QHB-DA: A Quantum Hybrid Blockchain-based Data Authenticity Framework for Supply Chain in Industry 4.0

Kening Zhang, Carman K. M. Lee, *Senior Member, IEEE*, Yung Po Tsang, *Member, IEEE*

***Abstract*—In the landscape of Industry 4.0, enhancing data traceability across the supply chain is imperative. With the development of quantum computers, blockchains traditionally used for traceability struggle to guarantee the authenticity of data. Furthermore, only chained blocks have been used in previous traceability systems, which has resulted in a full backup for each business unit in the supply chain, wasting storage resources significantly. Another problem is that there are differences in the data structure and consensus mechanisms of each unit, which makes maintenance difficult. To address these problems, it is encouraging to create a new blockchain with high scalability and resistance to quantum attacks. This paper innovatively proposes a quantum hybrid blockchain-based data authenticity framework (QHB-DA) with five layers, which not only accomplishes traceability, but also has assurance that data can withstand verification. In QHB-DA, blockchain utilizes a combination of DAG and chained structures to reduce data redundancy, in which quantum hashes are performed to connect blocks. Algorithms ED-QKD and D2B-QSC are designed to keep the information from being leaked during transmission and format conversion. Through cost-benifit analysis, security analysis and empirical experiments, feasibility of quantum hashing and the attack resistance of the QHB-DA are demonstrated, which can reduce storage wastage and completely implement the data authenticity.**

***Index Terms*—hybrid blockchain, quantum cryptography, supply chain, traceability, data authenticity.**

I. Introduction

THE blockchain technology is widely recognized as a dependable ledger for recording data in a way that is resistant to tampering. Due to the large amount of private data, its applications extend beyond just cryptocurrencies (Bitcoin [1] and Ethereum [2]), which finds significant capabilities and applications in the increasingly sophisticated fields of Industry 4.0 [3]. The significant shift towards self-organized production in Industry 4.0, including supply chain management (SCM), potentially changes the entire value chain by making products automatically manage manufacturing procedures [4], [5]. In modern supply chains, particularly in the context of Industry 4.0, products are increasingly responsible for managing their own manufacturing processes. This pattern requires industrial Internet-of-thing (IIoT) devices to collect data, and the authenticity of data is particularly important when various institutions co-operate together in SCM. However, false or compromised data can disrupt the entire supply chain, especially when smart contracts and automated processes rely on accurate inputs [6].

For example, smartphone manufacturers purchase raw materials containing screens, chips, and batteries from multiple suppliers and process them into phone components in factories. After rigorous quality control, the products are stored in warehouses and distributed globally through logistics networks to sales points. Phones are sold to end-users at various points of sale, along with after-sales service. Data collected throughout the process are recorded and integrated into a blockchain for comprehensive analysis and coordination, such as traceability, inventory management and production planning optimization. Blockchain ensures that data remain secure, transparent and immutable, which provides solid technical support for the efficient operation of the entire supply chain. If data is not authentic, the process automaton cannot be smooth.

As this collaborative regimes cut across different specific application scenarios, the data structures and consensus mechanisms vary considerably. This variance leads to the formation of the multichain environment, where distinct blockchain systems function as separate data entities. There is a pressing need to facilitate the exchange of data among these diverse blockchains, especially in the context of SMC in Industry 4.0, where seamless integration and data sharing are critical for efficient operations and decision-making. The evolution of interchain operation technology, propelled by multichain interaction, has led to indirect methods for data sharing, containing hash locking, relay chain, and notary scheme. Although these innovations address the issue of blockchain interactivity to some extent, certain issues in supply chain environments still require thorough research, particularly regarding the rapid and accurate exchange of data for tracking goods, ensuring authenticity, and maintaining transparency.

Firstly, the count of IoT devices surpassed the 20 billion mark by 2020, with projections suggesting an escalation to as many as 50 billion by the year 2025 [7]–[11]. In light of this exponential growth, the significance of facilitating transactions directly between devices, especially in the context of machine-to-machine (M2M) micro-payments, has become increasingly

The authors would like to thank the Research and Innovation Office of the Hong Kong Polytechnic University for supporting the project (Project Code: RMGT) and the associated fund (Project Code: K-ZB6V). The work described in this paper is also supported by the project (Project Code: 1-CD4E) of Research Institute for Advanced Manufacturing, The Hong Kong Polytechnic University *(Corresponding author: Carman K. M. Lee).*

Kening Zhang is with the Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong (e-mail: keningcs.zhang@connect.polyu.hk).

Carman K. M. Lee and Yung Po Tsang are with the Department of Industrial and Systems Engineering, Research Institute for Advanced Manufacturing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong (e-mail: ckm.lee@polyu.edu.hk; yungpo.tsang@polyu.edu.hk).

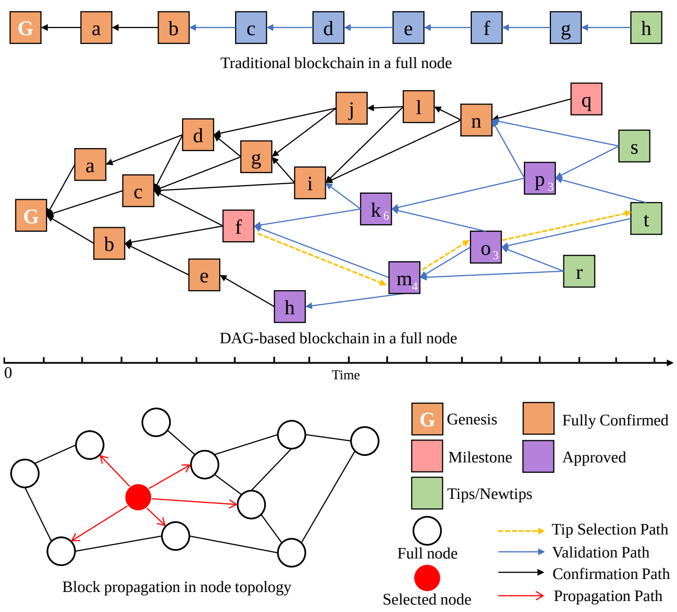


Fig. 1. Two types of blockchains and topology

critical [12]. Traditional blockchain is not applicable to massive Industrial IoT devices due to drawbacks such as TPS, energy consumed by mining and high transaction fees [13]. Therefore, the domain of distributed ledgers for IoT environments is witnessing a growing interest in blockchain technologies based on Directed-Acyclic-Graph (DAG). A prime example of this trend is IOTA in Fig. 1, which employs a DAG framework known as Tangle to manage transactions [14]. On the background of SCM within Industry 4.0, the ability to efficiently track, validate, and manage data across various stakeholders is essential. Given the massive scale of SCM networks and the proliferation of IoT devices in modern supply chains, the implementation of secure and scalable distributed ledger solutions becomes crucial. DAG-based blockchains like IOTA offer promising benefits for such environments by improving data sharing and reducing bottlenecks in transaction verification, which are key pain points in conventional SCM systems. However, the combination of DAG-based blockchains with traditional blockchain systems for SCM applications has not been fully explored yet. In the SCM system, the traditional blockchain generates many backups and high data redundancy. An advanced idea is that if the DAG-based blockchain and traditional blockchain are combined, not only the throughput of data can be improved, but also the problem of limited storage resources in data traceability is expected to be solved.

In addition, there is another aspect that needs to be considered in advance, and that is the threat of quantum technology (QT) to traditional cryptography, which can also pose challenges to blockchain security. These potential risks span from primary cybersecurity weaknesses to vulnerabilities emerging during the shift to the quantum computing era. In particular, the secure storage and transmission of data in SCM systems within Industry 4.0 can be significantly impacted by quantum attacks on cryptographic algorithms. There is a pressing requirement for algorithms that protect personal data and IT processing throughout and beyond the above period. As SCM systems become increasingly digitized and IoT devices proliferate, securing transactional data and ensuring traceability will depend on integrating quantum-resistant algorithms into blockchain solutions. There are several practical QTs available, such as quantum walks (QW), quantum superdense coding (QSC), quantum key distribution (QKD) and so on. QW is a quantum equivalent of random walks, which serves as a crucial resource for algorithmic development [15]. QW can be characterized as non-linear transformations of elements in Hilbert space into sets of probability distributions, which enables the conceptualization of discrete QW as chaotic systems, both in terms of discrete time and values [16]. QSC uses the principles of quantum entanglement and superposition to enhance communication efficiency. QKD depends on quantum properties like the no-cloning theorem and the observer effect. These properties guarantee that any eavesdropping attempt on the key can be detected, since the act inevitably alters the quantum states used in the key transmission. Therefore, the incorporation of quantum technologies such as QKD can enhance security frameworks for SCM, which provides resilience against quantum computing threats. This uniqueness of QTs forms a crucial cornerstone in the development of advanced security measures.

In such a case, cryptographic technologies and services based on QT can prove highly beneficial. Specifically, the hazards linked to data storage, management, traceability and sharing, commonly associated with blockchain and SMC, can be significantly reduced or even nullified through advanced quantum computing and communication technologies. Consequently, the implementation of an efficient and theoretically-sound secure pattern is necessitated, which operates with precision during the process of blockchain-based data processing in supply chain. To accomplish this goal, we proposed a data authenticity framework with hybrid blockchain (HB) combining traditional and DAG-based structure, in which cutting-edge QTs are adopted to ensure absolute security. Followings are the innovations and contributions of our paper.

1) We design a novel quantum hybrid blockchain (QHB)-based data authenticity framework named QHB-DA, in which quantum communication and blockchain technology are combined to handle large-scale and sensitive data for high efficient and authentic cooperation in supply chain.
2) A HB integrating DAG and traditional blockchain is proposed to save storage resources, where the linking of blocks and DAG adopts the quantum hash function (QHF) based on lively controlled alternate quantum walks (LCAQW) to keep post-quantum security.
3) Develop ED-QKD and D2B-QSC algorithms, utilizing QKD with BB84 protocol and QSC, which safeguards the network against potential eavesdropping threat.
4) Comprehensive cost and security analysis are well-presented, including theoretical and practical aspects, which demonstrates that QHB-DA can be deployed at regular cost and is resistant to quantum attacks.

The remaining organization of this article is structured as

TABLE I
PERFORMANCE AND PROPERTIES COMPARISON WITH MAIN QUANTUM OR NON-QUANTUM BLOCKCHAIN-BASED SYSTEMS

	QHB-DA (ours)	Sun et al. [17]	Rajan et al. [18]	Gao et al. [19]	Li et al. [20]	QB-IMD [21]	Cao et al. [22]	SynergyChain [23]
Resist quantum attacks	√	√	√	√	√	√	×	×
Specific scenarios	√	×	×	×	×	√	×	√
Security analysis	√	×	√	√	√	√	×	×
Cost analysis	√	×	×	×	×	×	√	×
High scalability	√	×	×	×	×	×	×	×
Data authenticity	√	×	×	×	×	√	×	×

Note: The symbol '√' indicates that the system proposed in the article meets the corresponding feature, while '×' signifies that the feature is not met.

follows. In Section II, we mainly introduce the related work of DAG-based blockchain technologies and the development of quantum computing. Section III presents the system framework of proposed QHB-DA. Section IV provides the quantum algorithms of communication, encryption and decryption. Then, we analyze the cost in Section V and security in Section VI of QHB-DA. In Section VII, we evaluate the performance of experiments. Finally, we conclude the contribution of our work and future direction in Section VIII.

II. Related Works

This section introduces current advances in data oracles and multichain of supply chain, DAG-based blockchain and quantum theory, especially about challenges and motivations of these components for QHB-DA. The excellent performance and properties of our proposed system compared with other quantum or non-quantum blockchain-based systems can be found through Table I.

A. Data Oracles and Multichain

Data oracles are capable of offering smart contracts detailed insights including temperature, geographic positioning, and the quality, quantity, and condition of products throughout the supply chain. Many large companies have already put data oracles into use. Abu Dhabi National Oil Company (ADNOC) and IBM [24] have utilized data oracles to track and validate oil and gas value on blockchain. De Beers [25] proposed a platform named Tracr, in which the quality and provenance of diamonds were recorded. Walmart and IBM [26] developed a blockchain platform to interact with IoT devices for the safety and traceability of food. Everledger [27] implemented a blockchain-based system to generate digital ports for wine bottles, including vintage, quality, origin and so on. These efforts effectively realize the intelligence and transparency of the supply chain under Industry 4.0 and make the SMC more in line with the requirements of smart manufacturing.

Moreover, multichain architecture is a topic well worth being investigated in supply chain. DShare, a concept presented by Cao et al. [22], focuses on query assessments and abstracts heterogeneous computations across data pools shared under diverse security protocols. Xuan et al. [28] and Chen et al. [29] proposed a motivational mechanism for blockchain nodes to strengthen data quality and reliability, though they overlooked user privacy. The authors suggested BlockchainDB [30], combines a decentralized network with conventional databases, which extends the blockchain's capabilities through standard data management practices. Specifically, the system utilizes blockchain for foundational storage and overlays it with a database layer. However, this integration poses challenges in protection against data tampering at the centralized level. Hwang et al. [3] in multichain systems, implemented a dual-layer main-side blockchain organization to simplify data management and minimize redundancy, in which both the main and side chains are structured equally, allowing effective data sharing among original participants in a uniform side blockchain. This approach, however, faces limitations in broadening its application, particularly in enabling multilateral data sharing among diverse blockchains due to heterogeneous data structures and the inability of different subchain systems to directly interact. SynergyChain [23] amalgamates data within a multichain system, enabling data sharing among heterogeneous facilities. But existing multi-organizational data processing methods lack consideration for the segregation and protection of private data. Furthermore, none of these cross-chain studies so far have considered high-throughput conditions, which makes the system operate much less efficiently. Therefore, cross-chain research under high throughput conditions remains an important direction to realize intelligent SMC for Industry 4.0.

B. DAG-based Blockchain

In the realm of DAG-based blockchain technologies, the field is still unfolding, with research primarily in its initial phases. A broader spectrum of DAG-based blockchains, embodying XDAG, Nxt, DagCoin, Orumesh, Nano, Byteball and IOTA, was subject to the comprehensive review and analysis by Pervez et al. [31]. In [32], the IOTA foundation has contributed to DAG mode by providing a range of simulated outcomes for the Tangle structure, scrutinizing parameters such as the cumulative weight and the count of tips, which reinforces the insights of the IOTA white paper. In a significant stride, Silvano et al. [33] presented theory, mathematical analysis and the ecosystem behind IOTA, which aims to give the systematic community's architecture and background of this technology. This provides immediate application value for transparency and traceability of the SMC, especially in efficiently tracking the use of IoT devices. In a different vein, Wang et al. [34] creatively developed and tested three unique attack strategies against IOTA, probing its security fortitude. Concentrating on contrasting various consensus algorithms, Cao et al. [35] revealed that while PoW and PoS are more reactive to shifts in network resources, DAG's sensitivity leans more towards network load factor. Li et al. [36] adeptly utilized the Markov chain model to elucidate the consensus procedure of IOTA, ingeniously crafting a classic double-spending attack scenario within this model and assessing the attack's success rate under diverse load conditions through a stochastic model. Beyond these advancements, some progress has been made on optimization of DAG-based blockchain systems. Wang et al. [37], [38] groundbreaking suggested a novel accelerator specifically for the IOTA-based blockchain to enhance capabilities, notably reducing CPU usage by offloading both the PoW and validation processes to compute in parallel on ReRAM. Address generation time in IOTA was strikingly diminished by Shafeeq et al. [39], who employed a cuckoo bloom filter to alleviate database constraints. There have also been several studies focusing on how to develop a comprehensive benchmarking tool for DAG-based blockchains. Dong et al. [40] put forth a framework dedicated to the performance evaluation of DAG-based structure. Park et al. [41], while also concentrating on these blockchains' functions, predominantly considered performance indicators, leaving out vital factors like security and robustness. Since the DAG-based blockchain is an up-and-coming structure, experiments and time are still needed to verify its security, which is hardly addressed in the current research.

C. QT-based Cryptography

As innovative hacking methods come into view, the current security protocols for blockchain face prominent challenges [42]. The advent of quantum computing, with its potential to change blockchain transaction data without affecting the hash value, looms as a future concern [43]. Therefore, the efficacy of some contemporary cryptographic methods is under threat from the capabilities of QT, which indicates possible vulnerabilities in blockchain technology due to quantum advancements [43], [44]. One promising direction to fortify blockchain security involves the creation of new block elements utilizing QT or post-quantum cryptography. Different initiatives are underway to devise blockchain architectures grounded in quantum models with the primary benefit of their resilience against quantum computer assaults [17]–[20]. A notable instance is the development of ”Logicontract”, a quantum blockchain framework introduced by [17]. This framework employs a digital signature mechanism based on QKD to counter potential quantum computer attacks. Another study [18] introduced an innovative conceptual blockchain that leverages quantum entanglement over time, which encodes the content in a temporal Greenberger-Horne-Zeilinger state. Gao et al. [19] conceived the ”quantum coin”, which is creatted in quantum Bell states. Furthermore, another framework for quantum blockchain, employing a lattice-based blind signature mechanism, was introduced in [20], which showcases the continuous evolution in this field. However, there are still relatively few applications at the network level, especially using QT to address the communication aspects of the blockchain, which needs special attention.

III. QHB-DA Design

In this section, we introduce the comprehensive system design of QHB-DA, which includes the entire framework and operational processes. Then, we give detailed content of various layers from a bottom-up sequential point of view.

A. System Framework

We propose a five-layer framework to achieve data authenticity in the supply chain, which includes data traceability and validation, as shown in Fig. 2. The core idea of this framework utilizes quantum technology and an HB to ensure that data is not tampered with and to increase the transaction throughput. It first stores the data generated by each business unit (BU) in the supply chain with DAG-based blockchains, and then integrates these heterogeneous chains into a traditional blockchain to ensure traceability. QT guarantees that the data will not be tampered with throughout this process. There is no need to worry about any technology or quantum computer that can destroy the data authenticity on the chain. Next we will describe the functional setup of each layer in order.

B. Perception Layer

The perception layer is a crucial component that interfaces with the physical world and has the responsibility for data collection. This layer includes various technologies like RFID labels, barcodes, scanners, and diverse sensors such as temperature, humidity, GPS, and cameras, which enables the perception layer to adjust sensor parameters based on collected data and capture real-time information. This layer's functionality is essential for accurate monitoring and data acquisition in SCM, contributing the foundational data input to the processing and traceability of subsequent layers.

C. DAG-based Blockchain Layer

In this layer, the operational workflow is characterized by a sequential and interlinked traceability mechanism for SCM, which innovatively combines origin, production, sales and consumer traceability. Based on these methods, DAG-based blockchains are employed in six BUs: *provenance, production, vendor, warehouse and stock management, logistics and distribution, and consumers*, which are characterized by their divergence from traditional linear blockchain models. They are designed to enable the efficient and simultaneous processing of multiple transactions and data points. The core functionality revolves around improving traceability and operational efficiency across various supply chain components, from product provenance to consumer data, which provides a scalable, transparent, and robust infrastructure for managing intricate supply chain networks, ensuring data integrity and optimizing the flow of goods and information, as shown in

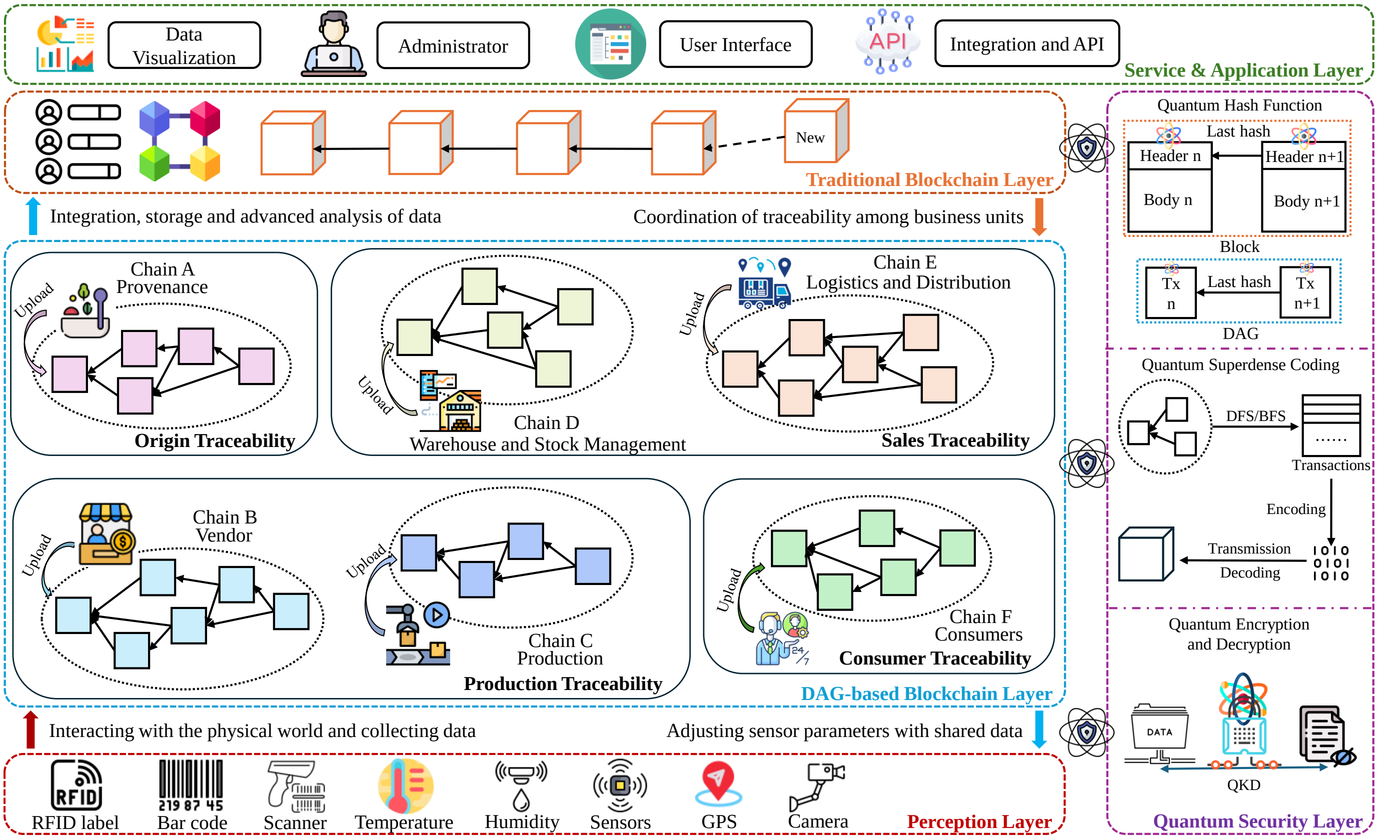


Fig. 2. The entire framework of proposed QHB-DA.

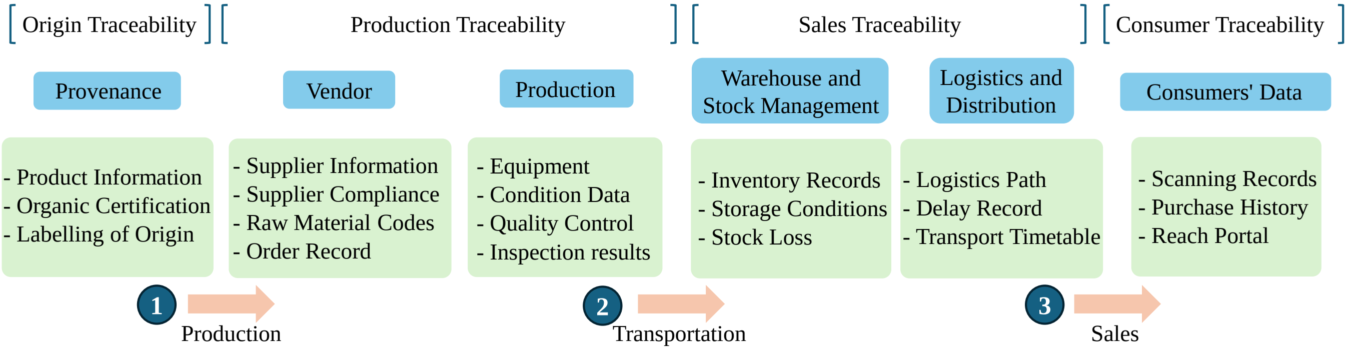


Fig. 3. Process of traceability in the proposed framework.

Fig. 3. Here are the details of heterogeneous traceability in the DAG-based blockchain layer.

1) *Origin Traceability:* This aspect of traceability emphasizes the importance of tracking the source of products. It involves verifying the products, ensuring they meet regulatory and ethical standards. The origin traceability is crucial for maintaining consumer trust, particularly in sectors where the source of products, such as food or pharmaceuticals, which is employed to provide safety and quality. Each product is assigned with a unique identifier, which is then uploaded to the DAG-based blockchain along with its origin details. Technologies like RFID and QR codes are used for tagging and scanning products. product information, organic certification and labelling of origin are stored on Chain A constructed by the provenance unit.
2) *Production Traceability:* The production traceability encompasses both the vendor unit and production unit. The data of the first part in Chain B involves supplier information, supplier compliance, raw material codes and order record, which is essential for supply chain integrity and effective recall management, if necessary. The second part in Chain C includes equipment, condition data, quality control and inspection results, which records quality assurance, compliance with manufacturing standards to identify and address issues in the production line.
3) *Sales Traceability:* This traceability deals with tracking the movement and storage of products through ware-

houses (Chain D) and their distribution logistics (Chain E), respectively. Inventory records, storage conditions and stock loss are uploaded on Chain D while data of the logistics path, delay record and transport timetable are registered on Chain E. This procedure works to manage inventory, ensure timely delivery, and understand the logistics pathways, especially in optimization and responsiveness of SCM.

4) *Consumer Traceability:* The consumer traceability pertains to tracking the end consumer's data, including scanning records, purchase history and reach portal. The aim of this module is to obtain needs and preferences of consumers, aid in market analysis, and drive customer-centric product development and marketing strategies.

D. Traditional Blockchain Layer

This layer utilizes the conventional blockchain structure, which includes a chain of blocks, each containing a header and a body. The header typically includes a QHF and references to the previous block (last hash), ensuring data integrity and security. Each block body contains a set of transactions (T_x), linking the current to the next block (n to $n+1$), which is uploaded from the DAG-based layer using D2B-QSC algorithm. The quantum blockchain's inherent structure ensures that once data is entered, it cannot be altered, providing a tamper-proof record.

E. Quantum Security Layer

In the Quantum Security Layer of the framework, the focus is on QHF, QKD and QSC techniques for data authenticity in SCM. QKD ensures secure communication by enabling two parties to produce a shared random secret key, which can only be known to them. Linking blocks in DAG-based and traditional blockchains with QHFs prevents the proposed system from being corrupted by quantum computers. QSC improves the throughput of data uploads from the DAG-based blockchain to the traditional blockchain. The detailed algorithms for this layer will be given in the Section IV.

F. Service and Application Layer

This layer primarily focuses on integrating user interfaces with the advanced technological aspects of the system, alongside providing Application Programming Interface (API) services. The quintessence of this layer lies in offering an intuitive, user-friendly interface, enabling efficient traceability and verification of system data and functionalities, such as logistics data, inventory status, and supply chain activities. Furthermore, it facilitates the integration of various applications, which enables smooth communication between different technological strata within the system. Consequently, the service and application layer not only enhances the user experience but also augments the overall operational efficiency, authenticity and security of the framework, aligning it with the intricate demands of SMC.

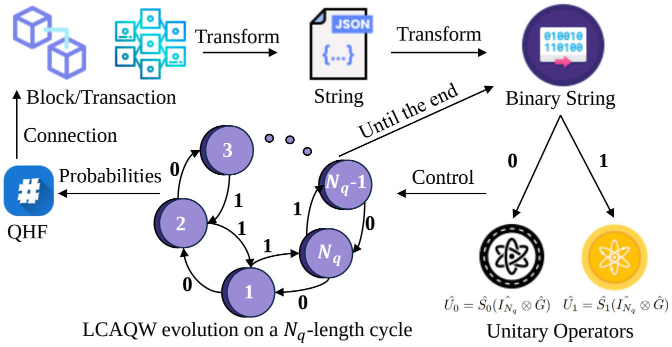


Fig. 4. Generation process of QHF.

IV. QT-based Algorithms for Proposed System

This section introduces QT-based algorithms for QHB-DA, which ensures the highest level of data authenticity and security in this SCM system, not just traceability. These proposed algorithms, including LCAQW-based QHF, ED-QKD and D2B-QSC, guarantee that QHB-DA will not be compromised by quantum computers in the future.

A. LCAQW-based QHF for Blockchain

There are two models of QW: discrete-time QW (DQW) and continuous-time QW (CQW) [45]. Standard DQW has two operators: coin operator C and shift operator S, and the system can be denoted as non-linear mappings of Hilbert space elements to the set of probability distributions, where $\mathcal{H}_\mathfrak{t} = \mathcal{H}_\mathfrak{p} \otimes \mathcal{H}_\mathfrak{c}$. When a particle (walker) evolves on an N-length cycle, jumping along the edges to reach neighboring vertices is permitted. The position space is composed of $\{|x\rangle, x \in \mathbb{Z}_N\}$, and the coin space usually comprises $\{|c\rangle, c \in \{0,1\}\}$. Based on this mathematic model, controlled alternate quantum walks (CAQW) became a major branch of technology for generating QHF. However, coin operations in this technology are two-dimensional ($|0\rangle$ and $|1\rangle$), which is prone to hash collisions, especially in a complex context like blockchain. Therefore, in our proposed system, we adopted LCAQW to generate QHF for traditional and DAG-based blockchains, where there is no longer a uniform expression for the quantum wandering limit distribution density in the triplet coin state [46], and it is better suited as a hash function [47], As shown in Fig. 4.

According to [47], we define shift operators $\hat{S}_0$ and $\hat{S}_1$ of the quantum walker on each vertex x_p as

$$\begin{aligned}\hat{S}_0 = \sum_{x_p \in \mathbb{Z}_{N_q}} & (|x_p + 1(mod\ N_q)\rangle \langle x_p| \otimes |0\rangle \langle 0| \\ & + |x_p - 1(mod\ N_q)\rangle \langle x_p| \otimes |1\rangle \langle 1| \\ & + |x_p + \lambda_0(mod\ N_q)\rangle \langle x_p| \otimes |2\rangle \langle 2|)\end{aligned} \tag{1}$$

$$\begin{aligned}\hat{S}_1 = \sum_{x_p \in \mathbb{Z}_{N_q}} & (|x_p + 1(mod\ N_q)\rangle \langle x_p| \otimes |0\rangle \langle 0| \\ & + |x_p - 1(mod\ N_q)\rangle \langle x_p| \otimes |1\rangle \langle 1| \\ & + |x_p + \lambda_1(mod\ N_q)\rangle \langle x_p| \otimes |2\rangle \langle 2|)\end{aligned} \tag{2}$$

where liveness parameters are subject to $\lambda_0, \lambda_1 \in \mathbb{Z}_{[N_q/2]}$, and $[\cdot]$ means a ceiling function, managing the particle to opt for an extra leap.

Then, we utilize the Grover operator G as the coin operator. $G = 2\left|v_g\right\rangle\left\langle v_g\right| - I_g$, where $\left|v_g\right\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$, and G can be given as following.

$$G = \begin{bmatrix} -\frac{1}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \end{bmatrix} \tag{3}$$

The evolution procedure of the total system is driven by unitary operators $\hat{U}_0, \hat{U}_1 \in \mathcal{H}_{\mathfrak{p}} \otimes \mathcal{H}_{\mathfrak{c}}$, which are regarded as:

$$\hat{U}_0 = \hat{S}_0(\hat{I_{N_q}} \otimes \hat{G}) \tag{4}$$

$$\hat{U}_1 = \hat{S}_1(\hat{I_{N_q}} \otimes \hat{G}) \tag{5}$$

In the procedure of LCAQW with λ_0 and λ_1, the quantum state amplitude of a particle at displacement x_p and step t can be denoted as $|\psi\rangle_{x_p,t} = \left[w^1_{x_p,t}, w^2_{x_p,t}, w^3_{x_p,t}\right]^\dagger = \sum_{\mathfrak{c}_q} w^{\mathfrak{c}_q}_{x_p,t} \left|\mathfrak{c}_q\right\rangle \in \mathcal{H}_{\mathfrak{c}}$, where $\mathfrak{c}_q$ means the amplitude in the coin register. Therefore, the state of the whole quantum system can be represented as

$$|\Psi(t)\rangle = \textstyle\sum_{x_p \in \mathbb{Z}_{N_p}} |x_p\rangle \otimes \left|\psi_{x_p,t}\right\rangle \tag{6}$$

Here, the input message $bmsg$ is used to control the QW of a particle, which is a binary string $'bm_1 bm_2 bm_3 \ldots bm'_t$, where each bit $\{bm_1, bm_2, bm_3, \ldots, bm_t\} \in \{0,1\}^t$. Specifically, the unitary operator $\hat{U}_0$ is adopted when $bm_j = 0$, otherwise, $\hat{U}_1$ will be applied. From this, we can determine the unitary operator controlled by the input message $\hat{U}_{inm} = \hat{U}_{bm_1}\hat{U}_{bm_2}\hat{U}_{bm_3}\ldots\hat{U}_{bm_t}$, where $\hat{U}_{bm_j} \in \left\{\hat{U}_0, \hat{U}_1\right\}, 1 \leq j \leq t$. Subsequently, the evolution of the quantum system from the initial state to the t-th time step with a unitary operator $\hat{U}_{inm}$ can be defined as

$$|\Psi_{inm}\rangle = \hat{U}_{inm}\,|\Psi(t=0)\rangle \tag{7}$$

When the QW of a particle controlled by $bmsg$ performs t steps, the probability of it appearing at the position x_p can be calculated by

$$p_{x_p} = \left\langle \psi_{x_p,t} \middle| \psi_{x_p,t} \right\rangle = \textstyle\sum^3_{\mathfrak{c}_q} \left\| w^{\mathfrak{c}_q}_{x_p,t} \right\|^2 \tag{8}$$

The total probability fulfills the requirement $\sum^3_{\mathfrak{c}_q=1} \sum_{x_p \in \mathbb{Z}_{N_q}} \left\| w^{\mathfrak{c}_q}_{x_p,t} \right\|^2 = 1$, in which $w^{\mathfrak{c}_q}_{x_p,t}$ be achieved by taking a measurement of the basis $|x_p, \mathfrak{c}_q\rangle$ through the following equation.

$$\left| \langle x_p, \mathfrak{c}_q | \left(\hat{U}^t \,|\Psi(t=0)\rangle\right) \right|^2 \tag{9}$$

Given an input binary message $bmsg$ derived from the block information, the QHF based on LCAQW can be generated by following steps with an initial state $|\Psi(t=0)\rangle = |x_p\rangle \otimes |\mathfrak{c}_q\rangle$, where $|\mathfrak{c}_q\rangle = w_1|0\rangle + w_2|1\rangle + w_3|2\rangle$.

1) Initialize a set of parameters $\{w_1, w_2, w_3, N_q, \rho, \delta, C\}$, where w_1, w_2 and w_3 are the amplitudes of coin registers, N_q means QW on an N_q cycle, ρ and δ satisfy the condition $10^\rho \ll 2^\delta$ and coin operator is G like equation (3).
2) Employ $bmsg$ to generate $\hat{U}_{inm}$ and complete the LCAQW, so that each vertex will create a probability $\mathfrak{p}_{x_p}(x_p \in \mathbb{Z}_{N_q})$, which can be calculated by equation (8) and (9), and then the total probability is denoted as $\mathcal{P} = (\mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_{N_q-1})$.
3) Obtain each part of the hash value by scaling up each probability value and performing a mod operation with $h_{x_p} = \left\lfloor \mathfrak{p}_{x_p} \cdot 10^\rho \right\rfloor \mod 2^\delta$. Through combining these δ-bits hashes, the final quantum hash value $h^q = h_0 \,||\, h_1 \ldots ||\, h_{N_q-1}$, where the bit length of h^q is $N_q \times \delta$.

Algorithm 1: ED-QKD algorithm using QKD with the BB84 protocol and AES method

```
Input: Number of quantum bits $n_{ed}$, Raw data $RData$, Indicator character $Str$
Output: Encrypted data $EData$ or Decrypted data $DData$
Initialize quantum circuit;
Initialize a series of quantum bits;
Randomly encode quantum bits on a state in one of two sets of ground states (rectangular or diagonal ground states);
$QKDkey$ ← QKDCirSim($n_{ed}$);
Replace regularly the Quantum Key $QKDkey$;
$QKDkeystr$ ← ListToString($QKDkey$);
$AESkey$ ← SeedToKey($QKDkeystr$);
$Cipher$ ← AESCipher($AESkey$);
if Str == 'Encrypt' then
    $EData$ ← $Cipher$.Encrypt($RData$);
    Return $EData$;
else
    if Str == 'Decrypt' then
        $DData$ ← $Cipher$.Decrypt($EData$);
        Return $DData$;
    end
end
```

B. ED-QKD Algorithm

During the communication for traditional blockchain of the various BUs in the proposed QHB-DA, we proposed a ED-QKD algorithm based QKD with BB84 protocol [48] to ensure the data authenticity. The core idea is to use the uncertainty principle of quantum state and the phenomenon of quantum entanglement to distribute the secret key in the process of synchronizing the traditional blockchain among BUs, and then use the AES key to encrypt and then transmit the data using the quantum key as the seed, and then decrypt the message when the terminal receives it to obtain the original data. The Algorithm 1 shows the process of encryption and decryption. Specifically, the detailed steps are given as follows:

1) *Key Generation:* The sender (BU i) prepares n_{ed} quantum states (e.g., photons), encoding these states in specific ways (usually using two or more orthogonal quantum states to represent binary 0 and 1).

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3479450

Algorithm 2: D2B-QSC Algorithm

```
// Upload data from DAG blockchain to
   traditional blockchain using QSC
Input: Supply Data from DAG Blockchain $DAGData$
Output: Traditional Blockchain $ChainData$
Initialize quantum registers;
Entangle two qubits to create a Bell state;
Connect the network between BUs and full nodes;
Initialize $BinaryData$ as an empty string;
$BellState \leftarrow$ result of the entanglement;
$DAGData \leftarrow$ latest data from the network;
Encrypting $DAGData$ using the ED-QKD Algorithm;
$BinaryData \leftarrow$ ConvertBinary($DAGData$);
$DataLength \leftarrow$ CalculateLength($BinaryData$);
$BLength \leftarrow$ ConvertBinary($DataLength$);
$BinaryData \leftarrow$ Combine($BLength$, $BinaryData$);
Append '0' on $BinaryData$ to keep the length is the
  same;
for pair in $BinaryData$ do
    if pair == '00' then
        Do not apply any operation;
    else
        if pair == '01' then
            pair.Apply(Pauli-Xgate);
        else
            if pair == '10' then
                pair.Apply(Pauli-Zgate);
            else
                pair.Apply(Pauli-Xgate, Pauli-Zgate);
            end
        end
        $EQubit \leftarrow$ QuantumCoding(pair);
        Add $EQubit$ to $EDataArray$;
    end
end
Decrypting $EDataArray$ using the ED-QKD
  Algorithm;
$ConvertedData \leftarrow$ ToBlockchainF($EDataArray$);
$ChainData \leftarrow$ TransferData($ConvertedData$);
```

2) *Quantum Transmission:* BU i sends these quantum states to the receiver (the full node) through a secure quantum channel, such as an optical fiber.
3) *Quantum Measurement:* Upon receiving the quantum states, the full node measures them and extracts the key based on the measurement results. Due to the nature of quantum states, any attacker attempting to intercept the quantum channel would disturb the quantum states, thus being detectable by BU i and the full node.
4) *Error Correction:* BU i and the full node exchange part of their information over a public classical channel to detect and correct errors caused by noise and imperfections in the quantum channel during transmission.
5) *Communication:* BU i encrypts the data with AES using the quantum key as a seed, and BU j decrypts the data once it has been received.

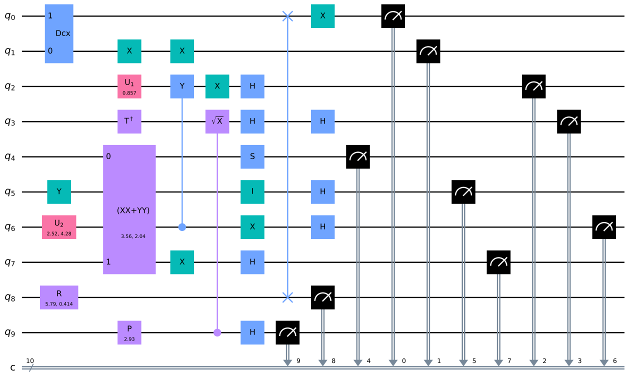


Fig. 5. One of analogue circuits for QKD-based encryption.

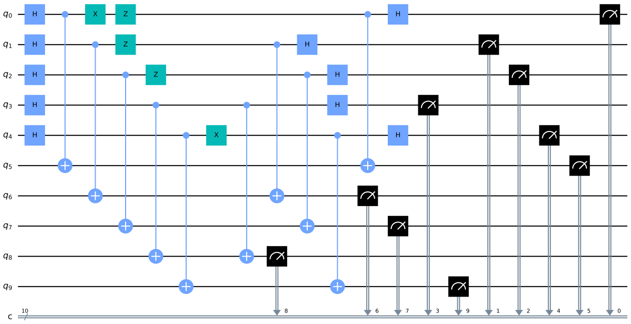


Fig. 6. Analogue circuit for D2B-QSC algorithm.

6) *Key Refresh:* To maintain continuous security of communication, BU i and the full node regularly repeat this process to generate new keys.

C. D2B-QSC Algorithm

In the QHB-DA, the proposed D2B-QSC algorithm based on [49] is employed to efficiently and securely transfer data from the DAG-based blockchain of each BU to the traditional blockchain. Initially, the full node generates a pair of entangled quantum bits, retains some, and sends the others to the nodes of various BUs. Therefore, the BU and the full node that creates the traditional blockchain have a general Bell state, respectively, i.e., they share an entangled pair. When BUs need to upload information, they utilize the quantum bits in their possession to perform QSC, which enables each quantum bit to carry two bits of classical information. Suppose s_1s_0 is a two-character string that the unit wants to send to the full node. s_1s_0 has four possible combinations, which are $\{00, 01, 10, 11\}$. Based on this bit string, the BU chooses one of the four unitary operators $U^Q \in \{I, X, Y, Z\}$ to apply to the entangled bits it owns.

When sending the classic bit s_1s_0, there are four options. If $s_1s_0 =' 00'$, the BU applies $I \otimes I$ to its corresponding Bell state part without having to do any arithmetic. If $s_1s_0 =' 01'$, $'10'$ or $'11'$, the BU adopts $X \otimes I$, $Y \otimes I$ or $XZ \otimes I$ to its corresponding Bell state part, respectively.

The encoded quantum bits are then sent back to the full node, which utilizes the properties of quantum entanglement, performs decoding operations to retrieve the encoded information. The full node combines q_0 with his own corresponding quantum bit q_1 by applying a reversible Bell operation to $q_0 q_1$ to disentangle it. First, a controlled non-gate operation is applied, where q_0 serves as the control bit. Then, a Hadamard transform is applied to the first quantum bit q_0 of the pair, which leads to the disentanglement of the Bell state and yields the unique state corresponding to the two-bit string.

Once the information is read, the full node records it on the traditional blockchain, ensuring efficient and secure integration of information from all BUs and facilitating traceability and verification of the entire supply chain's data. Details of this process are described in Algorithms 2.

V. Cost-Benefit Analysis

In this section, we present a comprehensive cost-benefit analysis of the proposed QHB-DA. By integrating both theoretical formulations and practical considerations, we aim to demonstrate the economic feasibility and efficiency of QHB-DA in Industry 4.0 supply chain scenarios.

A. Cost Factors

1) Development costs: The total development costs C_{dev} of QHB-DA include the quantum hash algorithm C_{qh}, quantum protocols C_{qp}, and blockchain architecture C_{blk}. Utilizing existing technologies and a modular design minimizes development effort. The cost equation is: $C_{dev} \sim (x_q \cdot (C_{qh} + C_{qp}) + x_b \cdot C_{blk})$, where x_q and x_b represent the allocation factors for quantum and blockchain components, respectively. Therefore, the development cost of QHB-DA can be controlled at a level comparable to that of traditional blockchain systems.

2) Operating costs: The costs C_{op} mainly come from computing and network resources, including reduced DAG computation β_{dag}, chained structure computation β_c, and network transmission cost β_n. With $\beta_{dag} \ll \beta_{full}$, where β_{full} represents full node verification in traditional blockchain, QHB-DA significantly lowers operating costs, especially in multi-node supply chain scenarios, by reducing redundant computations through D2B-QSC.

3) Storage costs: The total storage requirement is: $S_{sys} = S_{cri} + S_{val}$, which means storage for critical blocks and validation data. QHB-DA significantly stabilizes the storage cost through the high efficiency of the DAG structure, where the overhead is limited to the critical blocks and important data validation information, which diminishes the repetitiveness of the data storage.

4) Energy costs: Energy costs are associated with quantum protocols E_{qnt} and hash algorithms E_{qh}. Energy consumption for quantum protocols is: $E_{qnt} = \sum_{i=1}^{m} P_i \cdot T_i$, where P_i is the power consumption of the i-th key node, T_i is the execution time, and m is the number of key nodes. The energy consumption E_{qh} remains constant. Hence, QHB-DA achieves low overhead in terms of energy consumption, which is comparable to that of traditional blockchain systems, and even more advantageous in certain high-load scenarios.

5) Maintenance costs: Maintenance costs C_m are manageable due to the modular system, allowing separate updates for quantum c_{mq} and blockchain components c_{mb}, which avoids costly system overhauls.

B. Benefit Factors

1) Enhanced data authenticity and security: QHB-DA uses quantum-resistant algorithms to protect data from future quantum attacks, addressing risks to classical cryptographic systems. Additionally, its enhanced security ensures regulatory compliance, reducing both legal penalties and reputational damage.

2) Efficiency improvements: The hybrid blockchain structure improves transaction throughput and processing efficiency. The reduced need for full-chain validation and minimized redundant computations result in lower computational overhead. Moreover, QHB-DA lowers the requirements for computational and storage resources, leading to cost savings in both hardware utilization and energy consumption.

3) Supply chain value enhancement: QHB-DA improves traceability across the supply chain, enhancing transparency and trust, represented by the traceability improvement factor γ_{tra}. Then, the proposed system fosters collaboration among business units, leading to potential innovation, quantified by the collaboration benefit factor γ_{col}.

C. Net Benefit Analysis

To evaluate the overall net benefit B_{net} of implementing QHB-DA, we consider the balance between the total benefits B_{tt} and the total costs C_{tt}. The total costs encompass development, operating, storage, energy, and maintenance costs, which can be denoted as $C_{tt} = C_{dev} + C_{op} + S_{sys} + E_{tt} + C_m$, where $E_{tt} = E_{qnt} + E_{qh}$. The total benefits include enhanced security, efficiency improvements, and supply chain value enhancements, which is represented as $B_{tt} = B_{sec} + B_{eff} + B_{val}$, where $B_{val} = \gamma_{tra} + \gamma_{col}$.

Substituting the expressions for B_{tt} and C_{tt}, the net benefit can be formulated as

$$B_{net} = B_{tt} - C_{tt} \tag{10}$$

The previous analysis shows that B_{tt} is specific to QHB-DA and C_{tt} is inferior to baseline, therefore B_{net} exceeds the existing system, demonstrating economic feasibility.

D. Sensitivity Analysis

To assess the robustness of the net benefit B_{net} and understand the impact of uncertainties in cost and benefit estimates on the economic feasibility of QHB-DA, we perform a sensitivity analysis. By introducing percentage changes δ_B and δ_C in total benefits and costs, the adjusted net benefit B'_{net} can be calculated as:

$$B'_{net} = (1 + \delta_B) \cdot B_{tt} - (1 + \delta_C) \cdot C_{tt} \tag{11}$$

To prove $B'_{net} \geq 0$, we rearrange the above equation as:

$$\frac{B_{tt}}{C_{tt}} \geq \frac{1 + \delta_C}{1 + \delta_B} \tag{12}$$

This shows that as long as the initial ratio $\frac{B_{tt}}{C_{tt}}$ is sufficiently large, the system remains economically viable even under adverse changes in benefits or costs. Next, we analyze this inequality under different scenarios.

- In an optimistic scenario, where benefits increase ($\delta_B \geq 0$) and costs decrease ($\delta_C \leq 0$), the inequality (12) is naturally satisfied, signifying that the system is economically viable in optimistic conditions.
- In a pessimistic scenario, where benefits decrease ($\delta_B \leq 0$) and costs increase ($\delta_C \geq 0$). Here, the system can remain viable under adverse conditions if the initial ratio is favorable.
- In a neutral scenario, where $\delta_B = 0$ and $\delta_C = 0$, meaning benefits and costs remain unchanged, the net benefit is simply: $B'_{net} = B_{tt} - C_{tt} = B_{net}$.
- In extreme cases, such as complete loss of benefits ($\delta_B \to -1$) or doubling of costs $\delta_C \to +1$, the system can face challenges. This suggests that the system can become economically unviable under extreme conditions. However, such extremes are unlikely to occur in reality, and the system has been designed to ensure that it can remain stable within a reasonable range of fluctuations.

Through the above mathematical analysis, we demonstrate the robustness of the QHB-DA system in different scenarios. The structure and hierarchical design of the system enable it to cope with fluctuations in benefits and costs and maintain economic viability.

VI. Security Analysis

In this section, we conduct a comprehensive the security of QHD-DB through both theory and practice. On the theoretical side, we do statistical diffusion and obfuscation analysis and prove the security of the system under different attacks respectively. On the practical side, we build a threat model that demonstrate the security of the system by analyzing actual data flow diagrams (DFD).

A. Theory Analysis

1) Statistical Diffusion and Confusion: In order to prove the usability of our proposed LCAQW-based QHF, we have done tests on a statistical basis for diffusion and confusion. The standard steps are as follows.

(a) Create a hash $Hash1$ of the original binary message $mesg1$.
(b) Randomly reverse a bit in the $mesg1$ write it as $mesg2$.
(c) Recreate the hash of the modified message $mesg2$ and write it as $Hash2$.
(d) Calculate the number of distinct bits in $Hash1$ and $Hash2$ and denote it as N_i^b.
(e) Repeat the above process T times.

After completing the above test procedure, the following parameters are computed. The average changed number of hash bits is denoted as $\bar{N}^b = \frac{1}{T}\sum_{i=1}^{T} N_i^b$. The average change probability can be expressed as $P = \frac{\bar{N}^b}{N_q \times \delta}\sum_{i=1}^{T} N_i^b \times 100\%$. During T repetitions, the maximum value is N_{max}^b and the minimum value is N_{min}^b. Standard deviations of the changing numbers and probabilities are represented as $\triangle N^b = \sqrt{\frac{1}{T-1}\sum_{i=1}^{T}(N_i^b - \bar{N}^b)^2}$ and $\triangle P = \sqrt{\frac{1}{T-1}\sum_{i=1}^{T}(\frac{N_i^b}{N_q \times \delta} - P)^2} \times 100\%$.

TABLE II
The static number of changed bit

Parameters	$T = 1024$	$T = 2048$	$T = 10000$	Mean
$\bar{N}^b$	63.547	62.971	63.887	63.468
N_{max}^b	82	84	88	84.667
N_{min}^b	43	44	44	43.667
$P(\%)$	49.646	49.196	49.911	49.584
$\triangle\bar{N}^b$	8.404	7.455	7.693	7.851
$\triangle P(\%)$	6.565	5.824	6.010	6.133

In our experiments, we tested with $T = 1024$, 2048, 10000 severally, and the results are shown in the Table II. For LCAQW, we used a 16-Length cycle model ($N_q = 16$) with amplification factor $\rho = 10$ and sub hash length $\delta = 8$. Hence, the length of the hash value obtained is 128 bits, which satisfies the property that for any input, the hash length is fixed. The results show that when we randomly change a bit of the original message, the average number $\bar{N}^b$ and probability P of changes in the corresponding hash values are very close to the ideal values of $(N_q \times \delta)/2$ and 50%. $\triangle\bar{N}^b$ and $\triangle P(\%)$ are very small, which demonstrated the diffusion and confusion of the proposed algorithm. This property guarantees that it is infeasible to forge the corresponding cipher-text if the plaintext is known.

2) Intercept-Resend (IR) Attack: Eve, acting as an eavesdropper within the quantum channel, endeavors to intercept a traceability record of products. This interception facilitates the transmission of counterfeit traceability data across the supply chain to a subsequent block, thereby compromising the QHB-DA protocol. Nevertheless, during the security verification phase, the attacker Eve encounters a challenge in discerning whether the quantum particle adopts a linear or diagonal basis, which results in a 50% probability of error in each prediction. For a single-particle decoy qubit, the probability that an attack is detected can be calculated by $0.5 + 0.5 \times 0.5 = 0.75$. It is posited that the process encompasses Ω_α rounds of quantum state transmissions and Ω_β rounds of security checks within the blockchain over a period, with the total rounds $\Omega = \Omega_\alpha + \Omega_\beta$. Let the coefficient $\vartheta = \Omega_\beta/\Omega$. Consequently, the probability of Eve being detected is 0.75ϑ, $0.75\vartheta + 0.75\vartheta(1 - 0.75\vartheta)$, $0.75\vartheta + 0.75\vartheta(1 - 0.75\vartheta) + 0.75\vartheta(1 - 0.75\vartheta)^2 \ldots$. Therefore, the probability P_{Ira} is $0.75\vartheta\sum_{i=0}^{|b_{msg}|-1}(1 - 0.75\vartheta)^i$ after $|b_{msg}|$ rounds. When $|b_{msg}| \to \infty$, $P_{Ira} \to \infty$, the attack must have been detected.

3) Entangle-Measure (EM) Attack: Assuming Eve initiates an EM attack with the intention of ex-filtrating the cryptographic key and subsequently disseminating a counterfeit product ledger to facilitate double-spending, such an endeavor proves futile. Within the analog circuitry delineated for the D2B-QSC algorithm, as illustrated in Fig. 6, the BU node retains particle 1 in its possession and dispatches particle 2 towards the full node for every distinct state. To glean insights regarding the target qubit, Eve entangles the transmitted particle with an auxiliary particle possessed via unitary transformations. The Unitary operation is $U^Q|0\rangle|A\rangle = \kappa_1|0\rangle|A_0\rangle + \kappa_2|1\rangle|A_1\rangle$, $U^Q|1\rangle|A\rangle = \kappa_3|0\rangle|A_2\rangle + \kappa_4|1\rangle|A_3\rangle$. $|A\rangle$ is the auxiliary particle of the attacker, where $|A_0\rangle$ and $|A_1\rangle$ are orthogonal, $|A_2\rangle$ and $|A_3\rangle$ are orthogonal, and $|\kappa_1|^2 + |\kappa_2|^2 = |\kappa_3|^2 + |\kappa_4|^2$. In the proposed QHD-DA with Eve, $tr_A(U^Q|0\rangle|A\rangle)(\langle A|\langle 0|(U^Q)^\dagger) = tr_A(\kappa_1|0\rangle|A_0\rangle + \kappa_2|1\rangle|A_1\rangle)(\kappa_1^\dagger\langle 0|\langle A_0| + \kappa_2^\dagger\langle 1|\langle A_1|) = \kappa_1\kappa_1^\dagger|0\rangle\langle 0| + \kappa_2\kappa_2^\dagger|1\rangle\langle 1|$. Only when $tr_A(U^Q|0\rangle|A\rangle)(\langle A|\langle 0|(U^Q)^\dagger) = |0\rangle\langle 0|$ will Eve's attack go undetected. Therefore, the particles intercepted by Eve maintain a direct product association with the auxiliary particles introduced by Eve. Notwithstanding Eve's interception of node data within the blockchain, the acquisition of pertinent information through EM attack is rendered ineffective.

4) Forgery Attack: The encryption of a copy node's signature Θ_A with Q_A and the encryption of a new node's signature Θ_C with Q_C, coupled with the unconditional security provided by QKD analogue circuits, where the first two layers are designed as randomized circuits to enable timed replacement of quantum secret keys. One of the analogue circuits is shown as Fig. 5, which ensures the infeasibility of key forgery by an adversary, herein referred to as Eve. In the event that Eve attempts to compromise the protocol by selecting arbitrary bit strings, the primary node's detection probability is significantly high, represented as $P_{Fa} = 1 - 1/2^{(\iota_A + \iota_C)}$, where ι_A and ι_C signify the respective lengths of the keys Θ_A and Θ_C.

5) Impersonation Attack: In an attempt to compromise or alter traceability data within the proposed HB, an adversary, referred to as Eve, needs to masquerade as a legitimate node. This endeavor, however, is rendered futile as the integrity of the data is safeguarded by the exclusive sharing of quantum keys between BUs and full nodes. The absence of this key in the hands of the impersonator, who resorts to use a random binary string, is detected during the authentication phase through the discrepancy in the values of (Q, Θ) and (Q_i, Θ_i), signaling the presence of a fraudulent node.

B. Practical Analysis

The DFD of the threat model helps to visualize and assess potential vulnerabilities in the system, identifying data flows, entities involved and possible points of attack [50]. In Fig. 7, security threats can be systematically identified by mapping external entities, processing, data stores and data flows of QHB-DA. Here, we use the STRIDE method to prove the security of QHB-DA.

1) Spoofing: In QHB-DA, attackers can attempt to impersonate legitimate entities within the supply chain. However, ED-QKD ensures secure authentication, which prevents identity spoofing.

2) Tampering: Data tampering can compromise the integrity of transactions across the supply chain. QHB-DA's quantum hashing promptly detects any alterations, preserving data integrity.

3) Repudiation: Entities can deny actions they have taken within the system, challenging accountability. Immutable DAG and blockchain structures in QHB-DA provide verifiable records, preventing such repudiation.

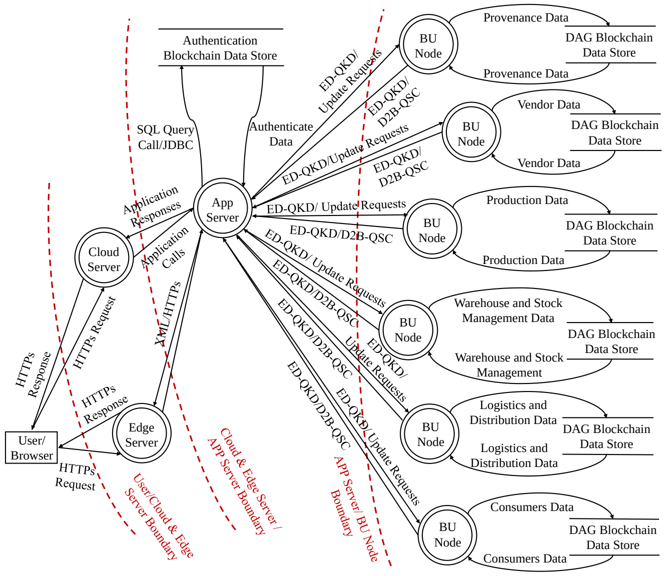


Fig. 7. DFD of QHD-DA for the holistic threat model.

4) Information disclosure: Sensitive data can be exposed during transmission or storage across the supply chain. QHB-DA mitigates this risk by using ED-QKD and D2B-QSC to secure key exchanges and prevent data leaks.

5) Denial of Service: Attackers can attempt to overwhelm RU nodes, disrupting service availability. Distributed architecture and DAG structure in QHB-DA enhance resilience, mitigating the risk of DoS attacks.

6) Elevation of Privilege: Malicious users can try to gain unauthorized access to higher system privileges. Quantum protocols in QHB-DA ensure tight access control, preventing such privilege escalation.

VII. Case Analysis

For empirical validation and practical demonstration of the QHB-DA framework, this section examines its application in a real-world supply chain scenario. The case study is organized into three key parts, including experimental settings, integration and scalability, and empirical validation.

A. Case Background and Analysis Settings

To provide empirical evidence supporting the practical implementation of the QHB-DA framework, we present a case study involving the supply chain of a premium product, specifically Wagyu beef. The supply chain for Wagyu beef typically involves six BUs, including tracking the origin of the cattle, suppliers providing the cattle, slaughterhouses and meat processing plants, storage and inventory control, transportation and delivery, and end customers. Each BU represents distinct entities that operate with their own unique datasets. These datasets differ not only in terms of structure and size but also in the way they interact with the blockchain. The cooperation of

BUs in this supply chain is critical for maintaining the quality and authenticity of Wagyu beef. Traditional blockchain-based traceability solutions, which rely solely on chained data blocks, face significant challenges in the context of the Wagyu beef supply chain. These challenges include:

- Data redundancy: Each BU in the Wagyu beef supply chain maintains a full backup of the blockchain, leading to substantial storage wastage. For example, both the vendor and the warehouse and stock management units might store identical data, resulting in inefficiencies.
- Differences in data structure and consensus mechanisms: Variations in data structures and consensus mechanisms across different units complicate maintenance and integration efforts.
- Quantum computer attacks: With the advent of quantum computing, traditional cryptographic methods used in blockchains are vulnerable to quantum attacks. This poses a significant threat to the authenticity of Wagyu beef data, as quantum computers can potentially break the cryptographic hashes that secure the blockchain, which leads to data tampering and loss of trust in the system.

The aforementioned challenges negatively impact the Wagyu beef supply chain by increasing operational costs, complicating data management, and potentially compromising data authenticity and traceability. For instance, the inability to efficiently manage and verify data can cause delays in identifying and addressing issues such as product recalls or quality control failures. Additionally, the threat of quantum computer attacks further exacerbates these issues by undermining the security and integrity of the Wagyu beef data.

To address the above traceability challenges in supply chains, we built a simulated QHB-DA system using python 3.9. First, we created data structures and related classes in $DAGBlockchain.py$ that BUs can instantiate to build their own DAG blockchain. Then, we created the function $bb84qkdSimu()$ in $DAGencryption.py$ to simulate the algorithmic process of ED-QKD. We also created the function $SDCnbits()$ in $CMcode.py$ to upload the data from the DAG-based blockchain to the traditional blockchain. Finally, the $main()$ function is used to test the whole system. In order to simulate the actual scenario more realistically, qiskit 0.45.1, qistkit-aer 0.13.1 and qiskit-terra 0.45.1 provided by IBM are utilized to build circuits to implement the quantum algorithm. Our experiments are conducted on Windows 11 (23H2). The machine is equipped with Intel (R) Core (TM) i7-10750H CPU @ 2.60GHz 2.59 GHz, 32.0 GB RAM, RTX 2060 GPU.

The study focuses on the complete traceability and data fidelity of a given product through multiple BUs of the supply chain. We collect real-time data from multiple active nodes, each contributing to the overall flow of the supply chain. Utilizing QHB-DA, we monitored, validated, and securely stored all transaction data at these nodes.

B. Integration and Scalability of QHB-DA

1) Modular design: The modular design of the QHB-DA framework is an important advantage for integration with existing systems. The modular design means that the quantum part of the system and the traditional blockchain part are separate and operate independently of each other, which makes integration more flexible. Our scheme allows for a gradual transition of existing systems to QHB-DA, rather than needing to replace the entire system at once. Specifically, parts of the traditional blockchain can remain unchanged, while the quantum security features in Fig. 2 can be introduced gradually as a separate module. Existing supply chain systems can continue to operate while starting to use the quantum security features of QHB-DA.

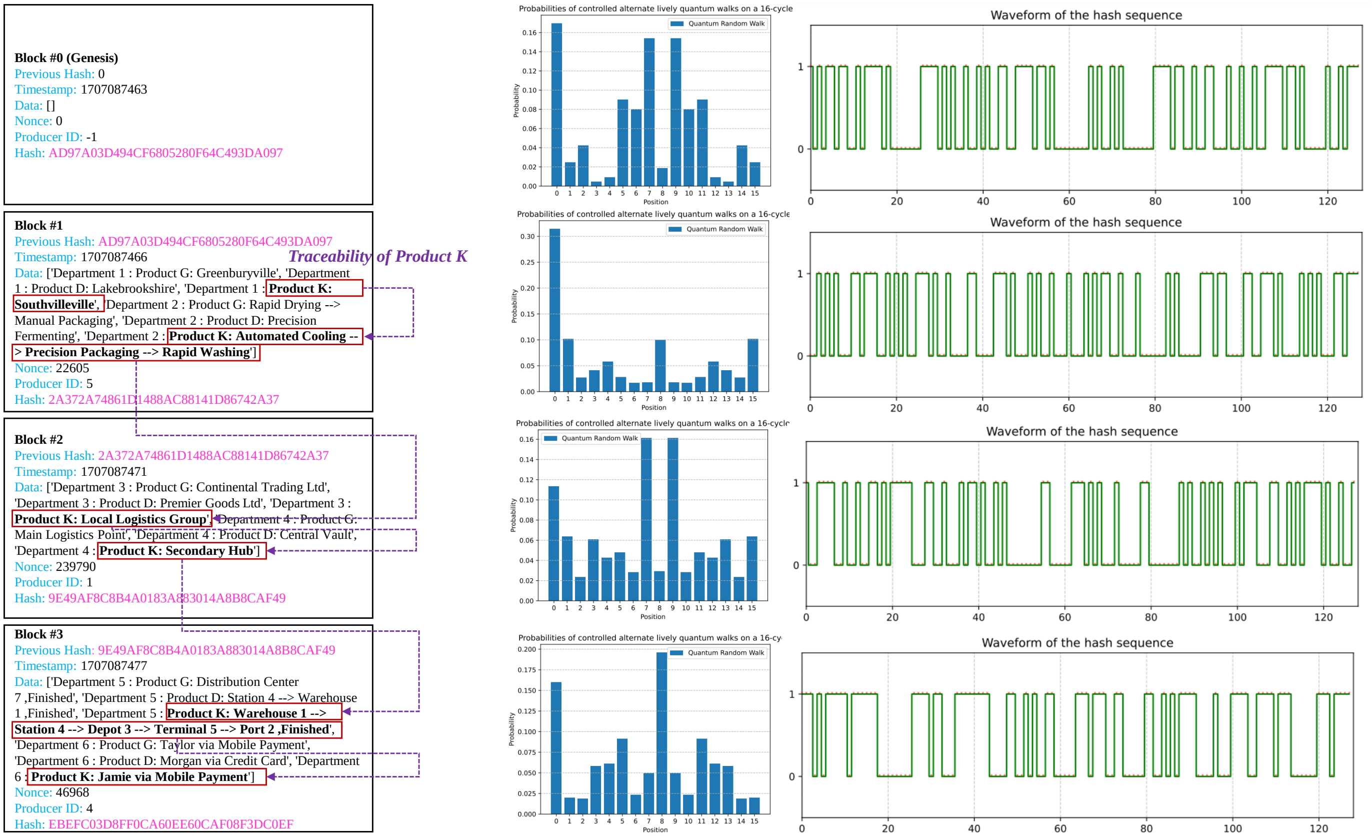
2) Data format and processing flow: The application layer uses a data conversion interface that complies with Electronic Data Interchange (EDI) standards, which allows data from existing SCM systems to be processed by the hybrid structure of QHB-DA. This safeguards against data loss, maintains traceability and integrity, and enables seamless integration with legacy systems. The EDI compliance guarantees that data exchange between different entities follows standardized formats, ensuring consistent and reliable communication across the supply chain.

3) Scalability: The DAG structure in the QHB-DA enhances scalability and processing efficiency by enabling parallel block and transaction processing. Unlike traditional blockchain systems, where each node must verify the entire chain, DAG allows nodes to concurrently process and validate different transactions, effectively reducing redundant computations. This parallelism not only accelerates transaction throughput but also supports distributed processing, making individual nodes in the supply chain independently handle their own data. Individual nodes in the supply chain can process their own data independently without relying on node-wide validation, which improves distributed processing capabilities and scalability in multi-node scenarios.

C. Empirical Valuation

Comprehensive experiments are conducted to demonstrate the applicability and effectiveness of the QHB-DA framework in real-world supply chain scenarios.

Here, a Wagyu beef supply chain was monitored, focusing on the complete traceability. The lifecycle of products, from production to final delivery, was traced through multiple supply chain nodes. Each node generated and processed real-time data, which was verified and stored in the QHB-DA framework. In the left of Fig. 8, we take the first four blocks of the traditional blockchain in QHB-DA as a retrospective demonstration. In the right, we give the probability distribution and the corresponding QHF for LCAQW simulation. As can be understood from the security analysis in the previous part and the uneven distribution of hashes in the figure, this quantum hybird blockchain is not only resistant to quantum attacks, but also fully secure to the level of an ordinary blockchain, which is completely tamper-proof. We use product K to stand for Wagyu beef and can derive that: the origin of the product K is 'Southvilleville'. The processing shows that K goes through 'Automated Cooling', then 'Precision Packaging', then 'Rapid Washing', and then it goes to the supplier 'Local Logistics Group'. The sale goes to the warehouse 'Secondary



Block #0 (Genesis)
Previous Hash: 0
Timestamp: 1707087463
Data: []
Nonce: 0
Producer ID: -1
Hash: AD97A03D494CF6805280F64C493DA097

Block #1
Previous Hash: AD97A03D494CF6805280F64C493DA097
Timestamp: 1707087466
Data: ['Department 1 : Product G: Greenburyville', 'Department 1 : Product D: Lakebrookshire', 'Department 1 : **Product K: Southvilleville**', 'Department 2 : Product G: Rapid Drying --> Manual Packaging', 'Department 2 : Product D: Precision Fermenting', 'Department 2 : **Product K: Automated Cooling --> Precision Packaging --> Rapid Washing**']
Nonce: 22605
Producer ID: 5
Hash: 2A372A74861D1488AC88141D86742A37

Block #2
Previous Hash: 2A372A74861D1488AC88141D86742A37
Timestamp: 1707087471
Data: ['Department 3 : Product G: Continental Trading Ltd', 'Department 3 : Product D: Premier Goods Ltd', 'Department 3 : **Product K: Local Logistics Group**', 'Department 4 : Product G: Main Logistics Point', 'Department 4 : Product D: Central Vault', 'Department 4 : **Product K: Secondary Hub**']
Nonce: 239790
Producer ID: 1
Hash: 9E49AF8C8B4A0183A883014A8B8CAF49

Block #3
Previous Hash: 9E49AF8C8B4A0183A883014A8B8CAF49
Timestamp: 1707087477
Data: ['Department 5 : Product G: Distribution Center 7 ,Finished', 'Department 5 : Product D: Station 4 --> Warehouse 1 ,Finished', 'Department 5 : **Product K: Warehouse 1 --> Station 4 --> Depot 3 --> Terminal 5 --> Port 2 ,Finished**', 'Department 6 : Product G: Taylor via Mobile Payment', 'Department 6 : Product D: Morgan via Credit Card', 'Department 6 : **Product K: Jamie via Mobile Payment**']
Nonce: 46968
Producer ID: 4
Hash: EBEFC03D8FF0CA60EE60CAF08F3DC0EF

Traceability of Product K
Probabilities of controlled alternate lively quantum walks on a 16-cycle
Quantum Random Walk
Probability
Position
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Waveform of the hash sequence
1
0
0 20 40 60 80 100 120

Fig. 8. The supply chain traceability, probabilities of each vertex, and binary waveform of quantum hash in traditional blockchain.

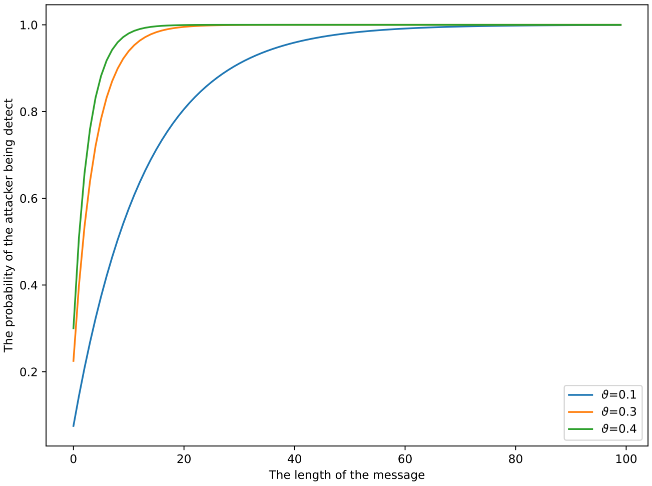


Fig. 9. The probability of the attacker being detected under IR attack varies with the length of the message.

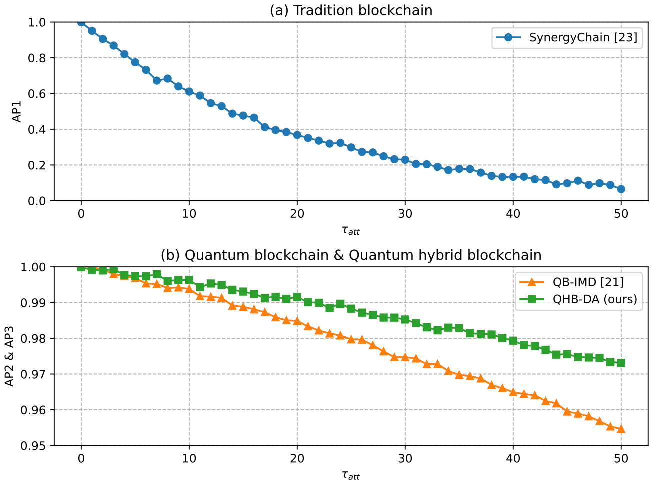


Fig. 10. Comparison of APs of three types of blockchains under different attack strengths τ_{att}.

Hub', and then the logistic process is from 'Warehouse 1', to 'Station 4', to 'Depot 3', to 'Terminal 5', and ends at 'Port 2'. Finally, the consumer 'Jamie' pays for the product K with a 'Mobile Payment'. The traceability process for other products can be similarly derived from the figure. While this testing focuses on specific supply chain scenarios, the QHB-DA framework is designed to be highly adaptable and scalable across various industrial contexts. The modular nature of the framework allows it to be customized for different types of supply chains, whether small-scale local operations or large-scale global networks.

The Fig. 9 shows the probability of an attacker being detected under IR attack as the length of the message varies. There are three curves representing three different ϑ values $(0.1, 0.3, 0.4)$. With the increasing of the length, the probability of detection sharply rises and then levels off. The curve

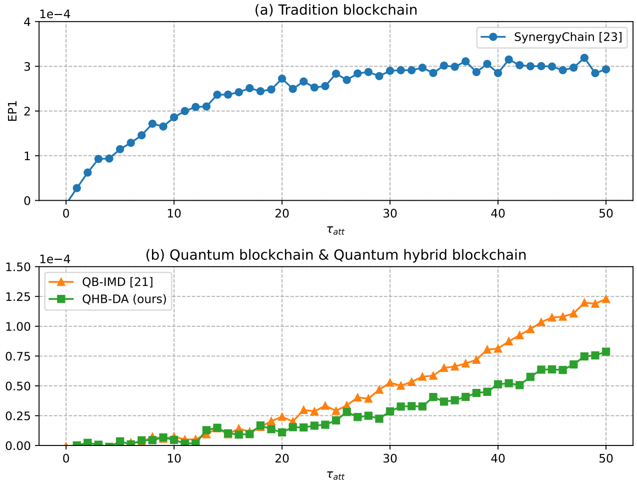


Fig. 11. Comparison of EPs of three types of blockchains under different attack strengths τ_{att}.

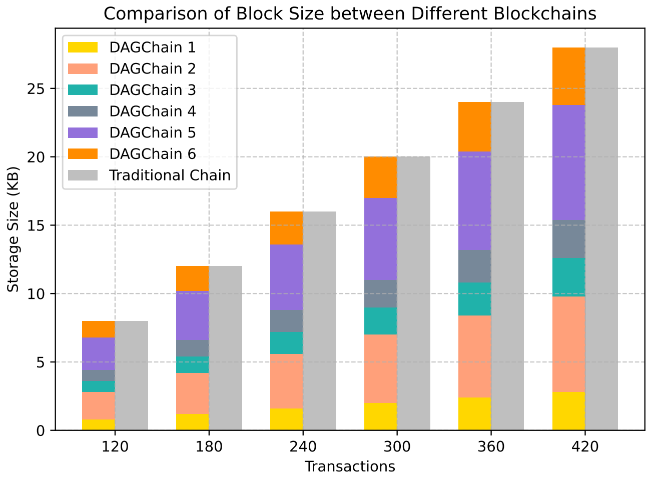


Fig. 12. Comparison of chain size between DAG-based blockchains for six BUs and a integrated traditional blockchain

with the larger ϑ value (green, $\vartheta = 0.4$) rises the fastest and reaches the high-probability threshold the quickest, which indicates that the system has greater robustness against attacks when the ϑ value is larger. Since blocks are generally very long in length when converted into binary strings, the attacks can almost always be detected in the proposed QHB-DA. However, the ϑ value should be set as large as possible to be on the safe side.

In Fig. 10 and 11, we compare available probabilities (APs) and escape probabilities (EPs) of traditional blockchain, quantum blockchain and QHB under various attack strengths τ_{att} after further system testing. The probabilities of these three types of blockchains are denoted as (AP1, EP1), (AP2, EP2) and (AP3, EP3), respectively. The EP is used to measure the risk that the system does not detect a problem, while the AP measures the ability of the system to function properly when needed. According to the definition of attack scenarios in [51], We assume that the attack strengths is the reciprocal of the attack failure time, i.e., $\tau_{att} = 1/t_{fail}$. The fig. 10 (a) shows that the AP of the traditional blockchain significantly decreases with the increase in attack strength τ_{att}, falling from 1.0 to below 0.2, which demonstrates a rapid decline in resistance of the system as the τ_{att} increases. In the fig. 10 (b), the quantum blockchain and QHB demonstrate better stability in their APs. Notably, the QHB (our system) outperforms QB-IMD [21], maintaining higher AP values (above 0.97) even under stronger attacks. The fig. 11 (a) presents the EP of the traditional blockchain gradually increases with the rise of τ_{att}. In fig. 11 (b), as τ_{att} increases, the EP of QB-IMD [21] gradually rises, but at a rate and final probability lower than that of the traditional blockchain. Meanwhile, the QHB maintains an extremely low level of EP, with almost no change across all tested attack strengths. Overall, the QHB demonstrates superior security as its AP is high and EP remains very low even under high-strength attacks, illustrating the potential of QT and hybrid structure.

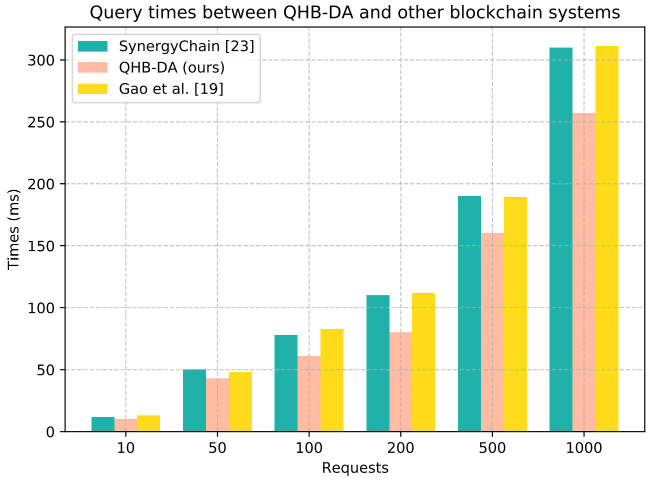


Fig. 13. Query times between ours and other blockchain systems

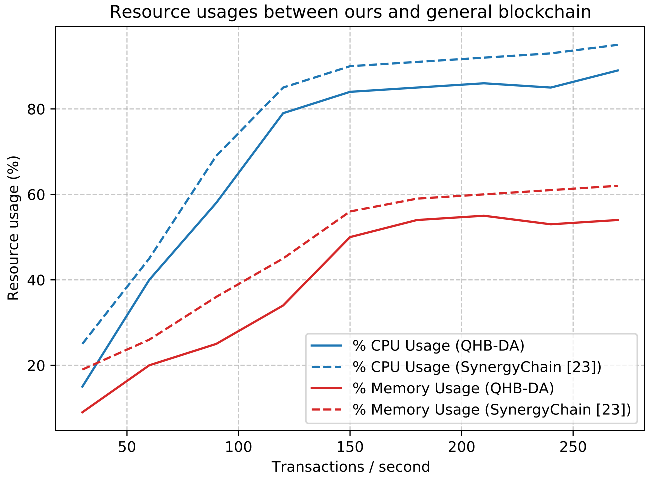


Fig. 14. Percentage of different resource usages between ours and general blockchain

The Fig. 12 The graph displays the proportion of occupancy

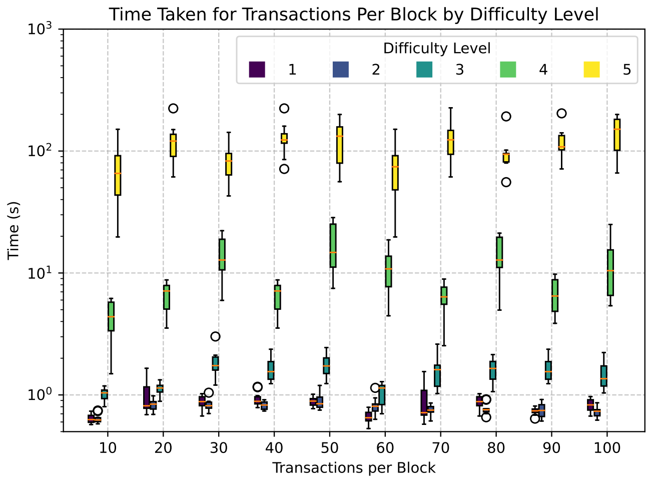


Fig. 15. Time taken to complete a mine at different nonce difficulty levels and different transaction in one traditional block.

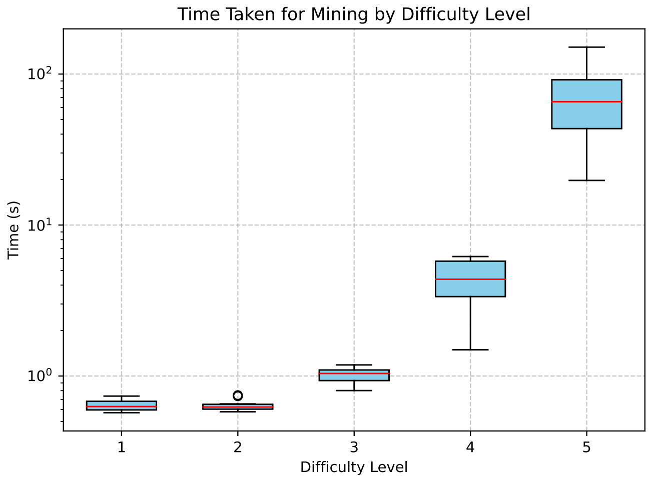


Fig. 16. Time taken to complete a mine at different nonce difficulty levels.

for block sizes between six different DAG-based blockchains for six BUs and an integrated traditional blockchain at various transaction volumes. As the number of transactions increases, the block size of all blockchains grows correspondingly. Most DAG blockchains demonstrate higher storage efficiency, particularly DAGChain 1, 3, 4, whose block sizes are relatively small across all transaction volumes. The result shows that this system provides an excellent solution for improving the scalability of the blockchain. There is no need for each BU to store entire blockchain information and still ensure data traceability. This is a great scheme for certain BUs that have fewer storage resources and significantly reduces storage costs.

In Fig. 13, we compare the query times among SynergyChain [23], the proposed QHB-DA and Gao et al. [19] across various numbers of requests. It is evident from the figure that as the number of requests increases, the query times for both blockchains also rise. Across all levels of requests, the QHB-DA consistently exhibits lower query times compared to Gao et al. [19] and SynergyChain [23], especially when the number of consecutive queries exceeds 100, which indicates that the QHB-DA is more efficient in processing query requests.

Fig. 14 illustrates the percentage of resource usage between our QHB-DA and SynergyChain [23] at various transactions per second. The QHB-DA shows a lower percentage of CPU usage compared to the general blockchain, showing higher efficiency in processing the same volume of transactions. On the memory side, the usage percentage for QHB-DA is also slightly lower than that of the SynergyChain [23], particularly noticeable when the transactions per second are 100. These results suggest that QHB-DA requires lower memory resources when dealing with a high volume of transactions.

Fig. 15 provides an in-depth view of the distribution of time required to process transactions per block during the blockchain mining process, across different difficulty levels ranging from 1 to 5. Across all difficulty levels, as the number of transactions per block increases, both the median time and the range of variation rise. The lower difficulty levels (1 and 2) show a smaller spread between the median time and the range, which reflects better stability and predictability in time estimation. At higher difficulty levels (especially 4 and 5), the dispersion of time significantly increases, suggesting that the variability in time taken to process the same number of transactions is greater under high difficulty, increasing uncertainty.

In Fig. 16, it is evident that there is a nonlinear relationship between the nonce difficulty level and the time taken to mine. Here, the nonce difficulty level is the number of '0' before the hash value. The time required for mining increases exponentially with each increment in difficulty level. This is particularly evident when comparing the median values between each level, where the time increases by orders of magnitude. For blockchain networks, the finding suggests that as the difficulty level increases, the network might experience longer delays in block creation, which can lead to slower transaction confirmations and potential network congestion. Therefore, it is of paramount importance to determine a good difficulty level for mining.

VIII. Conclusion

To achieve a secure, quantum computer-resistant, easily extensible data authenticity architecture in supply chain, this paper proposes a quantum hybrid blockchain framework named QHB-DA. The whole system is divided into five layers, including both DAG-based structure and traditional chain, and encrypts blocks using QHF, ED-QKD and D2B-QSC algorithms to ensure that they are not attacked by quantum computers. The hybird structure greatly reduces data redundancy, allowing BUs in supply chain to complete product traceability without having to store complete blocks of data. QHF ensures that the block information is theoretically immune to modification, in which statistical diffusion and confusion are proved mathematically. ED-QKD utilizes QKD technology as a seed to encrypt and decrypt the information with AES, which prevents attackers from eavesdropping on the secret keys during the communication process. BUs in the supply chain that are involved in building the blockchain change quantum keys with full nodes on a regular basis to maintain the security of the encryption system. D2B-QSC employs QSC technology, which not only improves the efficiency of block consolidation, but also avoids EM attacks. Cost-benifit and security analysis are presented and discussed in detail through modeling and practice. Considering the current experimental conditions and technological limitations, our work has to remain at the level of theory and simulation. In the future, we can make use of real quantum computers and optical quantum technology to enhance the feasibility and practicality of the present framework. We will also focus on testing the QHB-DA framework using diverse datasets obtained from various industries and geographical regions.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, 2008.

[2] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[3] K. F. Schulz and D. Freund, "A multichain architecture for distributed supply chain design in industry 4.0," in *Business Information Systems Workshops: BIS 2018 International Workshops, Berlin, Germany, July 18–20, 2018, Revised Papers 21*. Springer, 2019, pp. 277–288.

[4] W. Bauer, S. Schlund, D. Marrenbach, and O. Ganschar, "Industrie 4.0–volkswirtschaftliches potenzial für deutschland," *Berlin/Stuttgart*, 2014.

[5] M. Rüßmann, M. Lorenz, P. Gerbert, M. Waldner, J. Justus, P. Engel, and M. Harnisch, "Industry 4.0: The future of productivity and growth in manufacturing industries," *Boston consulting group*, vol. 9, no. 1, pp. 54–89, 2015.

[6] K. Huang, "Data authenticity," in *A Comprehensive Guide for Web3 Security: From Technology, Economic and Legal Aspects*. Springer, 2023, pp. 177–200.

[7] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: trick or treat?" in *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23*. Berlin: epubli GmbH, 2017, pp. 3–18.

[8] A. Bahga, "Blockchain platform for industrial internet of things," Scientific Research Publishing, Tech. Rep., 2016.

[9] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[10] S. Park and H. Kim, "Dag-based distributed ledger for low-latency smart grid network," *Energies*, vol. 12, no. 18, p. 3570, 2019.

[11] S. Dange and M. Chatterjee, "Iot botnet: The largest threat to the iot network," in *Data Communication and Networks: Proceedings of GUCON 2019*. Springer, 2019, pp. 137–157.

[12] S. Alam, S. T. Siddiqui, A. Ahmad, R. Ahmad, and M. Shuaib, "Internet of things (iot) enabling technologies, requirements, and security challenges," in *Advances in Data and Information Sciences: Proceedings of ICDIS 2019*. Springer, 2020, pp. 119–126.

[13] R. Singh, A. D. Dwivedi, and G. Srivastava, "Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention," *Sensors*, vol. 20, no. 14, p. 3951, 2020.

[14] S. Popov, "The tangle," *White paper*, vol. 1, no. 3, p. 30, 2018.

[15] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in internet of things," *Optics & Laser Technology*, vol. 124, p. 105942, 2020.

[16] A. A. Abd EL-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5g networks," *Future generation computer systems*, vol. 100, pp. 893–906, 2019.

[17] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, "Towards quantum-secured permissioned blockchain: Signature, consensus, and logic," *Entropy*, vol. 21, no. 9, p. 887, 2019.

[18] D. Rajan and M. Visser, "Quantum blockchain using entanglement in time," *Quantum Reports*, vol. 1, no. 1, pp. 3–11, 2019.

[19] Y.-L. Gao, X.-B. Chen, G. Xu, K.-G. Yuan, W. Liu, and Y.-X. Yang, "A novel quantum blockchain scheme base on quantum entanglement and dpos," *Quantum Information Processing*, vol. 19, pp. 1–15, 2020.

[20] C. Li, Y. Tian, X. Chen, and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Information Sciences*, vol. 546, pp. 253–264, 2021.

[21] Z. Qu, Y. Meng, B. Liu, G. Muhammad, and P. Tiwari, "Qb-imd: A secure medical data processing system with privacy protection based on quantum blockchain for iomt," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 40–49, 2023.

[22] Y. Cao, W. Fan, Y. Wang, and K. Yi, "Querying shared data with security heterogeneity," in *Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data*, 2020, pp. 575–585.

[23] J. Chang, J. Ni, J. Xiao, X. Dai, and H. Jin, "Synergychain: A multichain-based data-sharing framework with hierarchical access control," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14 767–14 778, 2021.

[24] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, "Blockchain in oil and gas industry: Applications, challenges, and future trends," *Technology in society*, vol. 68, p. 101941, 2022.

[25] M. Smits and J. Hulstijn, "Blockchain applications and institutional trust," *Frontiers in Blockchain*, vol. 3, p. 5, 2020.

[26] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with ibm," *The Journal of the British Blockchain Association*, vol. 1, no. 1, 2018.

[27] K. Wüst and A. Gervais, "Do you need a blockchain?" in *2018 crypto valley conference on blockchain technology (CVCBT)*. IEEE, 2018, pp. 45–54.

[28] S. Xuan, L. Zheng, I. Chung, W. Wang, D. Man, X. Du, W. Yang, and M. Guizani, "An incentive mechanism for data sharing based on blockchain with smart contracts," *Computers & Electrical Engineering*, vol. 83, p. 106587, 2020.

[29] W. Chen, Y. Chen, X. Chen, and Z. Zheng, "Toward secure data sharing for the iov: A quality-driven incentive mechanism with on-chain and off-chain guarantees," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1625–1640, 2019.

[30] M. El-Hindi, C. Binnig, A. Arasu, D. Kossmann, and R. Ramamurthy, "Blockchaindb: A shared database on blockchains," *Proceedings of the VLDB Endowment*, vol. 12, no. 11, pp. 1597–1609, 2019.

[31] H. Pervez, M. Muneeb, M. U. Irfan, and I. U. Haq, "A comparative analysis of dag-based blockchain architectures," in *2018 12th International conference on open source systems and technologies (ICOSST)*. IEEE, 2018, pp. 27–34.

[32] B. Kusmierz, "The first glance at the simulation of the tangle: discrete model," *IOTA Found. WhitePaper*, pp. 1–10, 2017.

[33] W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate internet-of-things data," *Future generation computer systems*, vol. 112, pp. 307–319, 2020.

[34] B. Wang, Q. Wang, S. Chen, and Y. Xiang, "Security analysis on tangle-based blockchain through simulation," in *Information Security and Privacy: 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30–December 2, 2020, Proceedings 25*. Springer, 2020, pp. 653–663.

[35] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of pow, pos and dag based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480–485, 2020.

[36] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph-based ledger for internet of things: Performance and security analysis," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1643–1656, 2020.

[37] Q. Wang, T. Wang, Z. Shen, Z. Jia, M. Zhao, and Z. Shao, "Re-tangle: A reram-based processing-in-memory architecture for transaction-based blockchain," in *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2019, pp. 1–8.

[38] Q. Wang, Z. Jia, T. Wang, Z. Shen, M. Zhao, R. Chen, and Z. Shao, "A highly parallelized pim-based accelerator for transaction-based blockchain in iot environment," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4072–4083, 2019.

[39] S. Shafeeq, S. Zeadally, M. Alam, and A. Khan, "Curbing address reuse in the iota distributed ledger: A cuckoo-filter-based approach," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1244–1255, 2019.

[40] Z. Dong, E. Zheng, Y. Choon, and A. Y. Zomaya, "Dagbench: A performance evaluation framework for dag distributed ledgers," in *2019 IEEE 12th international conference on cloud computing (CLOUD)*. IEEE, 2019, pp. 264–271.

[41] S. Park, S. Oh, and H. Kim, "Performance analysis of dag-based cryptocurrency," in *2019 IEEE International Conference on Communications workshops (ICC workshops)*. IEEE, 2019, pp. 1–6.

[42] H. Hasanova, U.-j. Baek, M.-g. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. 29, no. 2, p. e2060, 2019.

[43] N. Raychev, "Quantum blockchain," *Quantum Rev. Lett., 1*, vol. 2, no. 2, pp. 10–37 686, 2020.

[44] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[45] S. E. Venegas-Andraca, "Quantum walks: a comprehensive review," *Quantum Information Processing*, vol. 11, no. 5, pp. 1015–1106, 2012.

[46] M. Štefaňák, I. Bezděková, and I. Jex, "Limit distributions of three-state quantum walks: the role of coin eigenstates," *Physical Review A*, vol. 90, no. 1, p. 012342, 2014.

[47] P. Hou, T. Shang, Y. Zhang, Y. Tang, and J. Liu, "Quantum hash function based on controlled alternate lively quantum walks," *Scientific Reports*, vol. 13, no. 1, p. 5887, 2023.

[48] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical computer science*, vol. 560, pp. 7–11, 2014.

[49] A. Harrow, P. Hayden, and D. Leung, "Superdense coding of quantum states," *Physical review letters*, vol. 92, no. 18, p. 187901, 2004.

[50] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[51] S. Brown, "Overview of iec 61508 design of electrical/electronic/programmable electronic safety-related systems," *Computing and Control Engineering Journal*, vol. 11, no. 1, pp. 6–12, 2000.

Kening Zhang received the B.Eng. at the School of Computer Science and Technology from Anhui University in 2021, and M.Sc. at the Department of Computing of The Hong Kong Polytechnic University in 2022, respectively.

He is currently a Ph.D. student at the Department of Industrial and Systems Engineering of The Hong Kong Polytechnic University. His main research areas include blockchain, Internet of Things (IoT), quantum technology and distributed system.

Carman K. M. Lee (Senior Member, IEEE) received the B.Eng. degree in manufacturing engineering and Ph.D. degree in industrial and systems engineering from The Hong Kong Polytechnic University (PolyU), Hong Kong, China, in 2000 and 2004, respectively. She is currently an Associate Professor with the Department of Industrial and Systems Engineering, PolyU, where she is also the Program Leader of [B.Sc. (Hons.)] Enterprise Engineering with Management and the Lab-in-Charge of the Cyber Physical Systems Laboratory.

Dr. Lee has published more than 130 articles in various international journals and seminars. Her research interests include logistics and supply chain management, the Industrial Internet of Things (IIoT), cyber-physical systems, data analytics, and swam intelligence optimization. Dr. Lee was awarded the Silver Medal at the 47th International Exhibition of Inventions of Geneva in 2019 and the Outstanding Paper Award of Emerald Network Awards in 2019.

Yung Po Tsang (M'20) is currently a Lecturer at the Department of Industrial and Systems Engineering of The Hong Kong Polytechnic University. He received his BSc (Hons) in Logistics Engineering Management and PhD in the Department of Industrial and Systems Engineering from The Hong Kong Polytechnic University in 2015 and 2020, respectively. His current research areas cover artificial intelligence for decision-making, industry 4.0 technologies, and cold chain e-fulfilment.

Dr Tsang received the Outstanding Paper Award in IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) 2023, and 2019 Highly Commended Award from Emerald Literati Awards. He is also the certified ESG planner CEP®, committee member of manufacturing and industrial engineering section of IET Hong Kong, and council member of Hong Kong Logistics Association.