International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I11P101

Volume 74 Issue 11, 1-17, November 2026
© 2026 Seventh Sense Research Group®

Review Article

Electronic Payment Security in the Quantum Era: Evolution, Vulnerabilities, and Systematic Insights

A. Suganthi[1], K. Vidya[2]

[1,2]*Department of Information Science and Technology, College of Engineering, Anna University, Chennai, Tamilnadu, India.*

[1]*Corresponding Author: suganthiar93@gmail.com*

Received: 10 April 2026 Revised: 18 August 2026 Accepted: 26 August 2026 Published: 25 November 2026

Abstract *- Quantum technology is viewed as revolutionary for a digital economy, with quantum e-payment systems expected to offer new levels of security and transaction speed in the world of online financial transactions. This study, therefore, outlines the prospects of quantum technology with respect to e-payment systems towards redefining a safer and more efficient payment experience, considering several technological advancements that have been recently realized. This investigation is structured as a systematic analysis of research articles, where a total of 23 articles were identified, with those in-press articles, conference papers, review articles, and non-English publications being excluded. After analysing each article's objective and its context, a total of 13 studies were selected by adhering to the standard guidelines of the PRISMA statement in 2020. The 13 selected studies were categorized into two segments based on the primary technologies used, comprising 7 studies on Quantum E-Payment Systems and 6 studies on Blockchain-Integrated Quantum E-Payment Systems. The selected studies were analysed based on common criteria, including methodologies, security protocols, performance, strengths and limitations, and attack resistance, which points out three key factors responsible for the acceleration of quantum e-payment systems, namely quantum cryptography, quantum key distributions, and integration with blockchain systems. Such quantum-based technologies improve the current e-payment systems in terms of security, efficiency, and reliability to withstand future threats and disruptions. The specific timeline and curated database selection allow for a precise, high-resolution systematic analysis of the performance and security trade-offs of emerging quantum-resistant solutions; thus, the study establishes a robust foundation for next-generation secure financial transaction models.*

Keywords *- Quantum e-payment system, Quantum cryptography, Quantum Key Distribution, Information security, Blockchain.*

1. Introduction

All aspects of computer technologies, and with them electronic payment systems, develop rapidly with the advancement of quantum computing and quantum cryptography [1, 2]. Quantum e-payment systems conduct financial transactions through quantum mechanical principles to ensure security, efficiency, and reliability [3, 4]. Key quantum cryptographic techniques used in quantum e-payment systems include: One of the first elements developed in Quantum Information Science is Quantum Key Distribution (QKD), which enables two distant parties to establish a shared secret cryptographic key [5-7]. This is done under unconditional security, based on the principles of quantum mechanics. The most widely used QKD protocol is the BB84, introduced by Bennett and Brassard in 1984 [6-8]. Other tools are Quantum Digital Signatures (QDS), which complement QKD. The quantum digital signature confirms that the message is both authentic and, at the same time, intact [9-11]. They take advantage of the quantum states being tamper-evident since it is impossible for an attacker to clone the quantum signature due to the no-cloning theorem [3, 7, 12]. Quantum proxy blind signatures enable untraceable transactions [9, 13]. Such signatures make it possible for a proxy to sign a document on behalf of a user without revealing the content, while both maintaining the user's anonymity and data privacy [9, 11, 13]. A few of the proposed protocols with multi-proxy and group blind signatures increase the flexibility and scalability of the system [13-15].

The greatest benefit of quantum e-payment systems is the guaranteed strong security [7, 8, 16]. Quantum cryptographic techniques, based on the principles of quantum mechanics, promise to provide security that is not conditional on computational complexity [7, 8]. Another feature quantum e-payment systems have is enhanced privacy and anonymity [9, 10]. Quantum blind signature schemes respect the fact that users' transaction details have to be kept confidential so that clients' privacy remains intact, noting possible breaches and misuses of the respective data [11, 13]. Another benefit is quantum attack resistance. As quantum computers have been developed and are currently being made, they are acting as a potential threat to classical cryptographic systems [2, 16].

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

In contrast, quantum cryptographically proven techniques will resist such attacks and guarantee that transactions in finance are secure over the long term [7, 8]. One limitation of quantum e-payment systems is the technical complexity and huge resource requirements for implementation [17]. To give a precise example, Quantum Key Distribution systems depend on specialized hardware, such as single-photon sources and detectors, which are expensive and difficult to incorporate into existing infrastructure [7, 8]. Also, maintaining coherence quantum over long distances, in general, involves sophisticated error correction methods and quantum repeaters, which are, so far, mostly at a preliminary development stage [3, 7]. The major challenge in quantum e-payment systems is scalability. As of now, the existing quantum communication systems have not proved efficient enough for transaction volumes [17]. One possibility is that, due to the complex requirements of managing quantum states in very large networks, scaling would be suboptimal [3]. As well, quantum network solutions are characterized by highly costly deployment over large geographical areas, which may be prohibitive for most financial institutions [17]. Another limitation is the difficulty in incorporating quantum e-payment systems with existing financial infrastructures [2, 18]. However, these advances in quantum e-payment systems have few parallels or case studies in real-world applications. Most proposed works remain at the experimental level, with few actual applications demonstrating the feasibility and effectiveness of quantum e-payment systems [19]. Moreover, despite the increasing number of studies on quantum cryptography and secure electronic payment protocols, a systematic understanding of the evolution of electronic payment security, existing vulnerabilities, and the transition to quantum-secure payment systems remains limited, making it difficult to identify current research trends and implementation challenges [17-20].

Accordingly, this systematic literature review provides a comprehensive overview of quantum e-payment systems through an integrated analysis of the evolution of electronic payment security, recent advances in quantum-secure payment technologies, associated vulnerabilities, and implementation challenges, offering a unified perspective. Next, the paper identifies the key difficulties and constraints of these systems from technical, economic, and legal perspectives to guide future research efforts. A synthesis of the existing literature discusses the current status of quantum e-payment systems, providing valuable insights for researchers, policymakers, and industry stakeholders on the benefits and challenges of these innovative payment solutions.

2. History and Foundation of the E-Payment System

In fact, the payment systems originated in the early 20th century when Electronic Funds Transfer (EFT) made its debut. Back then, the EFT system was used for telegraphic transfer in essence and evolved with the invention of automated clearing houses in the 1960s. These allowed electronic processing to be done on high volumes of transactions between banks and reduced tremendously the checks that were being cleared on paper [21]. By late in the late 1990s and early 2000s, the arrival of the internet provided a space for such monumental improvements in the online payment systems [22]. In this very period, PayPal was developed and allowed a breakthrough in online payments via the provision of an integrated, friendly platform for e-commerce transactions securely [23].

One of the most significant milestones happened in the late 1990s when PayPal came into being; it is a secure, easy-to-use marketplace for online activity and has essentially redefined e-commerce with regard to simplifying transactions between buyers and sellers [22, 23]. As threats on cyber networks became more developed and sophisticated, MFA methods were adopted with enhanced layers of security added to online payment [24, 25]. MFA principles have become indispensable for countering risks associated with single-factor authentication protocols [24]. Development in this area is moving ahead in an effort to gradually catch up with growing needs for secure mechanisms required in digital payment systems [26, 27].

2.1. How the E-payment System works?

By definition, an electronic payment system or e-payment is a means of making transactions, be it buying products or services through digital means, without the usage of physical cash or paper checks [26, 28]. Many components and processes have to be followed during the operation of the e-payment systems in order to make safe and secure transactions [26, 27]. The prime system of e-payment is the EFT, which is a simple tool for electronically transferring money within bank accounts [21]. In a customer's initiation of payment, the system validates the details of the transaction, and then the user's identity is authenticated. This is normally carried out through MFA methods: two or more verification factors are used to get access to the account [24, 25]. The payment gateway is brought into play after the authentication process is successful.

A payment gateway may be defined as a service that processes all of the credit card transactions in both online and physical stores [29, 30]. It encrypts sensitive information like a credit card number to secure the passing of information between customers, merchants, and payment processors [25, 31]. It then forwards the transaction information to the payment processing system. The processor acts as an intermediary between the payment gateway and the corresponding financial institutions, forwarding a request to the bank that issued the card to check the availability of funds on the customer's account. The payment processor forwards the approval of the transaction, if any, from the bank to the payment gateway, which in turn forwards it to the merchant,

notifying of a completed transaction [30]. The other key element in most modern e-payment systems is tokenization. The system replaces all sensitive data of payment by a unique identifier or token that cannot be reversed back to the original information, making it very secure as it drastically minimizes the risk of data breach [25, 38]. Settlement is the last stage of e-payment where money passes out of the customer's bank account into the merchant's account. ACH refers to Automated Clearing House (ACH). The ACH batches and processes transactions, so it forwards and credits the funds in a proper and effective way [21, 30]. E-payment systems are made to accord both people and corporate entities with the high level of convenience, speed, and safety befitting this era. They are moving forward with the change in technology - for example, mobile payments and blockchain technology, among other inventions that keep advancing their operations and security [28]. Figure 1 describes the control flow of the e-payment process from initiation to settlement and reconciliation.

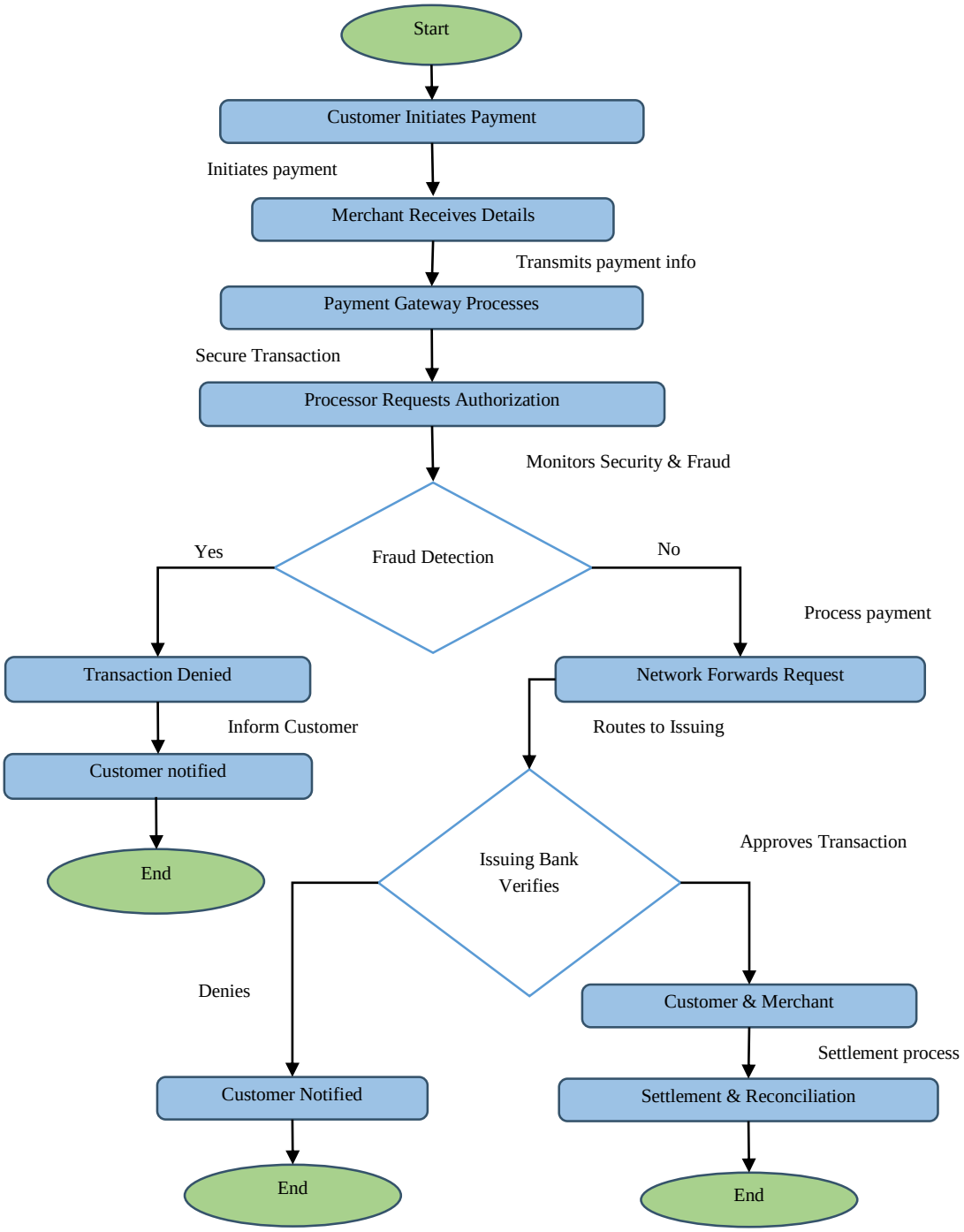

Fig. 1 Control flow of e-payment system

3. Overview of Current Cryptographic Algorithms

In the digital age, secure communication relies on cryptographic algorithms and protocols to protect sensitive data by guaranteeing that information exchanged among different nodes is preserved against unauthorized access, prevented from alteration or corruption during transit of messages through insecure networks [1, 32]. Cryptographic algorithms are essential to the privacy and security of people, from individuals to organizations, as they are widely used to secure websites and safe electronic payments. Not only for protecting data transmitted over the internet, but these cryptographic methods are also used to secure a variety of security protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) [31, 33]. Financial transaction protocols, e.g., Secure Electronic Transaction (SET) and 3-D Secure, were developed to prevent online payment fraud by adding a layer of authentication to card-not-present transactions, thereby improving the security for both parties [25, 34]. The core cryptographic protocols are described individually in the following sections.

3.1. Secure Sockets Layer

SSL originally meant Secure Sockets Layer. SSL is an authenticated and encrypted channel of communication over the Internet for networked computers [22]. Netscape introduced this protocol in the mid-1990s to provide secure Internet communication.

It ensures that data exchanged between a web server and a web browser remains confidential and intact [22, 35]. The SSL-secured web traffic, protected emails, and many other forms of internet communications became modernized, serving as the basis for secure internet transmissions [22].

3.2. Transport Layer Security (TLS)

SSL; Session initiation, the more improved and secure version of the protocol, that came in place of the SSL protocol, encrypting data sent over the internet, is TLS [33]. Actually, the design was meant to surmount problems faced by SSL. With more recent, powerful encryption algorithms and a superior form of key exchange, TLS has better resistance to attacks. It ensures information is confidential, integral, and authenticated when passed between applications through networks [33].

3.3. Secure Electronic Transaction (SET)

SET is the protocol for security in credit card-based transaction processing on the Internet. SET was developed by Visa and MasterCard, designed to enable secure credit card numbers to be transmitted with buyers, sellers, and banks [25, 26]. This allows for very strong data authentication techniques, securing credit card information from buyers to sellers to banks, through high-grade encryption, digital signature, and authentication technology; hence, the data passed from customer to merchant to banks and back cannot be revealed. [26, 27].

3.4. 3-D Secure

3-D Secure is a Visa and MasterCard protocol with an added security layer used in online credit or debit card transactions. It provides an added layer of protection to the goods and services purchased online [34]. During each transaction, the cardholder must enter a password or one-time code to facilitate that transaction. The protocol operates under these various brand names: Verified by Visa, MasterCard Secure Code [24, 34].

3.5. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography is an approach to public-key cryptography based on the algebraic functions of elliptic curves over finite fields. For instance, ECC has smaller key sizes and remains secure compared to many other encryption techniques, such as RSA. Key pre-agreement means that neither side alone can complete the protocol with success against a remote eavesdropper. This basically means that each point on the elliptic curve corresponds to a member of a group with an operation corresponding to the addition operation on groups [32].

3.6. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a widely used and highly secure symmetric key encryption algorithm to secure data. Advanced Encryption Standard has been the standard since 2001, standardized by the National Institute of Standards and Technology, as the standard mechanism for the encryption of sensitive information. It encrypts data in fixed 128-bit blocks using 128-, 192-, or 256-bit keys. The AES is highly resistant to known attacks; thus, it has become one of the most reliable encryption algorithms applied nowadays [36].

3.7. Hash Function and Digital Signatures

Basic cryptographic techniques to ensure data integrity and authentication are hash functions and digital signatures. A hash function is a function that accepts an arbitrary block of information as input and produces a fixed-length bit string, or simply, a hash digest as output. It follows that the process cannot be reversed; in other words, it is computationally infeasible to reconstruct the original data from the hash value. A digital signature, based on a hash function, is a cryptographic scheme to verify the origin and integrity of messages in a digital document. The digital signature of a message is the hash value that the sender creates and sends together with the message [37].

3.8. Tokenization

Tokenization replaces sensitive data with identification symbols or tokens that keep all the essential information regarding the data, though they do not reveal any of the data themselves [25, 38]. It replaces sensitive data with surrogate

values entirely, making it different from encryption, which changes the original data into a secure form. It is in this regard that tokenization proves useful, especially in matters relating to sensitive information: credit card details, social security numbers, and other sensitive identifiers used in the payment systems and financial transactions. These tokens replace the original data for processing without actually exposing the sensitive information to threats [26, 38].

3.9. Diffie-Hellman Key Exchange (DHKE)

A powerful cryptographic protocol allows two parties to safely derive a common secret over an insecure channel. First introduced in 1976 by Whitfield Diffie and Martin Hellman, DHKE enables participants to generate a common secret key, which will be employed as an example for symmetric encryption of the rest of their communication [39]. The strength of the algorithm arises above all from the problem of discrete logarithms and how resolving the Diffie-Hellman problem is computationally infeasible for any attacker, no matter whether they has all the available information during the exchange. DHKE is extensively applied to Internet protocols, including TLS/SSL on the web, and many applications where secure communications are needed [33, 39].

3.10. Data Encryption Standard (DES)

One of the first standards for electronic data encryption was the Data Encryption Standard, or DES. Specifically, its use was adopted by the federal government in 1977 because it originated with IBM in the mid-1970s. It is an algorithm where random 64-bit blocks of data are encrypted with just a 56-bit key [40]. While it had been broadly applied in many fields, starting from the 1970s, DES began to lose its reputation because it became breakable due to improved computational powers that made brute-force attacks feasible. But, in other aspects pertaining to the development of cryptographic standards, its role in history cannot be exaggerated. DES was a forerunner of modern methods of encryption and bestowed general influence on subsequent designs of encryption algorithms [40, 41].

3.11. Triple DES (3DES)

Triple Data Encryption Standard (3DES) is a symmetric-key block cipher built from three successive applications of the Data Encryption Standard (DES). In 3DES, the DES algorithm is applied three times in a row using two or three distinct keys, thereby providing an effective key size of either 112 bits or 168 bits. This considerably magnifies the strength of DES and effectively makes 3DES secure against brute-force attacks that could break the original DES [41].

4. Vulnerabilities of Cryptographic Algorithms to Quantum Attacks

The rise of quantum computing poses a threat to the security provided by many of the cryptographic algorithms and protocols that underpin modern digital security [1, 2]. Quantum algorithms, including Shor's and Grover's algorithms, utilize the principles of quantum mechanics to perform computations that are impractical for classical computers, thereby exposing vulnerabilities in existing cryptographic methods. Due to these vulnerabilities, Quantum E-Payment Systems were evolved, and over the years, technology has advanced a lot, which led to huge changes in the periphery of Financial Transactions and Payment Methods.

The current cryptographic solutions are very mature, but they grow weaker every day due to more advanced cyberspace threats and the emerging threat posed by quantum computing in the future [18, 19]. In this paper, the necessity for a quantum e-payment system is discussed to boost security while creating an immune-to-quantum-attacks practical implementation and fostering cryptographic techniques.

Table 1. Vulnerability of cryptographic protocols to quantum attacks

S. No.	Name of the Cryptographic Protocol	Year Introduced	Underlying Technology	Vulnerable to Quantum Attacks
1	Secure Sockets Layer (SSL)	1995	RSA, DSA, Symmetric Encryption	Vulnerable to Shor's algorithm (breaks RSA/DSA)
2	Transport Layer Security (TLS)	1999	RSA, ECDSA, Symmetric Encryption	Vulnerable to Shor's algorithm (breaks RSA/DSA/ECDSA)
3	Secure Electronic Transaction (SET)	1996	RSA	Vulnerable to Shor's algorithm (breaks RSA)
4	3-D Secure	1999	RSA	Vulnerable to Shor's algorithm (breaks RSA)
5	Elliptic Curve Cryptography (ECC)	1985	Curve Discrete Logarithms (ECDLP)	Vulnerable to Shor's algorithm (breaks ECC)
6	Advanced Encryption Standard (AES)	2001	Symmetric Block Cipher	Vulnerable to Grover's algorithm (reduces security)
7	Hash Functions and Digital Signatures	Varies (SHA-2: 2001)	Cryptographic Hash Functions, RSA, ECDSA	Vulnerable to Grover's algorithm (hash collisions)

8	Tokenization	2000s	Depends on underlying encryption	Not directly vulnerable (depends on encryption)
9	Diffie-Hellman Key Exchange (DHKE)	1976	Discrete Logarithms (DLP)	Vulnerable to Shor's algorithm (breaks DH)
10	Data Encryption Standard (DES)	1977	Symmetric Block Cipher	Vulnerable to Grover's algorithm (reduces security)
11	Triple DES (3DES)	1998	Symmetric Block Cipher	Vulnerable to Grover's algorithm (reduces security)

5. Research Methodology

In this research, a Systematic Literature Review (SLR) [42] was performed to investigate what is known well until now about quantum e-payment systems, especially from the perspective of quantum cryptography, information security, and network security. The reason for selecting the SLR was its systematic and comprehensive approach that is essential to synthesise evidence from existing literature.

One of the advantages of performing an SLR in this field is that it can carry out a deep synthesis on existing knowledge, so researchers and professionals have a better ability to understand what has been done within the scope where they want to act. This study can provide suggestions for future research by summarizing the literature systematically because it is a formal approach for synthesising the results of many studies in order to minimise selection bias, and the review can be easily replicated. The results of an SLR can help decision-makers, researchers, and practitioners to design quantum-resistant e-payment systems that are secure and reliable. The summary of cryptographic protocols vulnerable to quantum attacks is presented in Table 1.

5.1. Search Strategy

A broad search strategy is conducted here to identify and retrieve all relevant literature on quantum e-payment systems. It is formulated in accordance with the research questions and objectives of this review. The relevant information in the following academic databases- Scopus and Google Scholar are searched, and selected these databases because they contain numerous peer-reviewed journals, conference papers, and technical reports in the areas of computer science, cryptography, and finance.

The entry search queries were a mixture of the following keywords: quantum e-payment system, quantum electronic payment system, quantum payment, quantum finance, and quantum cryptography, among others. Results from the selected databases were then narrowed even further, seeking to only include journal publications between 2018 and 2024. In efforts to further restrict this review to a single level of appraisal and review, the grey literature and conference papers, along with technical reports, were excluded from the review. The article search resulted in 23; from these, the relevant records for the review, according to the selection criteria, were assessed for relevance.

5.2. Selection Criteria

The review process adhered to the selection criteria outlined by the PRISMA Statement 2020 [42]. It ensures a transparent and systematic review of high-quality studies on quantum e-payment systems. The review covered original research papers on quantum e-payment systems and quantum cryptography, published in English-language peer-reviewed journals during 2018-2024, with major emphasis on quantum key distribution and, more specifically, on security and authentication in financial systems.

Excluded were studies published before 2018, duplicates, grey literature, review articles, conference papers, case studies, technical reports, papers not in English, and works that were irrelevant or inaccessible. After the screening phase, a total of 23 articles were identified; five duplicated publications were removed, two irrelevant articles, one publication not in English, and two inaccessible papers were concluded, leaving 13 remaining for further review. Figure 2 provides the detailed systematic review process of the research.

5.3. Study Quality Assessment

A comprehensive study quality check was performed to ensure high standards. This involved Deduplication: All duplicates were identified and removed to minimize bias. Title and abstract screening: The focus was on quantum e-payment systems or related topics, especially in the domain of cryptography and security. Full text review: Articles had to meet criteria relevant to the research questions during the full-text assessment. Language Check: Only articles written in English were included. Accessibility check- Articles that were inaccessible or available only as abstracts were excluded. This was followed by the quality assessment that resulted in 13 articles to be considered for final inclusion. Figure 3 provides the graphical representation of the article selection process.

5.4. Data Extraction

This phase captured the following features from selected articles to provide consistency and relevance. Limit to Original Research- Only original research articles were included, while review papers, conference papers, case studies, and technical reports were excluded. Language and Area: The articles must be written in English, deal with quantum cryptography, information security, network security, and classical cryptography. Publications: All included studies were conducted between 2018 and 2024.

Geographical scope: The selected studies were conducted in different countries, thus providing a global narrative on quantum electronic payment systems.

Results from the data extraction provided a rich foundation for analysis of the literature about the Quantum E-payment system and revealed existing trends, challenges, and research gaps in the field. Figure 4 shows the distribution of published papers across six years (2018-2024).

5.5. Literature Review Analysis

During this phase of the systematic literature review, observations are documented, and the results are presented based on the information obtained from the finalized articles. Following the information extraction process, the 13 selected papers were classified into two main categories based on the employed technologies: Quantum E-Payment Systems, comprising 7 studies and Blockchain Integrated Quantum E-Payment Systems, comprising 6 studies.

5.6. Quantum E-Payment Systems

The first part of the review focuses on quantum e-payment systems, comprising 7 studies that employ quantum cryptography to secure confidential financial transactions. This includes studies on QKD, as well as quantum encryption and authentication mechanisms in the context of e-payment systems. The merits and demerits of these technologies are illustrated, along with the methodologies of each proposed research papers.

5.7. Blockchain-based Quantum E-Payment Systems

The second part of the review is solely focused on six papers that integrate blockchain with quantum e-payment systems. In these papers, the use of quantum cryptographic techniques combined with blockchain to reinforce the security, transparency and immutability in e-payment transactions are investigated. Figure 5 shows the proportion of the 13 selected studies, comprising 7 studies (53.8%) on Quantum E-Payment Systems and 6 studies (46.2%) on Blockchain-based Quantum E-Payment Systems.

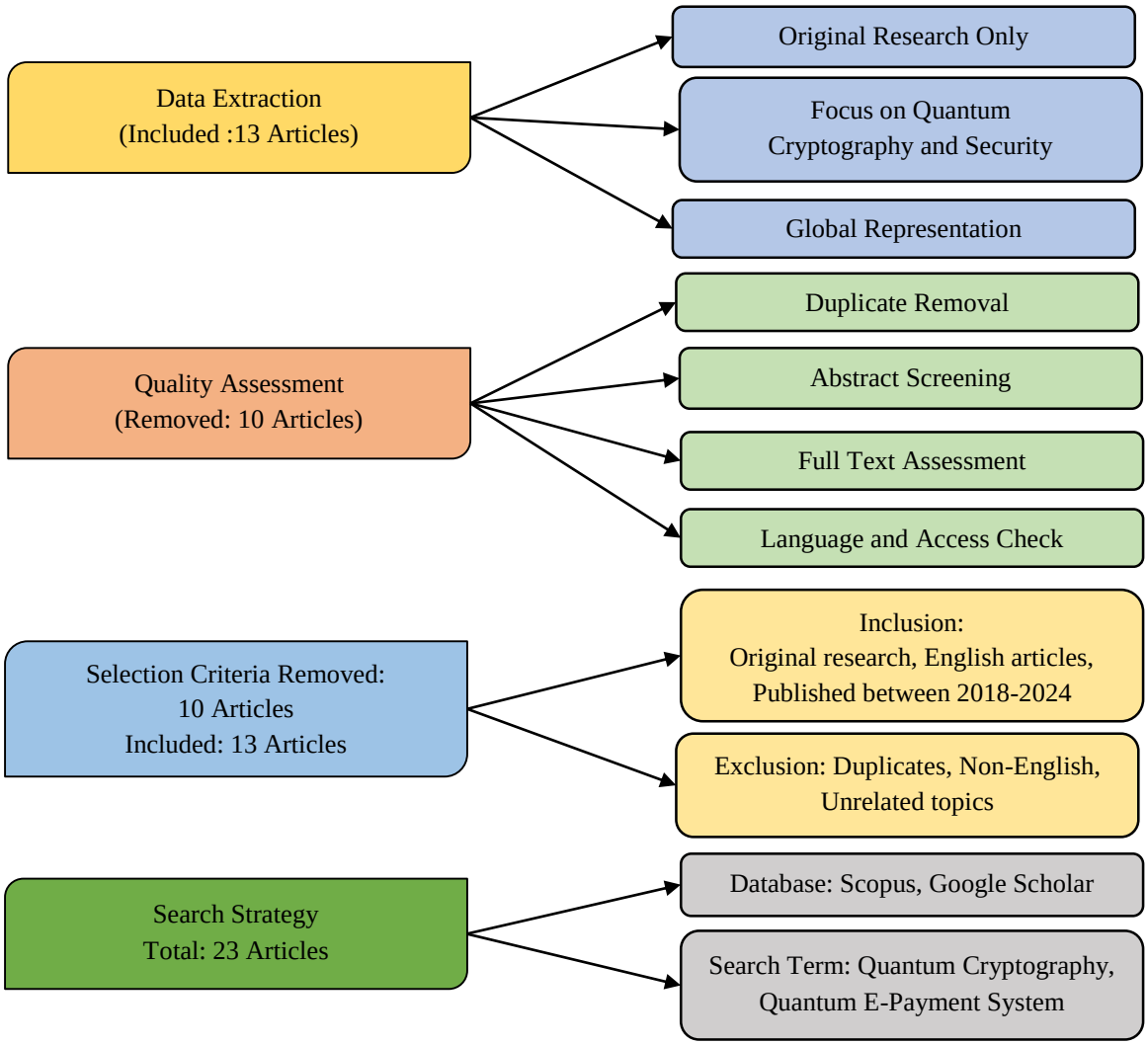

Fig. 2 Systematic review process

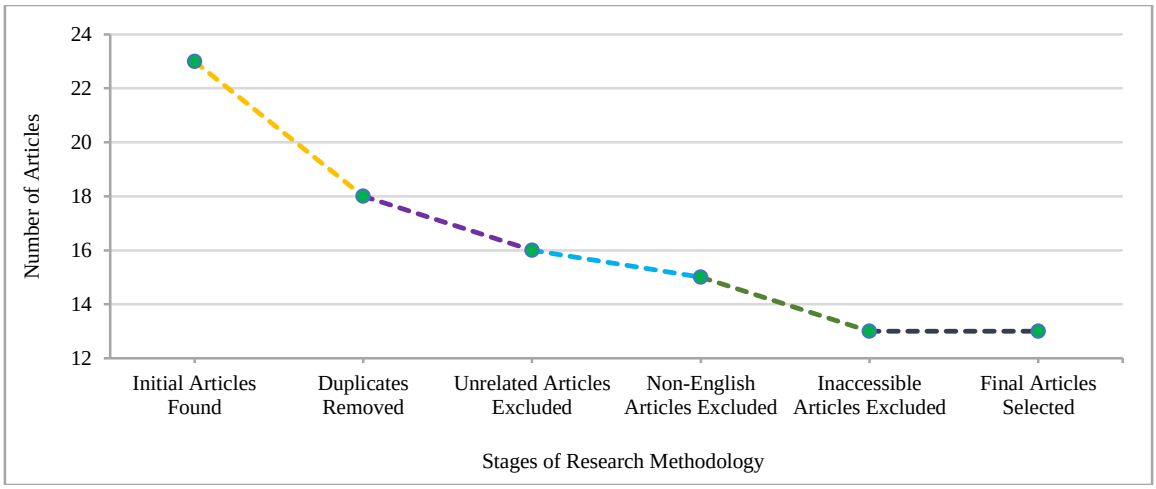

Fig. 3 Stages of article selection and filtering process

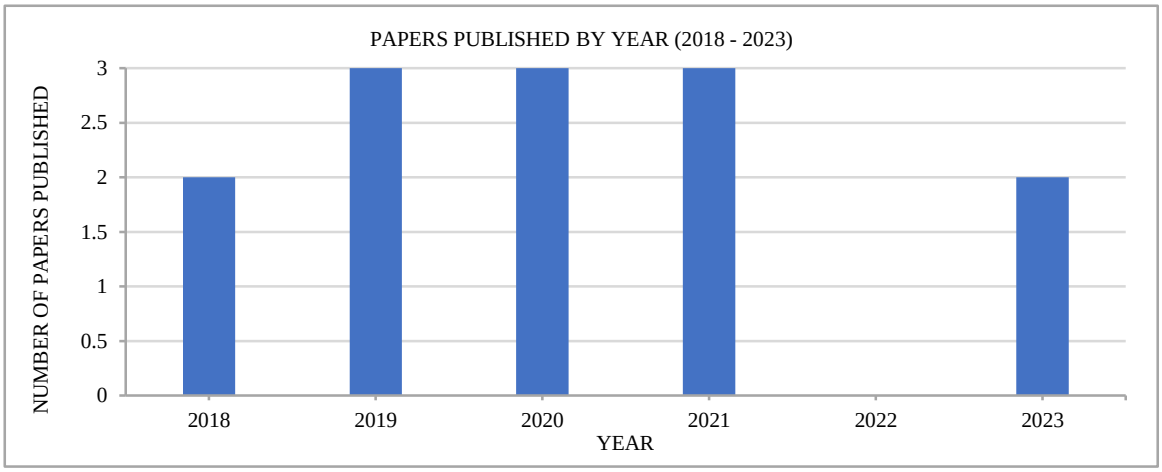

Fig. 4 Yearly distribution of published papers (2018 - 2024)

5.8. Results of Data Synthesis and Analysis

After extracting the required information from the selected articles, the findings were reviewed and synthesized to understand the different approaches reported in the literature. The strengths and limitations of each approach were examined using common criteria such as the methodology used, security protocols, performance, and resistance to attacks. The findings are presented through tables and graphs, covering the focus of each study, the cryptographic schemes used, implementation strategies, and the results reported by the respective authors. This presentation provides a clear view of the existing approaches in quantum e-payment systems, including both standalone and blockchain-integrated systems, and helps identify areas that may require further investigation in future research. Figure 6 provides the distribution of Papers published by journals.

5.9. Quantum E-Payment System Schemes

Niu et al. [43], the protocol is secure based on Quantum Key Distribution (QKD) and quantum blind signature and delivers privacy-preserving properties like user anonymity. It enables genuine transactions across third-party platforms and removes restrictions imposed by prior quantum e-payment systems. To ensure privacy, the protocol employs quantum teleportation and multi-proxy blind signatures to emphasize security properties such as blindness, undeniability and unforgeability. The use of Von Neumann measurements enhances the practical implementation of the protocol and make the protocol feasible with current technologies. The authors clearly show that their quantum-based approach is a secure payment solution for an interbank model and a third-party e-payment model.

Guo et al. [44] proposed a Quantum Blind Signature without Entanglement (QBE) based Trusted Third-Party e-payment protocol. The proposed protocol employs Quantum Key Distribution (QKD) and single-particle unitary operations to achieve unlimited security. It is a privacy-preserving design that preserves the correctness of transactions across different bank branches. For safe communication, it uses Quantum Z Gates and BB 84 protocol, and it also uses a decoy photon detection technique to prevent all types of attacks. The

experiments yield positive results in terms of the properties such as blindness, undeniability and unforgeability as well as unconditional security, making the protocol resilient to both internal and external attacks. The paper is a demonstration of the simplicity of its protocol, which is accomplished by the use basic quantum operations. The summary of Methodologies, Strengths, and Limitations of Quantum E-Payment is presented in Table 2.

Wen et al. [45] suggest a quantum mobile payment protocol using the entanglement coherence of a four-particle Greenberger – Horne - Zeilinger (GHZ) state. The protocol proposed in this paper is developed using Quantum Key Distribution (QKD) principles along with quantum blind signatures to achieve unconditional security in mobile payment. The protocol secures mobile payments with a quantum channel that contains a four-particle GHZ state and does not rely on computational complexity, which can be broken using quantum attacks.

A system uses BB84 protocol for key distribution and employs quantum operations for payment information. The authors note that their protocol guarantees blindness, fraud prevention and unconditional security; without using complex quantum fingerprint functions, which is feasible for practical mobile payment systems.

Tiliwalidi et al. [46] propose a quantum protocol combining the quantum proxy blind signature mechanism for a multi-bank electronic payment system. It allows users to pay safely using WeChat wallet, Alipay, and traditional bank accounts across different banks. The protocol applies Quantum Key Distribution (QKD), one-time pad methods, together with quantum multi-proxy blind signatures for unconditional security as well as user anonymity. The proposed protocol utilizes a six-qubit entangled quantum state together with controlled quantum teleportation and Von Neumann measurements followed by unitary operations; hence, it can be implemented using current technologies. Security analysis proved that the protocol is blind, non-disavowable, and forgery-resistant, achieving unconditional security against internal and external adversaries, in both passive and active attacks. Finally, it demonstrates the protocol's effectiveness for multi-bank e-payment systems. Table 3 provides the performance comparison of the Quantum E-payment schemes.

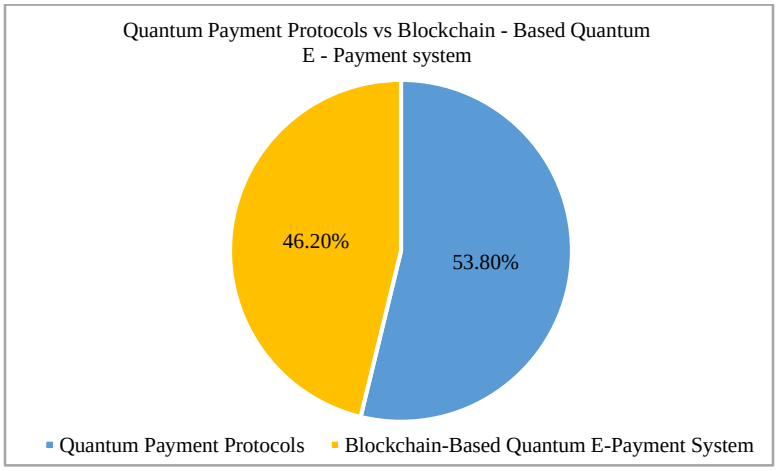

Fig. 5 Proportion of quantum payment protocols and blockchain - based quantum e - payment systems

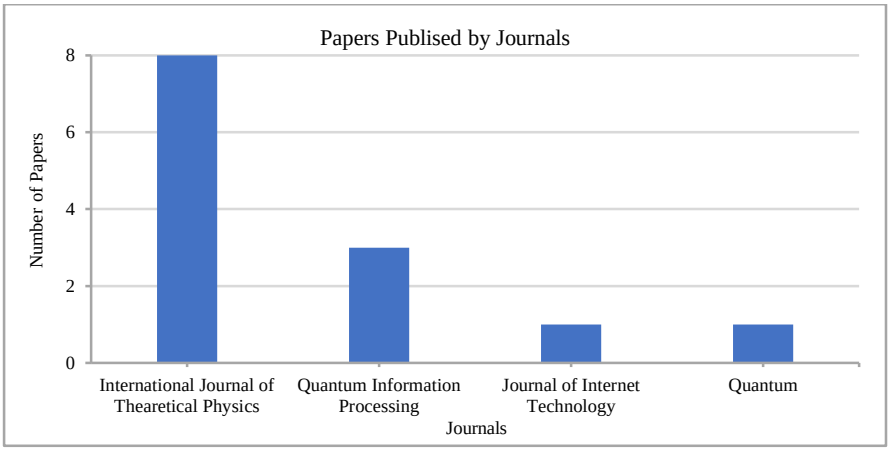

Fig. 6 Papers published by journal

Table 2. Methodologies, strengths, and limitations of quantum e-payment schemes

Author	Methodologies	Merits	Demerits
Niu et al. [43] (2018)	Quantum Multi-Proxy Blind Signature, Distribution of Key and Controlled Quantum Teleportation.	Provides full security and complete anonymity, and allows safe transactions by means of third parties.	Difficulties in the application of quantum technologies in third-party payment systems.
Guo et al. [44] (2018)	Quantum blind signature, quantum key distribution, decoy photon checking, without entanglement.	Provides unconditional security and user privacy, and avoids difficult entanglement processes	limited in scalability and still depend on secure quantum channels.
Wen et al. [45] (2019)	Quantum key distribution, four-particle GHZ state, quantum blind signatures.	Delivers safe mobile transactions, blindness and unconditional security.	Current implementation on real-world has limitations in real world implementation due to quantum entanglement.
Tiliwalidi et al. [46] (2019)	Quantum proxy blind signature, quantum key distribution, controlled quantum teleportation.	Anonymous, blind and non-forgeable multi-bank transactions.	Requires high resources for multi-bank transactions, harder to implements.
Xie et al. [47] (2020)	Quantum proxy blind signatures, controlled quantum teleportation, quantum key distribution.	Offering secure transactions, quick inter-bank settlements, builds trust & eliminates fraud.	The constraints of current quantum technology, computationally demanding.
Cai et al. [48] (2020)	Quantum blind computing, unitary operations, four-qubit cluster state, shared blind matrix.	Improves the evaluation of e-payment security, delivers data tampering and confidentiality.	Only for evaluation purposes; full potential cannot be realised without quantum technologies.
Lin et al. [49] (2021)	X-LIOP states, quantum key distribution, one-time pad encryption, without entanglement.	Leads to blindness and unforgeability without entanglement and practical implementation	Difficulty in creating and maintaining X-LIOP states, deployment constraints in practice.

Table 3. Performance comparison of quantum e - payment schemes

Criteria	Niu et al. [43]	Guo et al. [44]	Wen et al. [45]	Tiliwalidi et al. [46]	Xie et al. [47]	Cai et al. [48]	Lin et al. [49]
Flexibility	No	Yes	No	No	No	Yes	Yes
Blockchain Integration	No	No	No	No	No	No	No
Eavesdropping Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Real-World Applicability	High	Medium	High	High	High	Medium	Medium
Entanglement Usage	Yes	No	Yes	Yes	Yes	Yes	No
Noisy Channel Adaptation	Limited	No	Limited	Limited	Limited	No	Limited
Scalability	Medium	High	Medium	Medium	Medium	Low	Medium
Third-Party Dependence	Yes	No	Yes	Yes	Yes	Yes	No
Resource-Constrained Devices	Yes	Yes	No	Yes	Yes	No	Yes
Security and Privacy	High	Medium	High	High	High	Medium	High

Cai et al. [48] propose a method for an e-payment security system developed using quantum blind computing, which aims to improve the safety during network transactions. It involves unitary operations and a cluster state consisting of four qubits to avoid eavesdropping and secure user privacy. Security scores are encrypted with a shared blind matrix to ensure that data cannot be tampered by the third-party payment platform nor the users. It can determine how secure transactions are while at the same time protecting the private information of users. The author highlights the protocol unconditional security through security analysis analyses internal and external attacks. Moreover, it can be used in other scenarios, except e-payment, such as anonymous voting and teacher-student assessment. Figure 7 provides the results of the security features comparison based on Quantum e-payment system schemes.

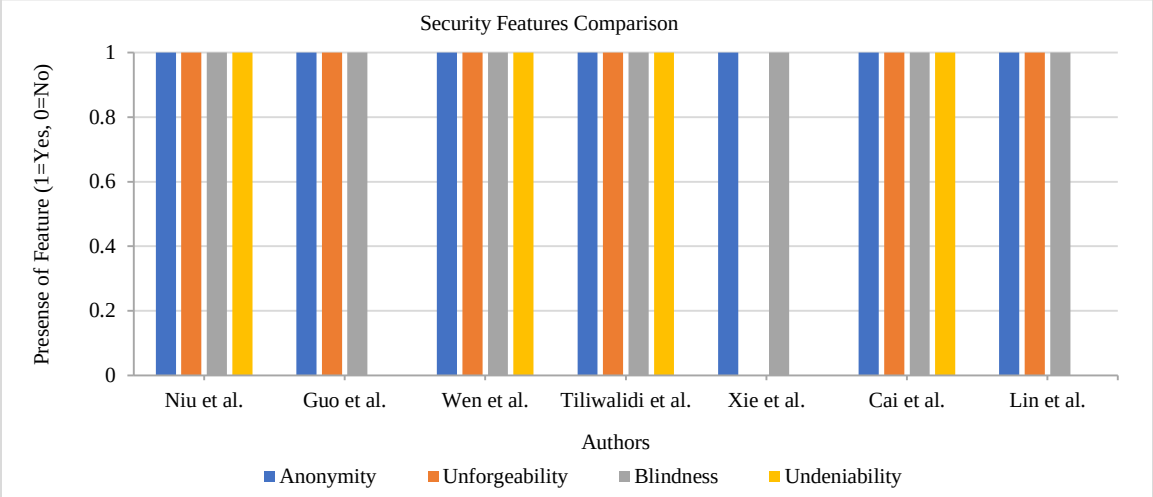

Fig. 7 Security features comparison for quantum e - payment system schemes

Lin et al. [49] design a quantum payment protocol developed using a special set of Local Indistinguishable Orthogonal Product states (X - LIOP). The proposed protocol stores purchase data in the form of X-LIOP states, restricting this information to only be visible between buyer and seller, but hidden from any outside parties, such as a bank. Communication is secured using Quantum Key Distribution (QKD) combined with one-time pad encryption within this protocol. It met the essential security properties of unforgeability, blindness, and undeniability while protecting against both internal and external attacks. Crucially, this cannot work with entanglement, so it is one of the most practical protocols for real-world implementation. Finally, the security analysis shows the protocol is efficient in preventing participants form forging or denying payment and effective in addressing e-payment disputes. Figure 8: The heatmap represents the resistance of seven different quantum E-payment protocols to various types of attacks.

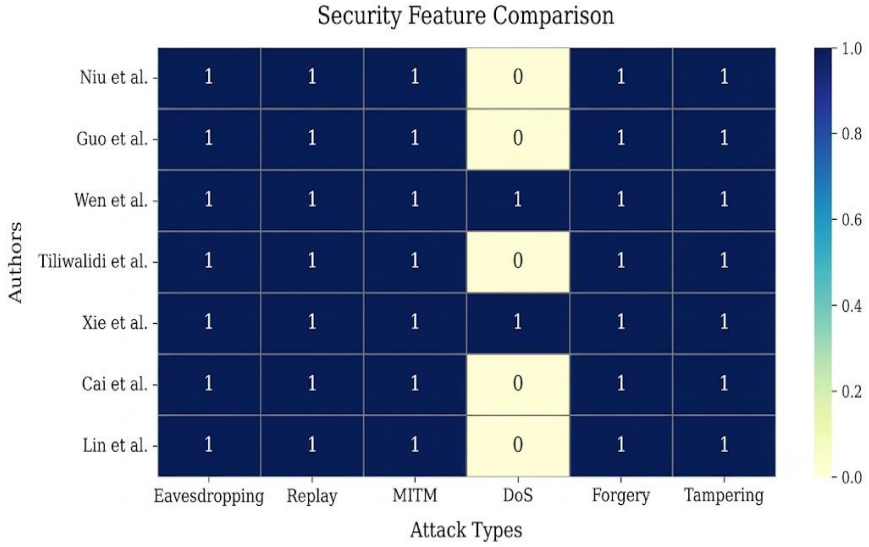

Fig. 8 Comparison of attack resistance in quantum e - payment system

5.10. Blockchain-based Quantum E-Payment Systems

Zhang et al. [50] present a new e-payment protocol based on blockchain and quantum signature technology to enhance security. The quantum key distribution, one-time pad encryption and quantum proxy blindness scheme are used to guarantee user anonymity and unconditional security. For secure and decentralized data storage, the transaction information is stored on blockchain. The message, blinding, trading, and payment section are the critical phases of the proposed protocol. The system is secure against forgery, denial, and frequent attacks such as man-in-the-middle. The proposed systems integrating quantum cryptography with blockchain security provide strong protection for inter-bank and inter-provincial transactions, removing the necessity for a third-party intermediary.

Coladangelo and Sattath et al. [51] propose a protocol for a hybrid classical-quantum payment system to provide a solution for the scalability problem of a blockchain. This system combines traditional blockchains and quantum lightning. The basic idea of the protocol is that the quantum states act as banknotes, and their usage in untrusted transactions is secured by a classical blockchain acting as a smart contract and dispute resolution mechanism. This is because the system under no circumstances depends on one central authority; the system works in a decentralized manner. Quantum communication sped up the transmission of information, as there is no transaction fee charged. Figure 9 describes the distribution of quantum technologies used in E-Payment Systems.

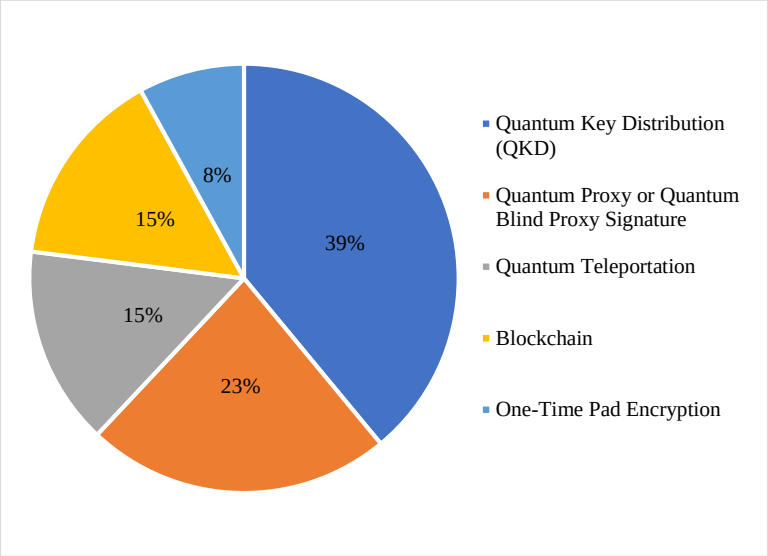

Fig. 9 Quantum technology in e - payment systems

Table 4. Performance comparison of blockchain - based quantum e-payment systems

Criteria	Zhang et al. [50]	Coladangelo et al. [51]	Gou et al. [52]	Xu et al. [53]	Li et al. [54]	Li et al. [55]
Flexibility	Yes	Yes	Yes	Yes	Yes	Yes
Blockchain Integration	Yes	Yes	Yes	Yes	Yes	Yes
Eavesdropping Detection	Yes	Yes	Yes	Yes	Yes	Yes
Real-World Applicability	Medium	Medium	High	Medium	High	High
Entanglement Usage	Yes	No	Yes	Yes	No	No
Noisy Channel Adaptation	Limited	No	Limited	Limited	Limited	Limited
Scalability	High	Medium	Medium	Medium	High	High
Third-Party Dependence	No	No	No	Yes	No	No
Resource-Constrained Devices	Yes	No	No	Yes	No	No
Security and Privacy	High	Medium	High	Medium	High	High

This ensures efficiency in operation. The paper also gives an overview of the challenges in practice and different ways to address these hiccups for practical implementation. This is a novel approach that utilizes quantum cryptography, along with blockchain technologies, to improve the scalability and security that comes with transactions. Table 4 shows the performance comparison of Blockchain-based Quantum E-Payment Systems.

Table 5. Methodologies, strengths, and limitations of blockchain-based quantum e-payment systems

Author	Methodologies	Merits	Demerits
Zhang et al. [50] (2019)	Makes use of quantum signatures and blockchain for secure payments	High-level security with blockchain and quantum signature; an increased level of reliance	May be computationally expensive to implement in practice.
Coladangelo et al. [51] (2020)	Combines quantum money with blockchain through quantum lightning for decentralized payment verification and scalability.	Prevents Blockchain scaling issue and double-spending.	Might face Difficulty in implementing quantum money and integration with blockchain.
Gou et al. [52] (2021)	Quantum encryption and blockchain to secure e-payment transactions for decentralized validation and User privacy.	Improves security and privacy via quantum cryptography; guarantees transaction integrity.	Real-world applications may face difficulties as it would require quantum infrastructure.
Xu et al. [53] (2021)	Uses semi-quantum cryptography and blockchain for mobile and low-resource environments.	Low computation overhead with its light-weight protocol; makes perfect fit for mobile and resource-constrained devices.	Can only support to semi-quantum capabilities, perhaps not as secure as a fully quantum solution.
Li et al. [54] (2023)	Measurement-device-independent quantum cryptography and blockchain to enhance e-payment security and immunity to certain attacks.	Offers protection from a range of assaults and security threats	Charges alerts in the context of precise quantum state management; practical deployment complexity.
Li et al. [55] (2023)	Twin-field quantum key distribution, blockchain and quantum encryption for secure long-distance e-payments transactions	Increases the distance of secure transactions across long distances through classical and quantum defense using twin-field QKD.	Relies on next-generation quantum backend with implementation difficulties on present-day systems.

Gou et al. [52] proposed a new quantum electronic payment protocol which incorporating block chain technology with quantum cryptography. The protocol involves Quantum Proxy Blind Signature (QPBS), Quantum Key Distribution (QKD) & controlled Quantum Teleportation. A major benefit is that it employs three-qubit entangled states, a notable improvement in quantum resource load compared to previous protocols with more qubits. The decentralized and immutable transaction storage brought by blockchain technology makes the protocol not vulnerable, as well more traceable. Without trust of a third party, the proposed protocol intends to be applied in a quantum e-payment system for enhancing fairness, auditability and security. The summary of Methodologies, Strengths, and Limitations of Blockchain-Based Quantum E-Payment Systems is presented in Table 5.

Xu et al. [53] put forward an efficient and low-requirements semi-quantum e-Payment protocol with a blockchain framework. In a nutshell, the protocol provides classical users like Alice with limited access to quantum channels and thereby making it more practical while not mandating full-fledged quantum feasibility. The payment information is transmitted securely through controlled quantum teleportation and Bell states, while blockchain technology guarantees traceability as well as correctness. The security analysis shows that the protocol can withstand several threat models, such as man-in-the-middle attacks and intercept-measure-resend. The resources of quantum are simplified by the semi-quantum cryptography and a three-qubit entangled state, facilitating its realization in practical usages. Figure 10 provides the results of the security features comparison based on Blockchain-Based Quantum E-Payment Systems.

Li et al. [54] propose a measurement-device-independent quantum protocol for e-payment based on secure blockchain technology. The protocol uses Bell states to simplify the quantum resources and resist side-channel attacks simultaneously. It uses a combination of quantum public-key encryption and blockchain technology to ensure not only transaction security but also privacy. It is designed to achieve anonymity, blindness, unforgeability and undeniability. It provides better feasibility with the currently available technologies than earlier protocols by solving issues from a third-party payment platform and using blockchain for documented, unalterable transaction records. Figure 11 shows the heatmap represents the resistance of six different quantum E-payment protocols to various types of attacks.

Li et al. [55] The authors propose a twin-field quantum encryption e-payment protocol combined with blockchain to improve security and efficiency. This protocol overcomes the

limitation of Pirandola – Laurenza - Ottaviani Banchi (PLOB) bound by utilizing Twin - Field QKD (TF - QKD) to perform identity authentication and eavesdropping detection. It ensures blindness, unforgeability and undeniability to mitigate inside and outside threats.

Blockchain implementation is too secure and transparent that could not become centralized. This approach demonstrates that quantum encryption and blockchain technology able to offer a less vulnerable solution for secure e-payment transactions.



Fig. 10 Blockchain - based quantum e - payment systems security features comparison

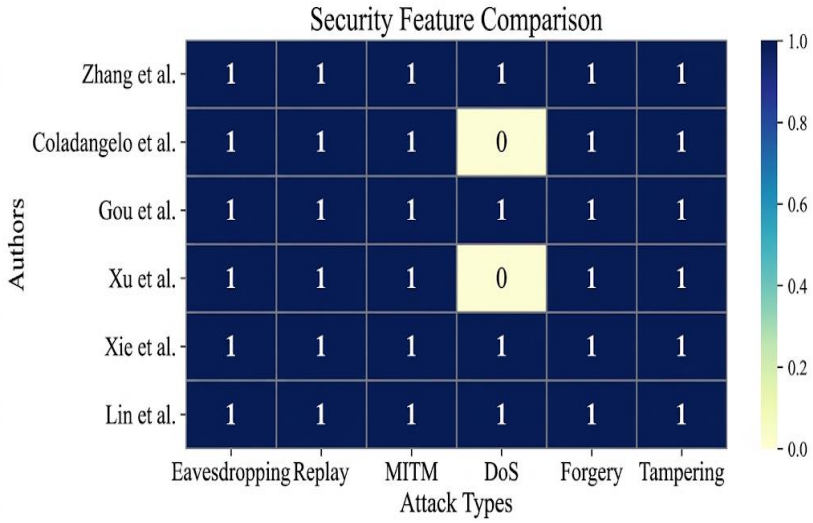

Fig. 11 Comparison of attack resistance in blockchain based quantum e - payment system

6. Future Research Direction

Future studies should focus on improving the accuracy and reliability of the received quantum states to further advance Quantum e-Payment Systems.

- The importance of making von Neumann measurements as good for actual uses in real life. Clearing these hurdles would lead to more dependable quantum payment systems in noisy backgrounds, Niu et al. [43].
- How to apply quantum blind signatures in more general network settings beyond the scenario, Guo et al. [44].
- To improve entanglement coherence in four particle GHZ state for more stable communication channels, Wen et al. [45]
- More attention on increasing the security of the six-qubit entangled state that these protocols work with. An expansion of the application of these systems to complex, multi-bank environments with diverse transaction types would present promising avenues for further research, Tiliwalidi et al. [46].
- Advanced eavesdropping detection methods are developed for further resilience of the system against quantum attacks, Xie et al. [47].
- Improving the performance of the system, particularly using hyperentanglement and super quantum gates, Cai et al. [48].

- To optimize the power of X-LIOP states for better security and efficiency and to use the protocol in complex financial setups, while exploiting as little resources as possible, Lin et al. [49].
- Practical implementations that integrate semi-quantum techniques and make quantum-secured transactions more accessible should be developed, Zhang et al. [50].
- The optimization of quantum teleportation and the adaptation of protocols to different blockchain networks are important research directions. Gou et al. [51].
- An increase in security and scalability could be the most needed characteristic for worldwide payment systems based on semi-quantum protocols. Research should also investigate if these could be extended to larger or more complicated payment scenarios. Xu et al. [53].
- How quantum money could be practically deployed into real-life financial systems with respect to security, robustness, and decentralized environments, Li et al. [54].
- Toward optimizing the TF-QKD performance with real-time trade and integrating with blockchain networks to maintain high performance, scalability, and security. Li et al. [55].

7. Conclusion

This paper examines the current status of e-payment systems with quantum features within the domain of quantum cryptographic techniques and describes the reported findings. The current study elaborates on quantum key distribution and blockchain-based quantum e-payment protocols, emphasizing the potential of the current security challenges in the dynamic digital economy. The literature review of the present paper has endeavoured to consider some of the quantum e-payment protocols through enrolling their strong and weak points and practical usage scenarios. It is also from such a systematic review that researchers and practitioners can grasp quantum e-payment systems and the technologies that lean on them.

Different approaches that strengthen system security were classified and analyzed, providing insights into their comparative performance. This review is trying to delve into these innovative solutions in detail and, at the same time, tries to contribute towards more research in quantum e-payment systems, so it is basic for future work. This work sets basis for the advancement of quantum-safe financial systems, as it also gives a direction toward building secure, efficient, and scalable quantum e-payment solutions.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

No funding was received for conducting this study.

Acknowledgments

Suganthi A: Conceptualization, Methodology, Writing - original draft. K. Vidya: Supervision, Review, Editing, Validation.

References

[1] Daniel J. Bernstein, and Tanja Lange, "Post-Quantum Cryptography," *Nature*, vol. 549, no. 7671, pp. 188-194, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[2] Vasileios Mavroeidis et al., "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, no. 3, pp. 1-10, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Michael A. Nielsen, and Isaac L. Chuang, *Quantum Computation and Quantum Information*, 10th ed., Cambridge University Press, 2010. [Google Scholar] [Publisher Link]

[4] Charles H. Bennett, and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Theoretical Computer Science*, vol. 560, pp. 7-11, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[5] Artur K. Ekert, "Quantum Cryptography based on Bell's Theorem," *Physical Review Letters*, vol. 67, no. 6, 1991. [CrossRef] [Google Scholar] [Publisher Link]

[6] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki, "Secure Quantum Key Distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595-604, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[7] Nicolas Gisin et al., "Quantum Cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145-195, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[8] Valerio Scarani et al., "The Security of Practical Quantum Key Distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301-1350, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] Jia-lei Zhang et al., "A Blind Signature Scheme Applying on Electronic Payment Scene based on Quantum Secret Sharing," *International Conference on Security and Privacy in New Computing Environments*, Tianjin, China, vol. 2, pp. 1-12, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Aman Gupta et al., "An Efficient and Secure Quantum Blind Signature-based Electronic Cash Transaction Scheme," *IET Quantum Communication*, vol. 5, no. 4, pp. 619-631, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Siavash Khodambashi, and Ali Zakerolhosseini, "A Sessional Blind Signature based on Quantum Cryptography," *Quantum Information Processing*, vol. 13, no. 1, pp. 121-130, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[12] Stephen Barnett, *Quantum Information*, Oxford Academic Press, 2009. [CrossRef] [Google Scholar] [Publisher Link]
[13] Xiaojun Wen, Yongzhi Chen, and Junbin Fang, "An Inter-Bank E-Payment Protocol based on Quantum Proxy Blind Signature," *Quantum Information Processing*, vol. 12, no. 1, pp. 549-558, 2013. [CrossRef] [Google Scholar] [Publisher Link]
[14] Ming-Hui Zhang, and Jia-Hui Xie, "High Fidelity Quantum Blind Dual-Signature Protocols," *Modern Physics Letters B*, vol. 36, no. 13, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[15] Haoyang Yu, and Yunxiao Qian, "Quantum Group Blind Signature Scheme based on Measurement-based Quantum Computation," *Proceedings SPIE 12290, International Conference on Computer Network Security and Software Engineering (CNSSE 2022)*, vol. 12290, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[16] Mhlambululi Mafu, Adriana Marais, and Francesco Petruccione, "Towards the Unconditional Security Proof for the Coherent-One-Way protocol,"0020*The 56th Annual Conference of the SA Institute of Physics, hosted by UNISA*, 2011. [Google Scholar]
[17] Michele Mosca, "Cybersecurity in an Era with Quantum Computers: Will we be Ready?," *IEEE Security and Privacy*, vol. 16, no. 5, pp. 38-41, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[18] Anshika Vaishnavi, and Samaya Pillai, "Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods," *Journal of Physics: Conference Series*, vol. 1964, no. 4, pp. 1-10, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[19] Teik Guan Tan, Pawel Szalachowski, and Jianying Zhou, "Challenges of Post-Quantum Digital Signing in Real-World Applications: A Survey," *International Journal of Information Security*, vol. 21, no. 4, pp. 937-952, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[20] Yaser Baseri et al., "Evaluation Framework for Quantum Security Risk Assessment: A Comprehensive Study for Quantum-Safe Transition," *Computers and Security*, vol. 150, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[21] David Bounie, Christian Picory, and Etienne Tricot, "Electronic Fund Transfers and ICT: Economic Stakes and Monetary Perspectives," *Internet Economics Workshop*, pp. 277-308, 2000. [Google Scholar]
[22] Carl Adams, and Simon Mouatt, "The Rise of Complementary Currencies and Corporafinance: E-commerce Driven Competition in the Financial Sector," *Journal of Internet Banking and Commerce*, vol. 15, no. 1, pp. 1-12, 2010. [Google Scholar] [Publisher Link]
[23] Lelieveldt Consultancy, "Research Study on the Integration of E-payments into the Online Transaction Process," *Institute for Prospective Technological Studies*, pp. 1-57, 2001. [Google Scholar]
[24] Ashutosh Saxena, "Dynamic Authentication: Need Than a Choice," *2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08)*, Bangalore, India, pp. 214-218, 2008. [CrossRef] [Google Scholar] [Publisher Link]
[25] Edward A. Morse, and Vasant Raval, "PCI DSS: Payment Card Industry Data Security Standards in Context," *Computer Law and Security Review*, vol. 24, no. 6, pp. 540-554, 2008. [CrossRef] [Google Scholar] [Publisher Link]
[26] Adam Ali.Zare Hudaib, "E-Payment Security Analysis in Depth," *International Journal of Computer Science and Security*, vol. 8, no. 1, pp. 1-14, 2014. [Google Scholar] [Publisher Link]
[27] Md. Asaduzzaman, "Security Aspects of E-Payment System and Improper Access Control in Microtransactions," *EasyChair Preprint*, pp. 1-7, 2020. [Google Scholar] [Publisher Link]
[28] Arti Gaur, and Sanju Verma, "E-Payment: A Bibliometric Analysis and Systematic Literature Review," *International Journal of Indian Culture and Business Management*, vol. 34, no. 1, pp. 45-72, 2025. [CrossRef] [Google Scholar] [Publisher Link]
[29] Nathalia Devina Widjaja, and Ardy Tedjawidjaja, "A Preliminary Study of Merchants' Intention to Adopt Online Payment Gateway in Indonesia," *International Journal of Future Computer and Communication*, vol. 1, no. 2, pp. 155-159, 2012. [CrossRef] [Google Scholar] [Publisher Link]
[30] Comptroller's Handbook, *Safety and Soundness*, 2014. [Google Scholar]
[31] DS Ms Charjan, PS Ms Bochare, and Yogesh R. Bhuya, "An Overview of Secure Sockets Layer," *International Journal of Computer Science Applications*, vol. 6, no. 2, pp. 388-393, 2013. [Google Scholar]
[32] Samta Gajbhiye, Monisha Sharma, and Samir Dashputre, "A Survey Report on Elliptic Curve Cryptography," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 1, no. 2, pp. 195-201, 2011. [Google Scholar]
[33] Kerry McKay, and David Cooper, *Guidelines for the Selection, Configuration, and use of Transport Layer Security (TLS) Implementations*, National Institute of Standards and Technology, Gaithersburg, MD, pp. 1-72, 2017. [Google Scholar] [Publisher Link]
[34] Mohammed Assora, and Ayoub Shirvani, "Enhancing the Security and Efficiency of 3-D Secure," *International Conference on Information Security*, Samos Island, Greece, vol. 4176, pp. 489-501, 2006. [CrossRef] [Google Scholar] [Publisher Link]
[35] D. Geer, "Taking Steps to Secure Web Services," *Computer*, vol. 36, no. 10, pp. 14-16, 2003. [CrossRef] [Google Scholar] [Publisher Link]
[36] Ako Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," *Cryptography and Network Security*, vol. 16, no. 1, pp. 1-12, 2017. [Google Scholar]
[37] Shaimaa H. Shaker, and Ghzwh G. Jumaa, "Digital Signature based on Hash Functions," *International Journal of Advancement in Engineering Technology, Management and Applied Science (IJAETMAS)*, vol. 4, no. 1, pp. 88-99, 2017. [Google Scholar]

[38] Sandra Díaz-Santiago, Lil María Rodríguez-Henríquez, and Debrup Chakraborty, "A Cryptographic Study of Tokenization Systems," *International Journal of Information Security*, vol. 15, no. 4, pp. 413-432, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[39] Robert Muth, and Florian Tschorsch, "SmartDHX: Diffie-Hellman Key Exchange with Smart Contracts," *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, Oxford, UK, pp. 164-168, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] Indumathi Saikumar, "DES-Data Encryption Standard," *International Research Journal of Engineering and Technology*, vol. 4, no. 3, pp. 1777-1782, 2017. [Google Scholar]

[41] O. Srinivasa Rao, "Performance Analysis of DES and Triple DES," *International Journal of Computer Applications*, vol. 130, no. 14, pp. 30-34, 2015. [Google Scholar] [Publisher Link]

[42] Rafael Sarkis-Onofre et al., "How to Properly use the PRISMA Statement," *Systematic Reviews*, vol. 10, no. 1, pp. 1-3, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[43] Xu-Feng Niu et al., "A Third-Party E-Payment Protocol based on Quantum Multi-Proxy Blind Signature," *International Journal of Theoretical Physics*, vol. 57, no. 8, pp. 2563-2573, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[44] Xi Guo, Jian-Zhong Zhang, and Shu-Cui Xie, "A Trusted Third-Party E-Payment Protocol based on Quantum Blind Signature Without Entanglement," *International Journal of Theoretical Physics*, vol. 57, no. 9, pp. 2657-2664, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[45] Xiaojun Wen et al., "A Mobile Quantum Payment Protocol based on the Entanglement Coherence of Four-Particle GHZ State," *Journal of Internet Technology*, vol. 20, no. 6, pp. 1861-1868, 2019. [Google Scholar] [Publisher Link]

[46] Kalibinuer Tiliwalidi, Jian-Zhong Zhang, and Shu-Cui Xie, "A Multi-Bank E-Payment Protocol based on Quantum Proxy Blind Signature," *International Journal of Theoretical Physics*, vol. 58, no. 10, pp. 3510-3520, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[47] Shu-Cui Xie, Xu-Feng Niu, and Jian-Zhong Zhang, "An Improved Quantum E-Payment System," *International Journal of Theoretical Physics*, vol. 59, no. 2, pp. 445-453, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[48] Dong-Qi Cai et al., "Implementation of an E-Payment Security Evaluation System based on Quantum Blind Computing," *International Journal of Theoretical Physics*, vol. 59, no. 9, pp. 2757-2772, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[49] Miao-Miao Lin et al., "A New Quantum Payment Protocol based on a Set of Local Indistinguishable Orthogonal Product States," *International Journal of Theoretical Physics*, vol. 60, no. 4, pp. 1237-1245, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[50] Jia-Lei Zhang et al., "A Novel E-Payment Protocol Implented by Blockchain and Quantum Signature," *International Journal of Theoretical Physics*, vol. 58, no. 4, pp. 1315-1325, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[51] Andrea Coladangelo, and Or Sattath, "A Quantum Money Solution to the Blockchain Scalability Problem," *Quantum*, vol. 4, pp. 1-44, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[52] Xiang-lin Gou et al., "A Novel Quantum E-Payment Protocol based on Blockchain," *Quantum Information Processing*, vol. 20, no. 5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[53] Yuguang Xu et al., "A Lightweight Semi-Quantum E-Payment Protocol based on Blockchain," *International Journal of Theoretical Physics*, vol. 60, no. 11-12, pp. 4196-4209, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[54] En Li et al., "Measurement-Device-Independent Quantum Protocol for E-Payment based on Blockchain," *Quantum Information Processing*, vol. 22, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[55] Guo-Dong Li, Jun-Jie Luo, and Qing-Le Wang, "Twin-Field Quantum Encryption Protocol for E-Payment based on Blockchain," *Quantum Information Processing*, vol. 22, no. 12, 2023. [CrossRef] [Google Scholar] [Publisher Link]