively.

However, when the source of intelligence information is unclear, it may lead to problems with quality and content. Research by Omar Al-Ibrahim et al. [3] also pointed out that the current intelligence information focuses on quantity rather than the quality of information. Furthermore, organizations may engage in the sharing community with opportunistic motives, such as minimal contribution or exploiting the intelligence provided by others, leading to free-riding behavior. Therefore, the tamper-proof information sharing process and contributing members are important issues for information sharing.

Blockchain as a tamper-proof and decentralized storage technology has gained lots of attention recently. Along with well-known cryptocurrencies, non-fungible tokens (NFTs) have also made frequent appearances in various reports and news. For instance, in December 2021, an NFT artwork created by the artist Pak was sold for a staggering $91.8 million [4]. This event brought blockchain applications into the global spotlight, with widespread adoption in not only the financial sector but also in enterprises [5], healthcare [6], and the legal system [7]. Additionally, countries worldwide are actively seeking international patents related to blockchain [8], with China and the United States leading the way, having filed nearly 55,000 patents as of June 2021. This highlights the international significance of blockchain as an indispensable, decentralized data storage technology.

Nevertheless, the emergence of quantum computing poses a threat to most public key algorithms used today, as established by major international companies such as Microsoft and Google. These research have demonstrated the potential impact of quantum computing on current cryptographic techniques [9,10]. Therefore, it has become imperative to replace national critical infrastructure with post-quantum algorithms, prompting the National Institute of Standards and Technology (NIST) to initiate a competition for post-quantum cryptography standards. Recognizing the escalating risks posed by advancements in quantum computing, the National Institute of Standards and Technology (NIST) has undertaken a comprehensive initiative to standardize post-quantum cryptographic (PQC) algorithms. As of August 2024, NIST has finalized its initial set of encryption standards designed to withstand quantum computer-based cyberattacks. The primary standard for general encryption is based on the CRYSTALS-KYBER algorithm, now referred to as ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism). For digital signatures, NIST has standardized two algorithms: ML-DSA (Module-Lattice-Based Digital Signature Algorithm), derived from the CRYSTALS–Dilithium algorithm, and SLH-DSA (Stateless Hash-Based Digital Signature Algorithm), based on the SPHINCS+ algorithm. In March 2025, NIST selected the HQC (Hamming Quasi-Cyclic) algorithm as an additional post-quantum encryption standard, serving as a backup to ML-KEM due to its reliance on different mathematical foundations. As quantum computing technology continues to progress, migrating blockchain systems to these standardized post-quantum cryptographic mechanisms is essential to ensure long-term security.

Aside from quantum threats, there exist other concerns related to blockchain technology, such as efficiency and the substantial consumption of computational resources. Blockchain generates a new block approximately every ten minutes, resulting in delayed data storage efficiency. Moreover, the proof-of-work (PoW) consensus mechanism used to mine new blocks requires nodes to compete for mining rights. The node that successfully solves the cryptographic puzzle first receives the reward, with nodes possessing higher computational power having a greater likelihood of winning. However, other nodes still expend computational resources despite having a nonzero probability of finding a valid solution. This inefficiency and wastage of computational resources present significant challenges in blockchain research.

To address these issues, we aimed to design Asynchronous Quantum-Resistant Blockchain for Secure Intelligence Sharing (AQRB), adopting the concepts of the SPHINCS+,

CRYSTALS-KYBER, and the dual blockchain to tackle quantum computing, blockchain efficiency, and computational power problems. Based on the PQCRYPTO project endorsed by the European Union [11] and NIST, AQRB picks the SPHINCS$^+$ algorithm as the post-quantum digital signature algorithm and CRYSTALS-KYBER for constructing AQRB. In conjunction with the implementation of a dual blockchain to tackle efficiency challenges, the new research utilizes the Libra [12] blockchain framework to achieve the following objectives:

- Quantum-resistant computation: All data stored on the blockchain remains secure and immune to quantum computing attacks or tampering.
- Data storage efficiency: Reduces synchronization delays by enabling an asynchronous transaction validation mechanism.
- Blockchain network balance: Encourages fair participation of nodes in the consensus process to prevent computational power centralization.

The rest of this research is organized as follows: Section 2 presents the literature review covering prior work. Section 3 provides a review and discussion of the relevant literature. Section 4 outlines the methodology of this research, detailing the system design, cryptographic integration, and threat model assumptions. Section 5 presents the results of the experiments, including performance benchmarks and implementation metrics. Section 6 provides security analyses, addressing confidentiality, integrity, and quantum resilience. Finally, Section 7 concludes the contributions of AQRB and outlines future research directions.

2. Literature Review

Recent advancements in quantum computing have intensified the urgency to develop blockchain systems resilient to quantum attacks. In response, researchers have begun to explore how blockchain architectures can be enhanced or redesigned to withstand the cryptographic threats posed by quantum algorithms. This section provides a review and comparative analysis of recent developments in this area. Section 2.1 presents an overview of the current research landscape surrounding post-quantum blockchain systems. Section 2.2 provides a comparative evaluation of representative blockchain studies based on five essential system-level features: data security, resistance to quantum computing attacks, lightweight storage burden, consensus efficiency, and sustainable maintenance.

2.1. Post-Quantum Blockchain Development Trends and Challenges

A systematic survey, such as Yang et al. [13], provided detailed comparisons between post-quantum and quantum blockchains, examining architectural, security, and performance trade-offs. Their findings suggest that while quantum blockchain technologies are rapidly evolving and hold significant potential, post-quantum blockchains continue to play a critical complementary role and cannot be entirely replaced by quantum blockchains. Subsequently, Parida et al. [14] highlighted foundational concepts and initial approaches in post-quantum-distributed ledger technologies. Their study also underscored key challenges, including high implementation costs and scalability limitations, indicating that several issues within post-quantum blockchain systems remain to be addressed.

On the other hand, Baseri et al. [15] focused on security risk assessment and migration strategies in the quantum era. They emphasized that failing to replace traditional cryptographic foundations before the arrival of quantum advantage could expose blockchain systems to systemic vulnerabilities. To address this, they proposed a "progressive migration strategy" that advocates the use of hybrid signature schemes and modular blockchain architectures, aiming to strike a balance between backward compatibility and quantum resistance.

2.2. Comparative Analysis of System-Level Features in Blockchain Architectures

To explore the practical applicability and long-term scalability of blockchain systems, this study reviewed and compared five critical system characteristics: data security, resistance to quantum computing attacks, lightweight storage burden, consensus efficiency, and sustainable maintenance. Data security refers to the system's ability to protect the integrity, immutability, and confidentiality of transaction data. It is a foundational pillar of blockchain design. Resistance to quantum computing attacks evaluates the system's cryptographic robustness against future quantum threats, which are capable of breaking classical encryption algorithms. Lightweight storage burden focuses on minimizing the cost of data synchronization and storage between nodes, which are especially important in environments like IoT or mobile devices. Consensus efficiency relates to transaction throughput, latency, and energy consumption—key indicators of blockchain scalability and performance. Finally, sustainable maintenance concerns the system's ability to maintain secure and efficient long-term operation without performance degradation. A comparison of the three representative studies is conducted based on the five aforementioned features, as shown in Table 1.

Table 1. Literature comparison table.

Feature/Literature	[16]	[17]	[18]
Data Security	✔	-	✔
Lightweight Storage Burden	✔	✘	✘
Consensus Efficiency	✔	-	✘
Quantum Resistance	✘	✘	✔
Sustainable Maintenance	✘	✘	✘

Note: ✔ indicates achieved, ✘ indicates not achieved, - indicates not mentioned.

Zheng et al. [16] proposed the Meepo architecture, a multi-execution and sharding framework for consortium blockchains designed to enhance cross-organizational scalability and efficiency. In terms of data security, Meepo supports isolated execution environments and private channels for each organization, effectively enabling data separation and access control. For storage burden, the sharding mechanism reduces the volume of data each node must store and synchronize, achieving significant optimization. Consensus efficiency is improved through the use of localized consensus mechanisms that reduce global synchronization, thereby enhancing transaction processing performance. However, while Meepo offers modular deployment, it lacks a systematic approach for ensuring long-term performance stability and operational integrity, and thus falls short in achieving sustainable maintenance. Additionally, quantum resistance is not addressed, as the system still relies on traditional cryptographic methods.

Mollah et al. [17] conducted a comprehensive survey on the application of blockchain in smart grid systems, highlighting its potential roles and technical challenges. In terms of data security, the study emphasizes blockchain's role in ensuring transparency and immutability of energy transaction data, thus enhancing trust, but lacks detailed analysis of cryptographic mechanisms. On quantum resistance, although the article mentions the potential threat of quantum computing, it provides no specific technical design or mitigation strategy. Regarding storage and maintenance, it identifies limitations in resource-constrained IoT nodes but does not propose concrete architectural solutions. Consensus efficiency is discussed theoretically, with references to consensus mechanisms like PBFT and PoW in smart grid contexts yet lacks experimental validation. Sustainable maintenance is discussed conceptually, with emphasis on decentralized governance and autonomy in

energy systems, but without architectural or procedural frameworks to ensure long-term maintainability.

Fernández-Caramés and Fraga-Lamas [18] focused on the emerging security threats of quantum computing to blockchain systems, making this study one of the earliest to explore post-quantum blockchain technologies in depth. In terms of data security, they emphasized the importance of cryptographic mechanisms and compared various post-quantum cryptographic (PQC) schemes for securing transaction data. Regarding quantum resistance, this study is the only one among the three to conduct a comprehensive technical review, examining the advantages and limitations of lattice-based, hash-based, and code-based schemes. In terms of storage burden, the authors noted that most PQC schemes result in significantly larger signature sizes, increasing storage and transmission costs and posing practical implementation challenges. Consensus efficiency is negatively impacted by the computational demands and verification delays of post-quantum signatures, limiting performance under current conditions. Sustainable maintenance is also not achieved, as the authors state that the lack of standardization and the complexity of PQC deployment present serious barriers to long-term operational viability.

3. Preliminary

The background knowledge of this research is introduced in this section. The components of SPHINCS$^+$ are described in Section 3.1, the content of CRYSTALS-KYBER is explained in Section 3.2, while the structure and characteristics of blockchain and dual blockchain are displayed in Sections 3.3 and 3.4, respectively.

3.1. SPHINCS$^+$

SPHINCS+ represents the first hash-based digital signature scheme selected by the National Institute of Standards and Technology (NIST) as part of its post-quantum cryptographic standards, originally introduced by Hulsing et al. [19]. Its primary advantage lies in eliminating the need to record the state of previously utilized signatures, inherently enhancing security against quantum adversaries. The SPHINCS+ structure mainly comprises three distinct components. The Forest of Random Subsets (FORS) operates as a few-time signature mechanism built upon multiple tree structures to effectively mitigate the probability of signature repetition and guard against forgery or replay attacks. The Winternitz One-Time Signature (WOTS+) serves as a one-time signature mechanism that generates public keys via iterative hash computations, linking FORS with the subsequent Extended Merkle Signature Scheme (XMSS). Finally, XMSS, an extension of the traditional Merkle tree methodology, constitutes the core hierarchical framework that systematically coordinates the signature generation process within SPHINCS+.

3.2. CRYSTALS-KYBER

CRYSTALS-KYBER, designed by Schwabe et al. [20]. and adopted as the sole post-quantum public key encryption and keyestablishment algorithm by NIST, relies fundamentally on the computational difficulty associated with the Learning with Error (LWE) problem. Its efficiency stems significantly from employing the Number Theoretic Transform (NTT) for polynomial multiplications, effectively reducing computational complexity from $O(n^2)$ to O(nlogn). In the key generation phase, a random matrix A, a secret vector s, and an error vector e are generated, enabling computation of the public key through the equation $b = As + e$. Encryption processes involve the sender computing polynomial values based on the recipient's public key and additional randomly selected vectors and error terms, embedding the message within the ciphertext. Subsequently, the recipient employs the corresponding private key to decrypt the ciphertext and successfully recover the original

message. The rigorous mathematical underpinning, computational efficiency, and robust protocol design collectively underscore CRYSTALS-KYBER's significance as a standard for secure cryptographic communications in the emerging quantum computing context.

3.3. Blockchain

Blockchain technology constitutes a decentralized, cryptographically secured data storage mechanism characterized by immutability, transparency, and traceability of recorded information. Within blockchain networks, participants collaboratively manage and verify transactional data, thereby ensuring integrity and accuracy without reliance on centralized authority. Upon initiation, transactions undergo digital signing procedures and are subsequently broadcasted across the network for validation by participating nodes. Miners assume responsibility for verifying and compiling these pending transactions into blocks, subsequently engaging in consensus mechanisms involving computationally intensive Proof-of-Work (PoW) algorithms. Miners competitively perform calculations, and the participant who successfully completes the required PoW computations first earns the privilege of adding the newly created block to the blockchain ledger. Following block dissemination, network nodes collectively validate the accuracy and legitimacy of transactions contained within the newly added block. Upon successful validation, the blockchain ledger is updated to reflect this addition, thereby sustaining a secure, decentralized, and transparent information management framework.

3.4. Dual Blockchain

In actuality, it takes a lot of time to synchronize block content to each node in the blockchain. Also, the original reputation value mechanism in the blockchain system is often designed to resist sybil attacks with high-cost computing. However, the lack of reward mechanism easily causes the application of blockchain systems to be inactive or even decline. In order to solve the above problems, Wu et al. [21] have introduced the design of a dual blockchain to allow nodes to only save information related to themselves. Specifically, a reputation value system with reward feedback is built up to maintain the block. The operation within the chain could be balanced to avoid uneven resources. As shown in Figure 1, each user has two chains, namely the transaction chain and the verification chain.

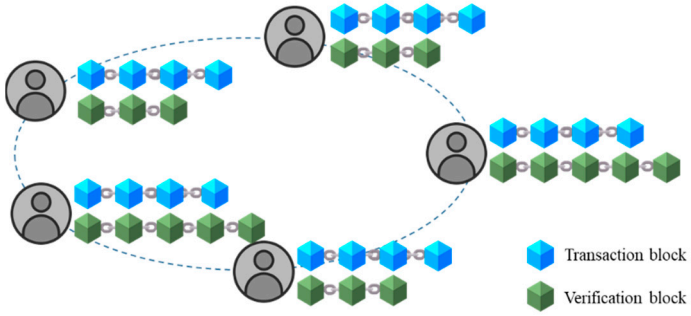


Figure 1. Dual blockchain architecture diagram.

The flowchart of the dual blockchain is shown as Figure 2. First, the private key SK is processed through RSA to generate public key PK, and PK is manufactured through the hash function to lay out the wallet address. When a transaction occurs, the buyer calculates the transaction information, before signing and broadcasting it to the blockchain. Finally, it is handed over to the verifier for transaction verification.

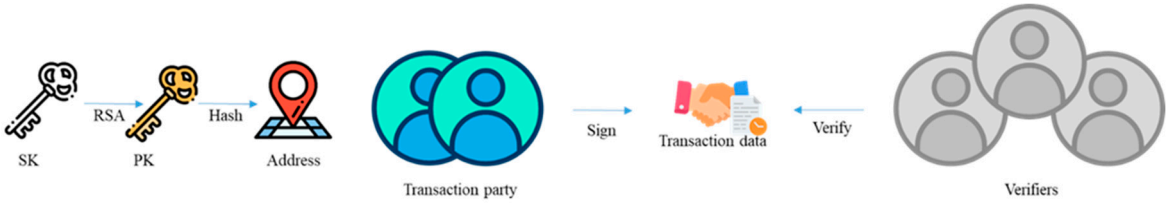


Figure 2. Dual blockchain flowchart.

4. The Proposed Method

The flowchart of the AQRB is shown in Figure 3, including three phases: building, sharing, and transactions. In the building phase, the post-quantum algorithm SPHINCS$^+$ and CRYSTALS-KYBER are introduced to generate the keys and addresses in blockchain. In the sharing phase, it explains the process of sharing and storing. The verifying phase illustrates how to verify the data and reputation in blockchain. After that, the data in the blockchain is uploaded by users. Finally, the transaction process is set when users propose the requirement. Notations used in the article are defined in Table 2.

Table 2. Notation table.

Notation	Illustrate
i	User i
P	Data provider
M	Data maintainer
B	Data buyer
$address_i$	Address of user i in the blockchain
$H()$	Hash function
$Enc()$	Encrypt function
$Sig()$	Signature function
SPK_i	Public key of user i in the blockchain
SSK_i	Private key of user i in the blockchain
PK_i	Public key of encrypting user i sharing intelligence
SK_i	Private key of decrypting user i sharing intelligence
TH	Transaction block header
VH	Verification block header
$BPTH$	Previous transaction block header of buyer
$SPTH$	Previous transaction block header of provider
$match$	Competitiveness
rew	Reward
rep	Reputation
tx	Transaction information
$proof$	Verify information
$Data$	Broadcast information
txt	Threat intelligence

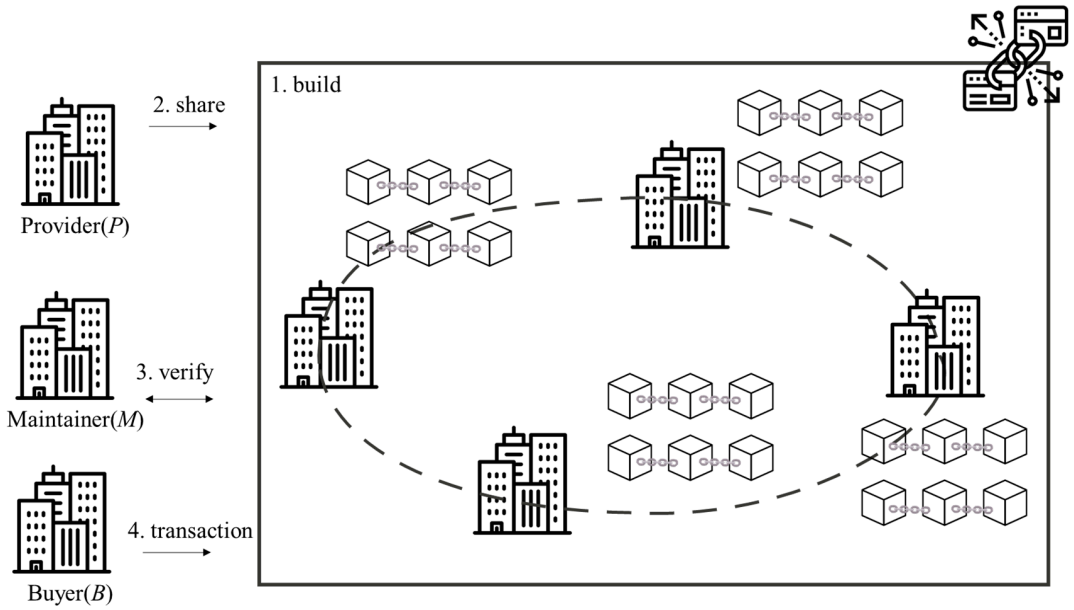


Figure 3. AQRB flowchart.

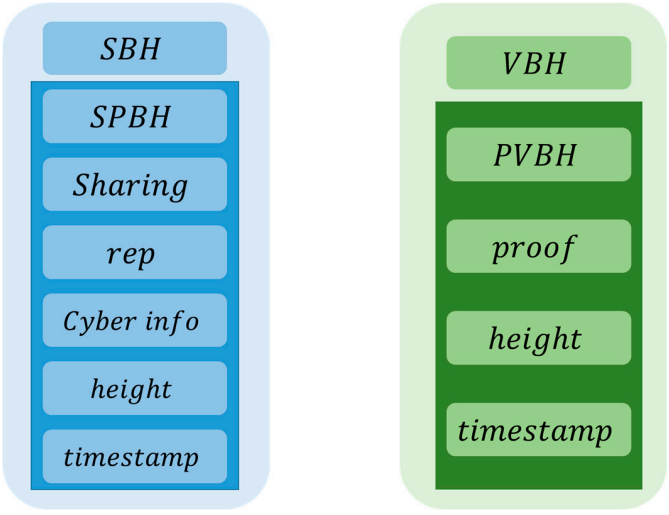
4.1. Building Phase

In the building phase, it delineates two key components; Section 4.1.1 introduces the block content within the dual blockchain framework, while Section 4.1.2 predominantly describes the key and address generation.

4.1.1. Block Content

This segment is depicted in Figure 4, showcasing the dual blockchain with contents, comprising two distinct chains: information chains and verification chains. The pertinent description is outlined below:

- Information chain: the content of the information chain is shown in Figure 4a, including sharing block header (SBH), previous sharing block header $(SPBH)$, $Sharing$, $height$, $Cyber\ Info$, rep_P, and $timestamp$.
- Verification chain: the content of the verification chain is shown in Figure 4a, including verification block header (VBH), previous verification block header $(PVBH)$, $height$, $proof$, and $timestamp$.



(**a**) (**b**)

Figure 4. Dual block content: (**a**) information block, (**b**) verification block.

4.1.2. Key Generation

Step 1: The key used for encrypting shared intelligence is created by CRYSTALS-KYBER. The process is shown in Figure 5. Initially, a random uniform matrix A is generated. Subsequently, the binomial vector s is derived from A, with the vector e representing error coding. Following this, b is computed, thus leading to the generation of the private key s and the public key (A, b).

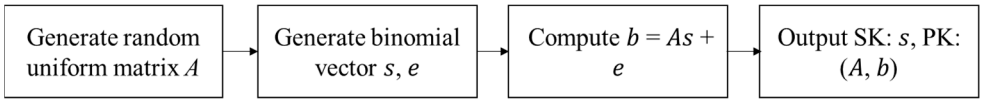


Figure 5. Intelligence key generation process.

Step 2: The blockchain key is constructed by SPHINCS$^+$, as shown in Figure 6. First, user i chooses a random number to create the private key seed $SSKseed$, sets it to the WOTS$^+$ and FORS bottom layer of SPHINCS$^+$, which goes through the hash function to build the WOTS$^+$ and FORS trees, and then XMSS connects FORS and WOTS$^+$ to generate a SSK and SPK.

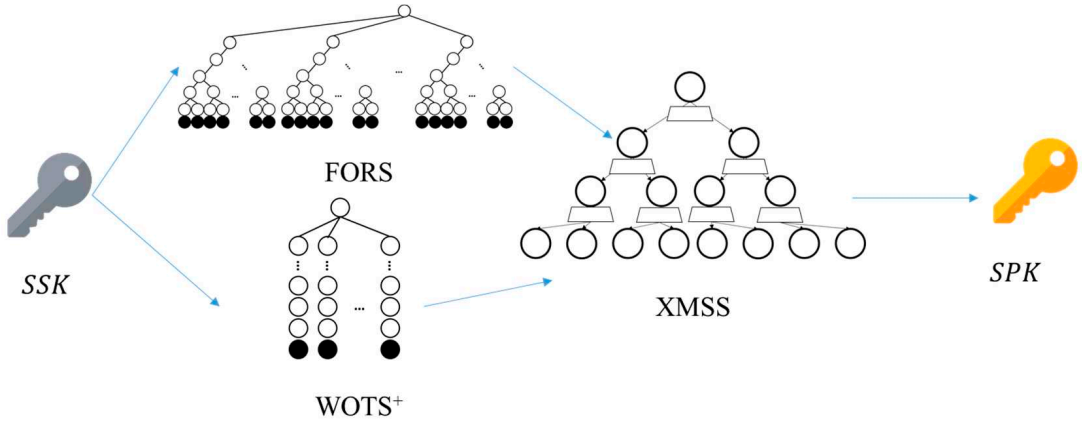


Figure 6. Blockchain key generation process.

Step 3: The public key SPK is input into SHA256 and RIPEMD160 to obtain PK hash. The outcome is further input into SHA256 twice. The first 4 bytes of consequence are combined with PK hash, while the concatenation result is passed to BASE58 to generate an $address_i$, as shown in Figure 7. Finally, $address_i$ and (A,b) are broadcasted on the blockchain work.

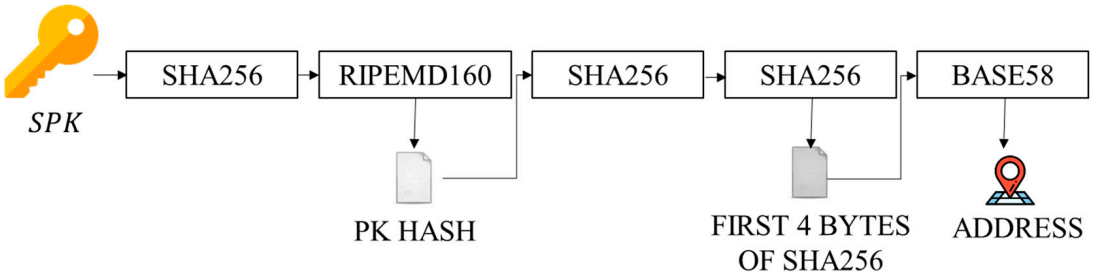


Figure 7. Blockchain address generation process.

4.2. Sharing Phase

This phase illustrates the process of information sharing, as shown in Figure 8.

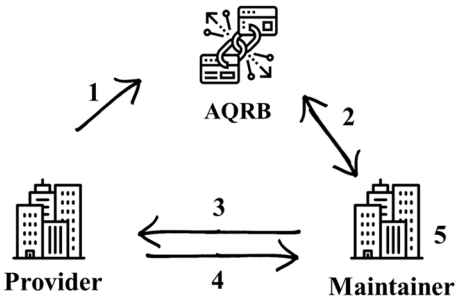


Figure 8. Intelligence sharing flowchart.

Step 1: P calculates and broadcasts $HTX = H(tx||timestamp)$ and signature $Sig_{SSK_P}(HTX)$ to AQRB.

Step 2: Once i obtains HTX and $Sig_{SSK_P}(HTX)$ from AQRB, it utilizes SPK_P to verify $Sig_{SSK_P}(HTX)$. If it is positive, i can be considered to become one of M in this transaction; otherwise, the transaction is not established.

Step 3: When i wants to become M, it calculates $match_i$ and rew_i through Equations (1) and (2).

$$match_i = rep_i \times (1 - e^{-\frac{\lambda}{\mu-\lambda+1}}) \tag{1}$$

$$rew_P = \frac{\left(\frac{1}{match_i} \times e^{-\lambda/(\mu-\lambda+1)}\right)}{2} \tag{2}$$

where λ and μ are the lengths of the information chain and verification chain. Next, i generates $req_i = \left\{SB_i^{latest}, VB_i^{latest}, match_i, rew_i\right\}$ and computes the signature $Sig_{SSK_i}(req_i)$. Finally, i transmits $Sig_{SSK_i}(req_i)$ to P.

Step 4: After P receives request, it verifies i identity. Then, P requests the content of the block from the relevant user recorded in SB_i^{latest} and VB_i^{latest}. Subsequently, P verifies the correctness of these two blocks. If they are correct, P ensures that the $match_i$ and rew_i are promised by i. Then, P continues to wait for willing participants until the total competitiveness satisfies Equation (3).

$$\sum_{i=1}^{n} match_i > 2 \times rep_S \times \left(1 - e^{-\lambda/(\mu-\lambda+1)}\right) \tag{3}$$

Step 5: When i receives a reply from P, it means that P has recognized i as M_i. Subsequently, M_i uses SPK_S to verify the correctness of the signature. At the same time, i checks whether rep_S^{latest} and rep_i^{latest} are correct. If they are valid, M_i uses SK_i to extract the tx||timestamp. Next, M_i calculates $HTX' = H(tx||timestamp)$ and compares the result with the HTX of Step 1. If they are the same, it means that M_i successfully obtains the information shared this time. M_i can create the latest block of $VB_i^{lastest+1}$.

4.3. Transactions Phase

This phase illustrates the intelligence sharing process, as shown in Figure 9. Numbers 1 to 3 in the figure correspond to Step 1 to Step 3 described below.

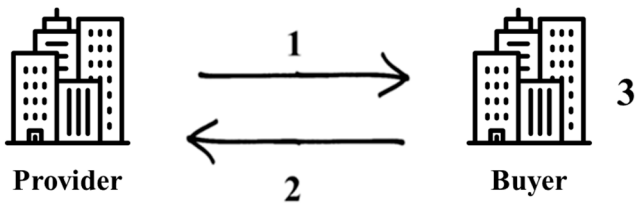


Figure 9. Intelligence purchase flowchart.

Step 1: When B obtains the information from P, B initiates a transaction with P to obtain the $address_P$ and PK_P, and then sends the purchase request to P.

Step 2: After receiving the request, P signs the message txt using its own private key SSK_P, obtaining the signature $Sig_{SSK_P}(txt)$. Subsequently, P encrypts both the original message txt and the signature $Sig_{SSK_P}(txt)$ using PK_B, resulting in $Enc_{PK_B}\left(Sig_{SSK_P}(txt)\right)$, which is then sent to B.

Step 3: Once B receives the data from P, it applies SK_B to decrypt and verify the identity of P by SPK_P. If it is correct, B broadcasts the $\mathrm{H}(txt)$ to the blockchain; otherwise, the transaction is not established.

Step 4: The miners compete to become V through Equation (1), and determine the number n of V when it reaches the condition as Equations (4) and (5).

Step 5: B obtains HTX through performing hash function $\mathrm{H}(\mathrm{H}(txt)||timestamp)$, and derives $Sig_{SSK_M}(HTX)$.

Step 6: B packs $Sig_{SSK_B}(HTX)$ into broadcast information $Data$ and broadcasts it to the AQRB, $Data = (Sig_{SSK_B}(HTX), tx, timestamp, SPK_B)$, including signature of B, transaction information, timestamp, and public key of B.

$$R_V - R_t > 0 \tag{4}$$

$$R_V = \sum_{i=1}^{n} match_i \tag{5}$$

5. Experiments Result

The experiments are conducted with Windows 10 64-bit operating system and Intel Core i7-10510U CPU 2.6 GHz processor. Section 4.1 offers the discussion on storage, while Section 4.2 focuses on the analysis of computational resource usage.

5.1. Storage Space Cost

AQRB leverages SPHINCS$^+$ as the algorithm to construct the blockchain and selects SPHINCS+-128f as the parameter with the same robustness as ECDSA (P-256). According to the information block and verification block content in Figure 10, the data size of Cyber information is 136,704 bits, $SPBH$ and $PVBH$ are 256 bits, $height$ and $timestamp$ are both 32 bits, $proof$ is 137,312 bits, and the total number of $Sharing$ and verification blocks depends on the number of information maintenance companies M. Therefore, the storage space is estimated based on the three conditions: supply and demand balance, oversupply, and undersupply. With the block establishment condition being twice that of the S reputation value, it requires 2–4, 5–7, and 1 company maintenance for each condition discussed.

In the context of supply and demand balance, when two to four companies take charge of maintaining data, $Sharing$ includes the $Sig_{SSK_i}(req_i)$, rep_i, and PK_i. If the data are maintained by two enterprises, $Sharing$ size is 273,984 bits and the two verification blocks are 274,624 bits. In the case that three enterprises are involved in the provision, $Sharing$ size is 410,976 bits and the verification block is 411,936 bits. When four companies are involved in the maintenance, $Sharing$ size is 547,968 bits and the verification block is 549,248 bits. Therefore, while two to four companies join the data play, it takes 685,632 to 1,234,240 bits for the information block. In comparison, in cases of oversupply and undersupply, the data sizes are 1,508,552 to 2,057,152 and 411,328, respectively.

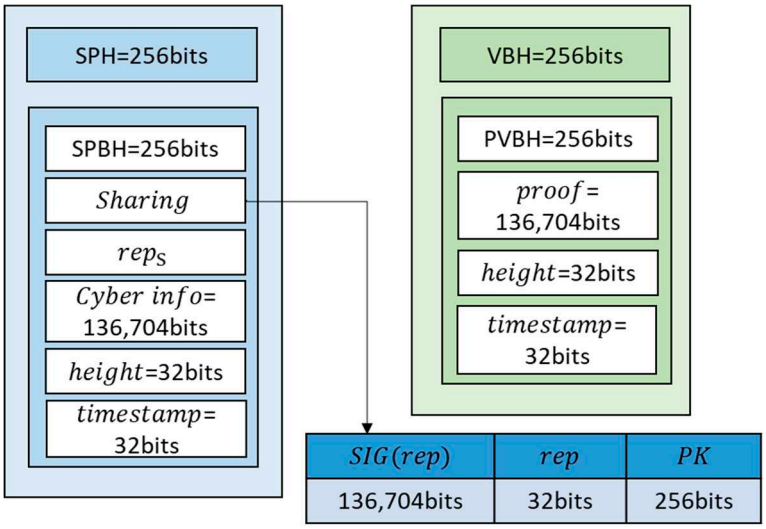


Figure 10. Block storage space cost.

Figure 11 illustrates the storage costs of sharing block and verification block under different numbers of companies participating in the data maintenance. As the number of companies increases, the storage space required for both sharing block and verification block increases, impacting the total storage space consumption. Figure 12 illustrates the advantage of AQRB in terms of storage cost compared to popular blockchain like Bitcoin and Ethereum. As of now, the record shows 46 million users, with an average block size of 1.5 MB for Bitcoin. Ethereum has 378,000 users with an average block size of 72,000 bits. In contrast, AQRB requires the storage of only those nodes that are pertinent to its operation, thereby achieving significant data storage efficiency.

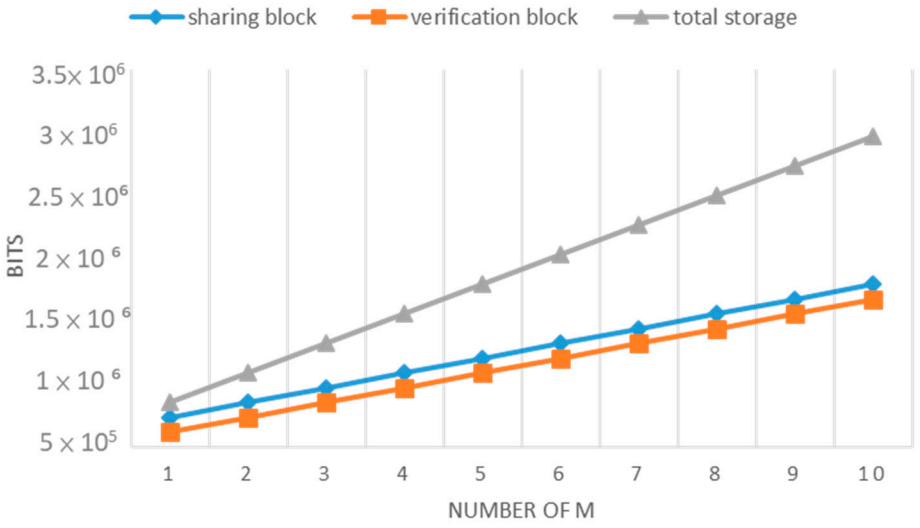


Figure 11. Storage cost for a different number of companies.

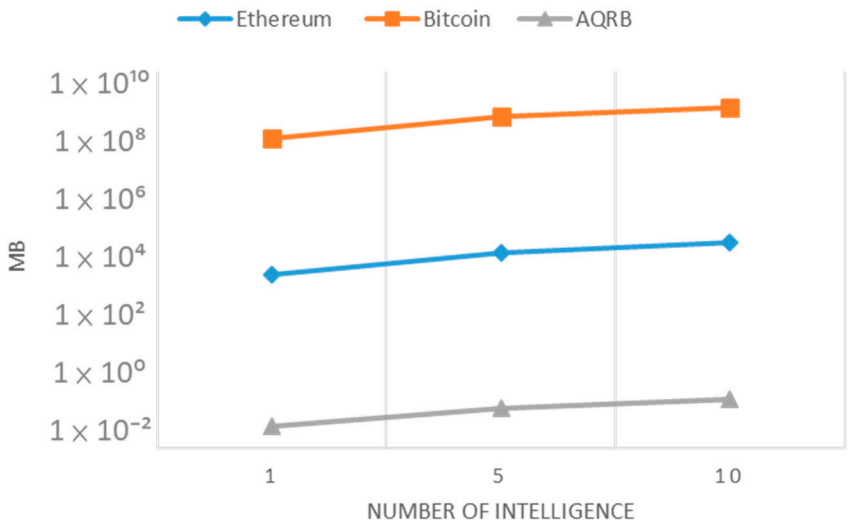
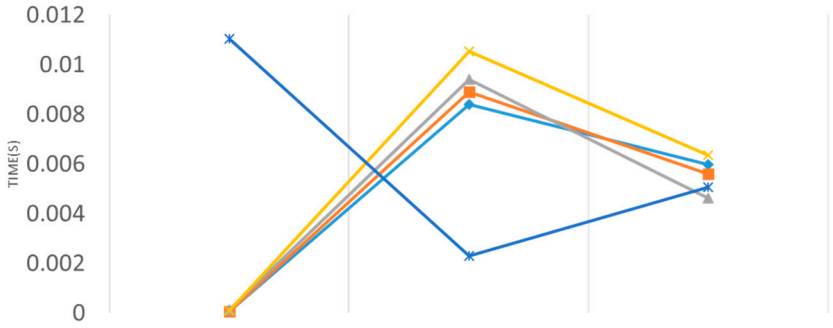


Figure 12. Storage space cost for different blockchains.

5.2. Computational Resource Usage

In this subsection, we evaluated the computational resources by assessing the algorithms used, the time spent at each stage, and the differences in the number of M and B, using a data size of 1 MB.

The computational performance comparisons between SPHINCS+ and ECDSA in terms of key generation, signature, and verification under the configurations of sha128f, sha192f, sha256f, and haraka128f against the P-256 curve of ECDSA are shown in Figure 13. The table below the graph provides the specific times for each operation. Although SPHINCS+ exhibits slower performance in signing operations, its key generation and verification times are comparable to those of ECDSA. Moreover, SPHINCS+ offers the higher robustness against quantum attacks, ensuring a better level of protection. For a deep insight into the phase analysis, the time consumption at different stages is illustrated in Figure 14.



	Key generate	Signature	Verify
sphincs+(sha128f)	0.0000668	0.008403	0.005956
sphincs+(sha192f)	0.0000718	0.008881	0.005597
sphincs+(sha256f)	0.000114	0.009411	0.004626
sphincs+(haraka128f)	0.000087	0.010529	0.006342
ecdsa(p256)	0.011025	0.002299	0.005051

Figure 13. Computational performance of SPHINCS$^+$ vs. ECDSA.

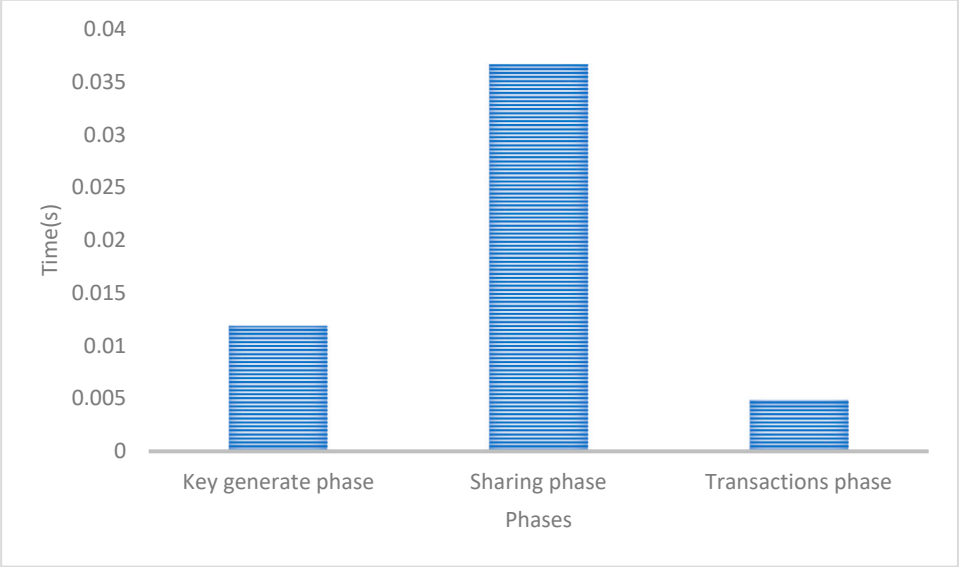


Figure 14. Computational resource usage across phases.

The further-detailed computational resource usage in the sharing phase by the number of companies maintaining the blockchain is displayed in Figure 15. It is clear that the increasing number of companies has led to the linear increase of computational resources required for the sharing phase. The computational resource usage during the transactions phase relative to the number of transactions is depicted in Figure 16. As the number of transactions increases, resource usage shows a significant rise, highlighting the computational cost associated with the higher transaction volumes.

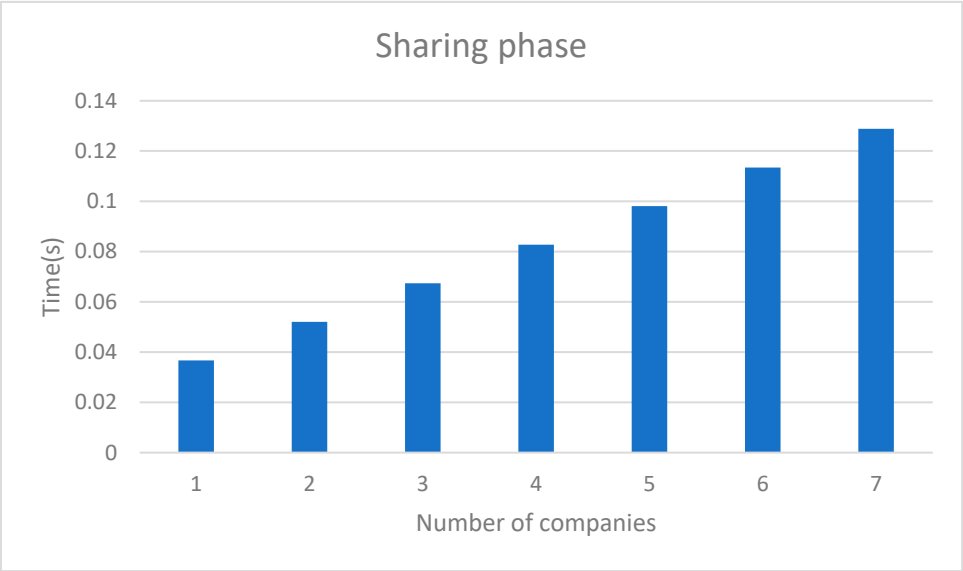


Figure 15. Sharing phase resource usage by the number of companies.

These results have demonstrated a detailed analysis of the computational efficiency and resource requirements for different post-quantum cryptographic algorithms, evidencing the balance between security and performance in a blockchain environment.

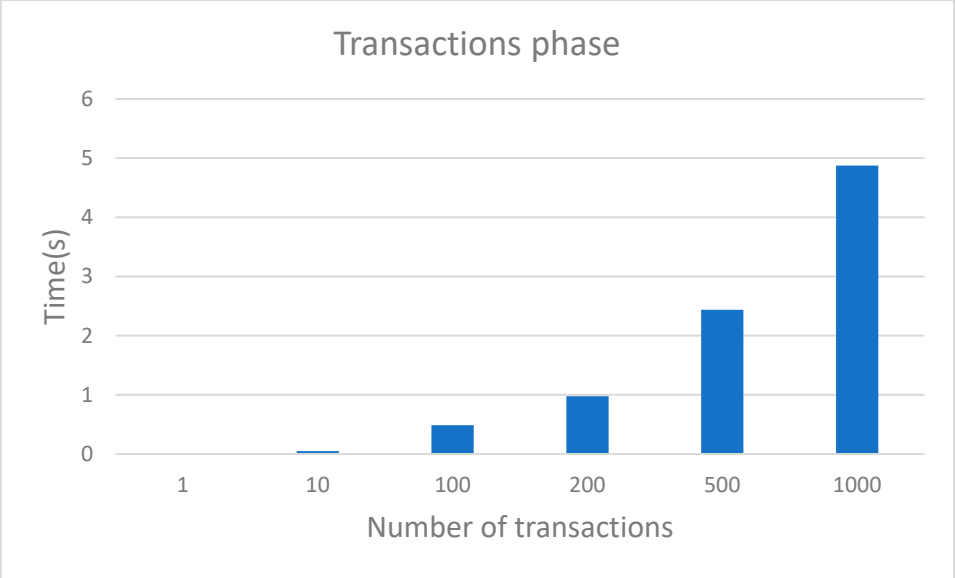


Figure 16. Transactions phase resource usage by the number of transactions.

6. Security Analysis

This section analyzes the security of the post-quantum blockchain model designed in AQRB. The characteristics of data security, resistance to quantum computing attacks, lightweight storage burden, sustainable maintenance, and consensus efficiency between related works and AQRB.

☐ Data Security

Concerning the blockchain-based [16] and post-quantum blockchain studies [17,18], users must store data from all nodes. To tamper with the information, an attacker needs to control at least 51% of the network computational power; thus, ensuring data security as demonstrated in [16–18].

On the contrary, the data are stored by the responsible maintaining enterprise once the intelligence sharing is initiated in AQRB. After the sharing phase, other enterprises can request the intelligence through the acquisition phase. According to the concept of network externalities, the value of a product increases with the number of users. Thus, as more entities seek the shared intelligence, its value escalates. Consequently, the more enterprises acquire the intelligence, the more enterprises are involved in maintaining it, thereby enhancing data security in AQRB. This approach ensures that data security is proportional to the value of the information, thereby achieving a robust data security model.

☐ Resistance to Quantum Computing Attacks

Resistance to quantum computing attacks refers to the ability of cryptographic algorithms to withstand attempts at decryption using quantum computers. In [16], blockchain technology relies on ECDSA for its signature algorithm. However, ECDSA has been proven insecure under quantum computing attacks, rendering current blockchain applications vulnerable to such attacks. Recent studies [17,18] have investigated various post-quantum algorithms, including Falcon, Dilithium, and Rainbow. In July 2022, NIST has selected Falcon and Dilithium as parts of the post-quantum digital signature standards, while the Rainbow signature scheme has suffered from key recovery attacks, leading to its exclusion from the final list of recommended algorithms.

As with AQRB, SPHINCS+ is adopted as the foundational digital signature algorithm for constructing the blockchain, which is recognized by NIST as a post-quantum digital signature standard. Therefore, it inherits the capability to withstand quantum computing at-

tacks. This adoption ensures that the blockchain is secure against the computational threats posed by quantum computers, offering a significant security advantage over traditional cryptographic methods.

- Lightweight Storage Burden

The characteristic of lightweight storage burden refers to reducing the amount of data that needs to be stored and synchronized across a blockchain network. Traditional blockchain architectures, including most post-quantum blockchain studies [17,18], primarily apply Proof-of-Work (PoW), Proof-of-Stake (PoS), or Proof-of-Activity (PoA) as consensus mechanisms. These systems require all participating nodes to store and synchronize the entire transaction history, regardless of their relevance to specific data exchanges. As a result, the storage requirements scale with the chain's growth, imposing a heavy burden on all nodes.

In contrast, the Meepo framework proposed by Zheng et al. [16] introduced a sharded consortium blockchain with multiple execution environments, allowing organizations to process and store only relevant transactional data within their own domains. This localized data handling effectively reduces the synchronization and storage load on individual nodes. Similarly, AQRB adopts an asynchronous dual blockchain model [22], where data are maintained only by the involved enterprises. There is no need to synchronize all blocks across the network, thereby significantly reducing overall storage demands and enhancing scalability.

- Sustainable Maintenance

Sustainable maintenance in a blockchain concerns the system's ability in maintaining its long-term operations and security without degrading performance. The essential operations of blockchain-based [16] and post-quantum blockchain studies [17,18] are influenced by factors such as mining rewards, total currency, and transaction demands. Nodes may opt to perform transactions or mining exclusively. Such imbalanced behaviors, like solely validating or solely initiating data storage, will negatively impact the blockchain network, leading to its decline and failing to meet the requirements for sustainable maintenance.

In AQRB, the sharing and maintenance are interdependent. Before acquiring information from others, users must first share their intelligence. Units seeking intelligence must spend their earned reputation values and assist in maintaining data security. This mechanism ensures a balanced operation of the intelligence platform, preventing any participant from gaining intelligence without contributing. Thus, AQRB can guarantee that users either provide shared intelligence or contribute to blockchain verification, achieving sustainable maintenance.

- Consensus Efficiency

Consensus efficiency refers to the speed and effectiveness, with which a blockchain network can reach agreement on the validity of transactions. Traditional systems based on PoW and PoA [16] provide high reliability but require global validation by a majority of the network's computational resources. This results in significant time delays, particularly as network size and transaction volume increase. Post-quantum blockchain approaches [17,18] face additional challenges due to slower signature generation and verification speeds when using quantum-resistant algorithms such as hash-based or lattice-based schemes, further lowering consensus throughput.

Zheng et al. [16] addressed this issue by proposing localized consensus mechanisms in their sharded architecture, where only the relevant shards participate in transaction validation, thereby reducing consensus latency. Building upon this idea, AQRB employs an asynchronous, contribution-balanced consensus mechanism. In this design, only the

relevant parties are involved in each data sharing or acquisition event. This targeted participation dramatically improves consensus speed and efficiency, allowing the system to process transactions more effectively within the same time frame compared to traditional global consensus methods.

7. Conclusions

AQRB integrates a post-quantum, dual blockchain architecture to enable quantum-resistant computation. This architecture adopts SPHINCS+ and CRYSTALS-KYBER as its core cryptographic algorithms, ensuring robust data security against potential quantum attacks. The dual-chain design effectively reduces the burden of full network synchronization, thereby significantly lowering the overall storage requirements across the system. Furthermore, storage costs are dynamically adjusted based on real-time supply and demand conditions. Experimental evaluations demonstrate that the proposed architecture achieves superior efficiency and reduced storage consumption compared to conventional blockchain systems, highlighting its scalability and resource optimization capabilities. In addition, AQRB employs an asynchronous balancing contribution mechanism, wherein only relevant parties participate in each data sharing or acquisition event. This selective involvement enhances consensus efficiency by minimizing unnecessary communication overhead. Users are also required to contribute information before accessing new data and must expend earned reputation points to obtain information. This reputation-based access model contributes to maintaining data security and supports the sustainable operation of the blockchain ecosystem.

Looking ahead, research will focus on further optimizing the consensus efficiency and scalability of dual blockchain architectures, particularly in high-throughput or real-time applications. In addition, investigating hybrid cryptographic systems that integrate multiple post-quantum algorithms will enhance the system's resilience against diverse quantum attack vectors. To strengthen privacy and data sovereignty, the integration of advanced privacy-preserving technologies such as zero-knowledge proofs, homomorphic encryption, and biometric authentication will be explored. These technologies aim to provide strong security protections without compromising user anonymity, making it feasible to build blockchain systems that can handle both scalability and post-quantum threats in real-world applications.

Author Contributions: Conceptualization, J.-S.L.; Methodology, Y.-Y.F.; Formal analysis, C.-J.C.; Investigation, J.-S.L.; Writing—original draft, Y.-Y.F.; Writing—review & editing, J.-S.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: Author Chit-Jie Chew was employed by the company AAA Security Technology Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Ponemon Institute. The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies. 2019. Available online: https://stratejm.com/wp-content/uploads/2019/08/2019_Ponemon_Institute-Value_of_Threat_Intelligence_Research_Report_from_Anomali.pdf (accessed on 18 May 2025).
2. America's Cyber Defense Agency. Automated Indicator Sharing (AIS). Available online: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais (accessed on 18 May 2025).
3. Al-Ibrahim, O.; Mohaisen, A.; Kamhoua, C.; Kwiat, K.; Njilla, L. Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligenc. *arXiv* **2017**, arXiv:1702.0055. [CrossRef]
4. Block, F. PAK's NFT Artwork 'The Merge' Sells for $91.8 Million. PENTA. 2021. Available online: https://www.barrons.com/articles/paks-nft-artwork-the-merge-sells-for-91-8-million-01638918205 (accessed on 18 May 2025).
5. Mobility Open Blockchain. MOBI. Available online: https://dlt.mobi/ (accessed on 18 May 2025).
6. Azaria, A.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
7. Qin, N. The Evidence is in: Chinese Courts Use Judicial Blockchain Platform to Store Data. yahoo!finance. 2022. Available online: https://finance.yahoo.com/news/evidence-chinese-courts-judicial-blockchain-084704515.html (accessed on 18 May 2025).
8. Shen, T. China Sees Most Blockchain-Related Patent Applications, Followed by U.S., South Korea: Report. fastForkas. 2021. Available online: https://forkast.news/headlines/china-blockchain-patent-applications-us-south-korea/ (accessed on 18 May 2025).
9. Microsoft Azure Quantum Team. The Quantum Computing Effect on Public-Key Encryption. Microsoft. 2018. Available online: https://cloudblogs.microsoft.com/quantum/2018/05/02/the-quantum-computing-effect-on-public-key-encryption/ (accessed on 18 May 2025).
10. Swayne, M. Google Already Using PQC to Protect Internal Communications. Microsoft. 2022. Available online: https://thequantuminsider.com/2022/11/21/google-already-using-pqc-to-protect-internal-communications/ (accessed on 18 May 2025).
11. PQCRYPTO. Initial Recommendations of Long-Term Secure Post-Quantum Systems. Post-Quantum Cryptography for Long-Term Security. 2015. Available online: https://pqcrypto.eu.org/docs/initial-recommendations.pdf (accessed on 18 May 2025).
12. Libra. An Introduction to Libra. 2019, pp. 1–12. Available online: https://www.diem.com/en-us/ (accessed on 18 May 2025).
13. Yang, Z.; Alfauri, H.; Farkiani, B.; Jain, R.; Di Pietro, R.; Erbad, A. A survey and comparison of post-quantum and quantum blockchains. *IEEE Commun. Surv. Tuts.* **2024**, *26*, 967–1002. [CrossRef]
14. Parida, N.K.; Nayak, S.; Das, P.; Bhoi, A.K.; Mohanta, B.K. Post-Quantum Distributed Ledger Technology: A Systematic Survey. *Sci. Rep.* **2023**, *13*, 13911. [CrossRef] [PubMed]
15. Baseri, Y.; Hafid, A.; Shahsavari, Y.; Makrakis, D.; Khodaiemehr, H. Blockchain security risk assessment in quantum era, migration strategies and proactive defense. *arXiv* **2025**, arXiv:2501.11798.
16. Zheng, P.; Xu, Q.; Zheng, Z.; Zhou, Z.; Yan, Y.; Zhang, H. Meepo: Multiple Execution Environments per Organization in Sharded Consortium Blockchain. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3562–3574. [CrossRef]
17. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 18–43. [CrossRef]
18. Fernández-Caramès, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
19. Aumasson, J.-P.; Bernstein, D.J.; Beullens, W.; Dobraunig, C.; Eichlseder, M.; Fluhrer, S.; Gazdag, S.-L.; Hülsing, A.; Kampanakis, P.; Kölbl, S.; et al. SPHINCS+—Submission to the 3rd Round of the NIST Post-Quantum Project. v3.1. 2022. Available online: https://sphincs.org/data/sphincs+-r3.1-specification.pdf (accessed on 18 May 2025).
20. Schwabe, P.; Avanzi, R.; Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Seiler, G.; Stehle, D.; et al. CRYSTALS-Kyber. Cryptographic Suite for Algebraic Lattices. Available online: https://pq-crystals.org/kyber/index.shtml (accessed on 18 May 2025).
21. Wu, W.C.; Chew, C.J.; Chen, Y.C.; Wu, C.H.; Chen, T.H.; Lee, J.S. Blockchain-based WDP Solution for Real-time Heterogeneous Computing Resource Allocation. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 3810–3821. [CrossRef]
22. Hong, W.C.; Yang, R.K.; Chen, Y.C.; Li, B.; Lee, J.S. Efficient Peer-to-Peer E-Payment based on Asynchronous Dual Blockchain. *J. Internet Technol.* **2020**, *21*, 1375–1385.