Quantum Information Processing (2024) 23:101
https://doi.org/10.1007/s11128-024-04316-x

Quantum blockchain architecture using cyclic QSCD and QKD

Mandeep Kumar[1] · **Bhaskar Mondal**[1]

Received: 3 January 2024 / Accepted: 14 February 2024 / Published online: 10 March 2024

Abstract
Quantum blockchain (QBC) is a novel decentralised concept anticipated to offer an alternative to the classical blockchain to provide transaction security and transparency. The QBC frameworks can offer the most tangible advantage against the security threat posed by quantum computers on the classical blockchain. The proposed scheme offers a new QBC framework in which voting is performed by the Quantum-Secured Yet Another Consensus (QSYAC) algorithm to create a fast decentralised QBC. QSYAC algorithm is also used to ensure the reliability and fault tolerance of the blockchain framework. The classical information and the chaining are provided using a single qubit state and quantum entanglement. The transactions are signed via a cyclic permutation of the computational distinguishability of the quantum states problem, and quantum key distribution protocol is used for secure key sharing. Assuring the security of the key and the blockchain, the suggested model is more effective and safe from potential quantum assaults than earlier systems.

Keywords Blockchain · Consensus · QKD · QSYAC · Cyclic QSCD · Quantum blockchain

1 Introduction

Blockchain is a distributed shared data block linked with each other and forms a chain of blocks [1]. Satoshi Nakamoto first announced the notion of blockchain technology [2] in 2008. Since Bitcoin is produced, distributed, exchanged, and kept via a decentralised ledger system (blockchain), it is the most well-known example of blockchain

✉ Bhaskar Mondal
bhaskar.cs@nitp.ac.in

Mandeep Kumar
mandeepk.ph21.cs@nitp.ac.in

[1] Department of Computer Science and Engineering, National Institute of Technology Patna, Patna, Bihar 800005, India

technology in use. The unique feature of the blockchain is that it guarantees trust without needing a reliable third party. It does this by ensuring that a data record is accurate and safe. Blockchain's usage of a distributed network is just one of its many advantages, which makes transaction data transparent and secure. This technology is garnering a lot of interest from a range of industries, including finance, energy, health care, and political issues, and it is not only about Bitcoin and other cryptocurrencies.

The most critical aspects of blockchain technology are consensus algorithms and digital signatures. An approach for getting different systems or processes to agree on a single data value is known as a consensus algorithm in computer science. Consensus algorithms are designed to ensure dependability in networks with multiple problematic nodes. Blocks can be generated using consensus procedures, and transaction data can be secured using digital signatures.

The consensus algorithm Proof of Work [3] is what Bitcoin [2] employs. Proof of stack [4], delegated proof of stack [5], yet another consensus (YAC) algorithm [6], quantum byzantine agreement (QBA) [7, 8], delegated proof of stake with borda count and node behaviour [9], and quantum secure YAC (QSYAC) [10] are examples of consensus algorithms. These consensus algorithms have been effective in producing blocks of data on transactions that are determined to be created and approved by all parties. Every block is uniquely recognised by a hash value that is produced by combining the hash value of the previous block and the data pertaining to the current transaction with an appropriate hash algorithm. Blocks join together to build chains by joining the hashes. The blockchain's security is mostly dependent on the digital signature, hash function, and consensus process [3–10]. The QBA framework [7, 8] presents a multicast round where the primary player signs and multicasts the message to backups. Parties are divided into three categories during the block generation process, employing quantum digital signature (QDS). In contrast, the QSYAC consensus categorises parties into two and utilises the toeplitz group signature (TGS) [11].

The security of blockchain technology is influenced by the strength of the traditional signing and encryption system, which is based on digital signatures. The two encryption techniques that are frequently utilised in the digital signatures of a standard blockchain are elliptic curve cryptography (ECC) [12] and RSA [13], which is extensively used for secure data transmission. In 1994, Shor et al. demonstrated that discrete logarithms [14], such as RSA and ECC, can be easily solved using the quantum algorithm. Therefore, devising new techniques to prevent the threat of quantum computing has become crucial. Quantum cryptography, based on the peculiar properties of quantum mechanics, is one effective technique to secure a quantum network. QKD protocols, such as the well-known B92 [15], COW [16], and BB84 protocol [17], are also utilised in quantum information. Even in the presence of quantum processing, these tactics enhance the safety of communication operations.

According to Kirchhoff's principle, all modern cryptosystem algorithms should be open to the public. A quantum public-key signature technique that can deal with the problem of a lost quantum signature has just been described in Ref. [18], which is based on the Hadamard and $H_{\pi/4}$ operators where the verifier is not required to execute a quantum exchange test in Ref. [18]. However, the key generator had to maintain the classical one-way function (COWF) method. The Kerckhoff principle was broken since the COWF privately guaranteed the security of all signer's secret

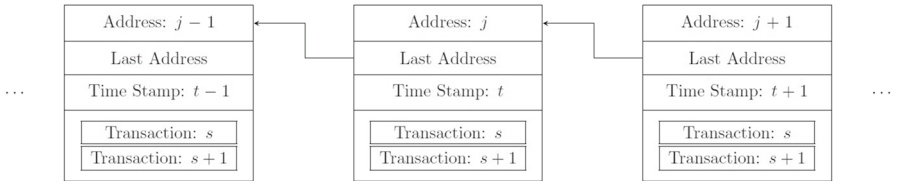

Fig. 1 Classical blockchain structure

keys. Hence, the complete security of the signer's private keys cannot be guaranteed by a COWF.

A blockchain framework comprises a block header and a block body, as shown in Fig. 1. The header of the block will provide the addresses of the current and previous blocks, while the body of the block will contain any transaction data (including the transaction signature). The block body contains transaction information with a signature for the verification procedure. An explicit address can change the block's hash value. Using the block addresses, one can begin at the end of the block and move towards the necessary information.

Classical blockchain security is in danger as a result of the development of quantum computers [19–21]. Digital signature techniques in some traditional blockchain systems depend on complicated challenges like discrete logarithms or factoring big integers. Shor's quantum algorithms [14], on the other hand, can resolve these issues in polynomial time, making the related traditional digital signature systems insecure. Grover's quantum search algorithm [22, 23] can additionally square root accelerate the computation of hash function inverses, significantly increasing the processing capacity of nodes equipped with quantum computers. Nodes using quantum computers may monopolise block mining in blockchain systems that use PoW [2] or PoS consensus algorithms [4, 24], potentially opening the door for a 51% attack [25]. Additionally, DPoS [5] may be vulnerable to quantum assaults if the DPoS voting procedures rely on conventional cryptographic techniques that are breakable by quantum computers.

The vulnerability of traditional digital signatures and hash functions in classical blockchain systems poses a significant challenge, potentially solvable by quantum computers. Conventional encryption using public and private keys is at risk from quantum computing. Quantum cryptography is increasingly utilised across various fields, including artificial intelligence, blockchain technology, and big data initiatives. The blockchain community is actively researching ways to ensure the scalability of blockchain technology in quantum applications to counter the threat posed by quantum computing [26–29]. Moreover, research explores the application of quantum mechanics to enhance blockchain security, known as QBC, including the development of quantum digital signatures to authenticate transactions. Recent experimental studies have investigated quantum principles in QBC systems to improve security measures [30, 31]. Quantum cryptography offers a viable solution, utilising quantum techniques to defend data against quantum attacks and maintain the secrecy and integrity of blockchain data.

This paper utilises multi-bit encryption [32] instead of one-bit encryption. The proposed blockchain framework employs a multi-bit quantum public-key cryptosys-

tem (PKC) termed quantum state computational distinction with cyclic permutation ($QSCD_{cyc}$) to ensure security. Multi-bit quantum PKC provides higher security by offering a larger key space compared to one-bit encryption, enhancing cryptographic strength. As the signer will receive private and public keys, the signature and verification algorithms are asymmetric. A y-bit message is signed using trapdoor information π, and the quantum public key of the verifier is used to validate the signature. Unconditionally secure QKD protocols, Refs. [15, 17, 33–35] are used to assure security. This paper utilises quantum mechanics principles to fortify the security of the QBC against hash rate attacks, double-spending attacks, and signature forgery. Our framework achieves heightened security by reducing the number of operations and transactional activities.

The main contribution of this paper is summarised as follows:

- Using quantum voting, a novel consensus process known as QSYAC creates blocks quickly. The fairness of the QSYAC consensus process is guaranteed, while block creation is guaranteed by this method.
- The quantum bit (qubit) is used to design the quantum block, and the blocks are lined through the quantum entanglement, which provides the chaining in the blockchain.
- The paper also presents a detailed security analysis and comparison among various similar blockchain schemes.

This paper is organised as follows: Sect. 2 describes the QBC framework in preliminary along with similar work on QBC. It also introduces the block generation method using QSYAC and the voting concept. Section 3 describes the scheme of signing and verifying the blockchain transaction and represents the key generation process for the proposed work. Section 4 provides the security analysis of the proposed scheme. In addition, it compares with the existing blockchain schemes. Section 5 provides scopes, application impact, challenges, and the limitation of the work. Section 6 concludes the paper.

2 Preliminaries

This section introduces the QBC structure and blockchain generation using QSYAC. It mainly focuses on the preliminaries and related work on the QBC.

2.1 Quantum blockchain

A QBC is created using the concept of quantum physics, like quantum state and quantum entanglement (QE). A block of the QBC is represented using the quantum state like $|\psi\rangle = \frac{|0\rangle+e^{i\theta p}|1\rangle}{\sqrt{2}}$ where p is used to represent the classical information. Figure 2 shows the blockchain structure. The link between the blockchain is created using the QE. As shown in Fig. 2, each quantum block has a state entangled with the state of the immediate next block in the QBC. Unlike the classical blockchain, the QBC is connected by a controlled Z (CZ) operation shown in Eq. (1), also known as an entangled state.

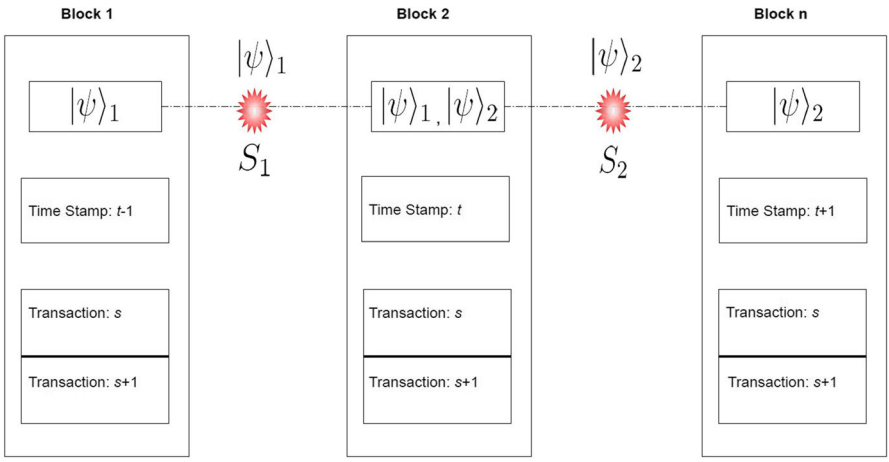

Fig. 2 Quantum blockchain structure, where S_1 and S_2 are the source to generate engagement pair $|\psi\rangle_1$ and $|\psi\rangle_2$, respectively

$$\mathrm{CZ} = |0\rangle\langle 0| \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + |1\rangle\langle 1| \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1}$$

Most of the blockchain frameworks are based on a similar concept [20, 36] and [21]. QBC, based on QE, stores information in a quantum state. Each block contains two entanglement pairs, except the first and last block in the blockchain, and the timestamp t is generated automatically for each block.

2.2 Block generation using QSYAC

The consensus process QSYAC is a modification of YAC and uses TGS instead of the public-key signature, where the client nodes and peer nodes are the two different categories of participants in QSYAC. The proposed framework must have at least $\frac{2}{3}$ trusted nodes [37] in the blockchain for the verification of the new blocks. QSYAC is a round-based block-generating algorithm. There is a distinct proposing peer node in each round. Other peer nodes are called voting peers. Assume the set of all peer nodes is $\{1, \cdots, n\}$. The peer node $(r \mod n) + 1$ becomes the proposed peer node for round r, and all other peer nodes become voting peer nodes. Transactions are created by client nodes and distributed to all peer nodes. Voting peer nodes will update and validate the block proposal. Voting peer nodes are in charge of approving transactions in proposals, validating them, and putting them in blocks to form the blockchain. The QSYAC protocol [10] is as follows:

(i) *The proposing phase*: A block proposal is prepared by the proposing peer and sent to the voting peer nodes after signing it with the TGS scheme [11].
(ii) *The voting phase*: Voting peer nodes trade votes among one another. After receiving a proposal, the voting peer node verifies it. The two elements that make up the pair that symbolise the voting peer node's vote on the block

are the block's hash value and the TGS of that hash value. Each peer node receives an order for the current round when they vote for a block. A function that creates the order takes the block's hash value, resulting in an order for all the peer nodes. To produce an output with a uniform distribution, it needs an order function, $\mathcal{F}$, for two peer nodes. With respect to two orders of peer nodes, $\mathcal{OD}_1 = \{o_1, \cdots, o_n\}$ and $\mathcal{OD}_2 = \{o'_1, \cdots, o'_n\}$, it is true that $\{a \in \{0,\ 1\}^L : \mathcal{F}(a) = \mathcal{OD}_1\}| = |\{a \in \{0,\ 1\}^L : \mathcal{F}(a) = \mathcal{OD}_2\}$, L being the hash value's length.

(iii) *The decision phase*: Each peer node receives a vote for a block in the prescribed sequence. The hierarchy to be $(o_1, \cdots, o_n)$. The following decision phase determines whether a block is accepted or rejected:

(a) Let $i = 1$;
(b) Every vote is transmitted to the peer node o_i
(c) *Accept message*: A percentage greater than $\frac{2}{3}$ of all network peer nodes is considered to be a majority. This set of votes permits the construction of an accepting message for the block once o_i has obtained a majority of votes for one block. The o_i notifies all peer nodes that they have been accepted. A peer node adds the newly generated block to its local blockchain as soon as it receives an accepting message and also broadcasts the message to all other peer nodes after finishing the round.
(d) *Reject message*: When o_i fails to secure the majority votes for any of the blocks, a rejecting message is sent. Similar to how the acceptance message is broadcast by o_i, so is the rejection message. In the event of a rejecting message or the absence of an acceptance message after a predefined waiting period, a peer node *T*ransfers its vote to the peer node o_{i+1}. Peer node o_{i+1} is then included as a decision-making step.
(e) If there is no accepting message provided, the block is rejected, the blockchain is not updated, and the decision-making process is finished.

All honest peer nodes will add the identical block to the proposing peer node's blockchain in this round if the proposer is an honest peer node. All trustworthy peer nodes will still receive an accepted message and add the identical block to the o_1 blockchain, even if it is not honest.

2.3 QKD for secure key sharing

One of the most crucial parts of quantum cryptography is the distribution of quantum keys, which can only be accomplished with certain techniques. It is possible to exchange keys using the quantum physics principle as the foundation for security. The B92 [15] protocol is based on the Heisenberg Uncertainty Principle, used for key distribution. In a typical B92 protocol utilising polarisation encoding, Alice transmits Bob a stream of single photons using the quantum channel, with each photon's polarisation state being randomly chosen between any two non-orthogonal measurement basis as shown in Fig. 3, such as $|0'\rangle$ and $|1'\rangle$, where $\langle 0'\rangle 1' \neq 0$. The classical binary bits 0 and 1 are encoded using these two polarisation states. The measurement basis

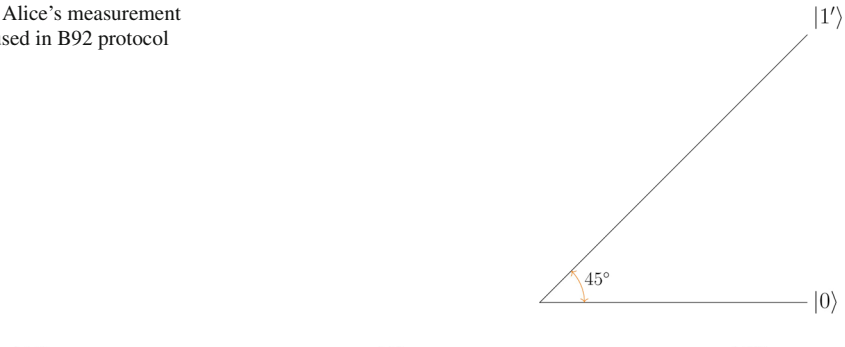

Fig. 3 Alice's measurement basis used in B92 protocol

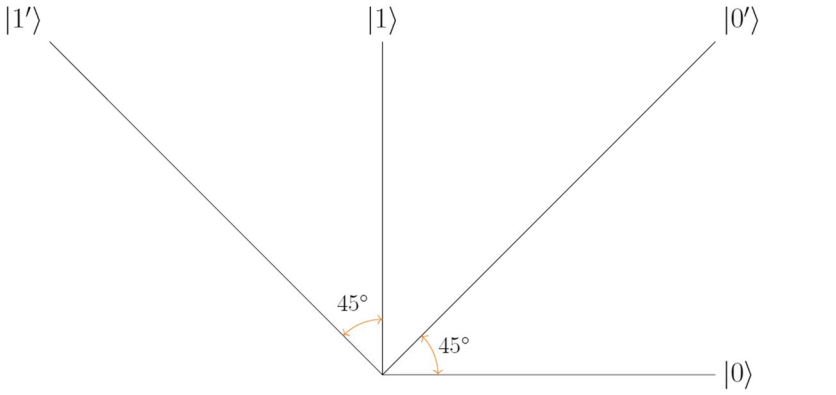

Fig. 4 Bob's measurement basis used in B92 protocol

for which Alice and Bob agreed on the B92 protocol is shown in Figs. 3 and 4. The protocol working procedure is as follows:

(i) Bob randomly selects the computational basis $|0\rangle$, $|1\rangle$ or the $|0'\rangle$, $|1'\rangle$ to measure the quantum bits. Among these randomly selected basis, he only uses $|0\rangle\langle 0|$ or $|0'\rangle\langle 0'|$ for measurement.
(ii) Once receiving the bit from Alice, Bob creates a key if he gets $|1\rangle$ or $|1'\rangle$ as a result of measurement from the quantum bit positions.
(iii) Bob announces his bit positions to Alice using a public channel.
(iv) During the public announcements, Alice and Bob will agree on the identical bit position, and these similar bits will key for both.

Note that when the measurement is applied with the measurement state $|0\rangle$ or $|0'\rangle$, it always returns a 0 result.

2.4 Related work

Bera et al. [38] introduced a device-independent QKD (DI-QKD) scheme utilising random quantum states for key distribution. They used randomly generated states from the Haar distribution that were uniformly produced to examine the effectiveness of entanglement-based QKD techniques. The average secure key rate for each state with

a different DI-QKD rank was analysed as part of the study. Evaluating the randomness of the generated states, they measured their Bell nonlocality and entanglement. Results indicated that as the rank of the random states increased, the effectiveness of DI-QKD in terms of the secure key rate decreased. Moreover, they showed that for both general and optimum collective attack strategies, the secure key rate of DI-QKD falls between that of a pure state and a Werner state for mixed two-qubit states of any rank with identical levels of entanglement.

Based upon findings of Ref. [36], Hu et al. [39] examined the effectiveness of measurement-device-independent QKD (MDI-QKD) in conjunction with asymptotic decoupling (AD), considering statistical fluctuations to improve practical utility. Their research showed that, under typical experimental conditions, incorporating statistical fluctuations through the AD approach could significantly increase the secure key rate and transmission distance of realistic MDI-QKD systems while also improving their resilience to background error rates. Notably, the AD approach can be quickly used in real-world applications since it can be easily incorporated into current MDI-QKD systems without needing hardware modifications.

Ye et al. [40] have proposed a circular mediated semi-QKD (M-SQKD) protocol that utilises Bell states. This protocol involves the successive transmission of qubits between classical users and third party (TP). Additionally, using a circular transport topology, they have demonstrated the M-SQKD protocol's absolute security. Specifically, they have used the particular parameters that two communicating parties may estimate to get a lower bound on the protocol's key rate and noise tolerance (i.e. error tolerance). In addition, they expanded the suggested protocol to multi-party scenarios to enable key distribution between more than two "classical" users because of the scalability of the circular transport structure. Therefore, this protocol may be applied to safeguard the confidential information of several classical users, providing further opportunities to expand the application of the semi-quantum protocol to multi-party situations.

A new quantum encryption framework was presented by Kawachi et al. [32] in 2012, which provides quantum state computational distinction with completely flipped permutations ($\mathrm{QSCD_{ff}}$) computing problem. There are some important properties of $\mathrm{QSCD_{ff}}$: (i) a trapdoor in $\mathrm{QSCD_{ff}}$ that can be exploited to decode the quantum ciphertext; (ii) the $\mathrm{QSCD_{ff}}$ is at least as difficult to solve computationally as the graph automorphism [41] issue in the worst case. The numerical distinction the $\mathrm{QSCD_{ff}}$-problem fulfills some very useful cryptographic features that aid in designing a quantum PKC whose security is ensured by the computational intractability of the graph automorphism problem (GA). Like $\mathrm{QSCD_{ff}}$, $\mathrm{QSCD_{cyc}}$ is a multi-bit quantum PKC with useful cryptographic characteristics.

Wang et al. [37] used $\mathrm{QSCD_{ff}}$ and stake vote consensus algorithm to create a quantum-based blockchain. They ensure the security of the blockchain framework by pushing the malicious behaviour of DPoSB [37] and Stake vote. They use $\mathrm{QSCD_{ff}}$-based quantum public-key cryptography (PKC) on encrypting single-bit messages using the key of length $O(n \log n)$-qubit for encryption.

A blockchain created using time-based entanglement cannot track transaction data back to its source since the QKD blockchain method, such as BB84, does not use quantum signatures. The overall security enhancement of the blockchain is severely

hampered by this constraint. By utilising quantum features for an additional layer of security, quantum signatures are essential in verifying the authenticity and integrity of transactions. However, in a time-based entanglement blockchain, the inability to track and validate transactions is compromised by the untraceability of transaction information, which reduces security. The $QSCD_{ff}$ quantum-based blockchain can overcome this problem.

Li et al. [36] proposed a QBC using the concept of quantum entanglement. They used quantum-deligated proof of stack (QDPoS), a voting-based consensus mechanism, to generate a new block. They have used a single qubit to design the quantum block (node). Each node in their blockchain uses a quantum digital signature Ref. [42] to sign the information before sending it to other nodes. Using the QDPoS, the verified node is written in the blockchain system.

The QDPoS consensus mechanism, which primarily relies on quantum voting, has been used to survive potential quantum attacks on classical voting systems. Similar to DPoS, QDPoS obtains consensus more quickly and fairly than PoW and PoS while using less processing power. QDPoS proves to be a beneficial option for QBCs, especially in a quantum setting. Future QBC proposals can use the QDPoS consensus technique.

Qu et al. [20] have proposed a blockchain for securing electronic media records in the Internet of Medical Things, similar to Le et al. [20] work. They have used the QEMR protocol to avoid external attacks like intercept-measure-repeat and entanglement-measure attacks. The hash value of each block is kept in a quantum state, and a timestamp is generated automatically. They have used a quantum authentication process to guarantee the privacy and security of electronic medical records.

The proposed blockchain links the blocks through entangled states. The timestamp is automatically formed while joining quantum blocks using controlled processes, reducing the storage needed. Each block's hash value is stored in a single qubit. The protocol includes a quantum authentication process to track medical records and guarantee their confidentiality and privacy in IoMT systems.

Banerjee et al. [43] have proposed a blockchain framework using a weighted hypergraph state. Hypergaph is a multiparty entanglement approach. Their proposed protocol for the blockchain uses a single qubit to represent the classical block, and the vertex of the hypergraph is used for the chaining. The protocol has been tested for security and effectiveness in the presence of a quantum computer-based attacker. It makes use of the entanglement of these weighted hypergraph states. Additionally, a suggested technique describes how to set up a QBC utilising an IBM quantum computer that is open to the public.

3 Proposed work

A new blockchain framework is introduced based on QSYAC as shown in Fig. 5. To sign and verify the newly generated block $QSCD_{cyc}$ protocol is used. The blockchain includes three parties, node S, which signs the transaction; node V verifier of the transaction, and node T, a trusted authority for keeping the keys. To manage the security of the keys, the B92 QKD protocol is used.

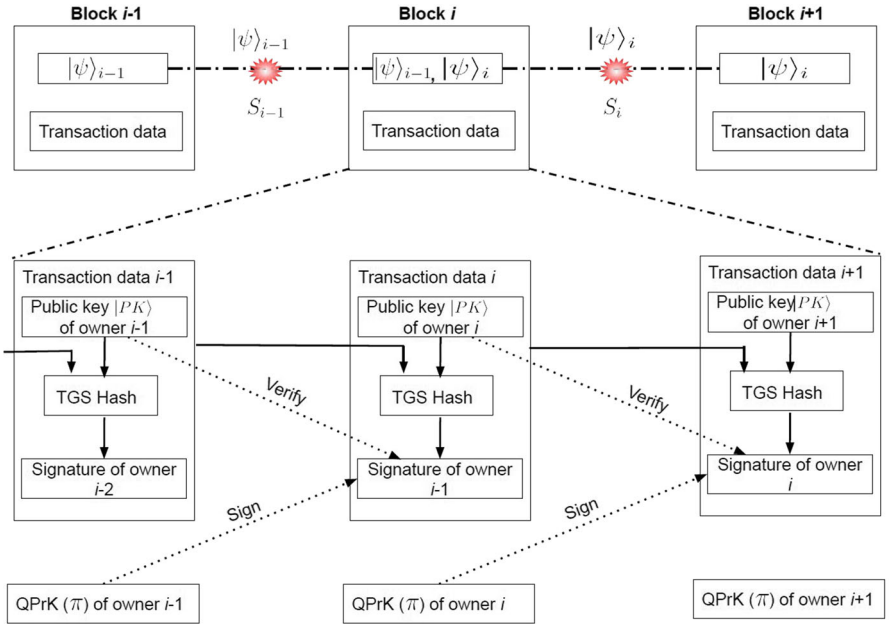

Fig. 5 Proposed QBC architecture using QSYAC

3.1 Singing and verification of transactions

The transactions are signed by quantum nodes using a quantum one-way function based on QSCD_{cyc}. The signing and verification processes are necessary to ensure a transaction's security. The proposed framework uses the quantum one-way function based on the QSCD_{cyc} to complete the signature process.

3.1.1 Overview of QSCD_{cyc}

Set up a hidden permutation π (private key for a node) that will be saved in specific states of the quantum bit. Let's assume that $x \geq 2$ divides y for any fixed number $y \in N$, where $N = \{y \in \mathbb{N} : y \; is \; even \; and \; (\frac{y}{2} \mod 2 = 1)$. Having the following structure, the π, new hidden permutation is a $\frac{x}{y}$ cyclic disjoint permutation of length x:

$$\pi = (j_0 j_1 \cdots j_{x-1}) \cdots (j_{y-x} j_{y-m+1} \cdots j_{y-1}) \tag{2}$$

where $(j_0, \cdots, j_{y-1}) \in \mathbb{Z}_y$ and $j_a \neq j_b$, if $a \neq b$ for any pair $(a, \; b)$. The hidden permutation π has two properties:

(i) It should not contain any fixed points: $\{\pi(j) \neq j; \; j \in \mathbb{Z}_y\}$
(ii) Order is of the form: $\{\pi^x = (id)\}$

For all distinct permutations, $\mathcal{K}_y^x \subseteq S_y$. For $y \in N$, S_y is symmetric group of degree y and $\mathcal{K}_y^x = \{\pi \in S_y : where \; \pi^2 = id \; and \; \forall j \in \{1, \cdots, y\}[\pi(j) \neq j]\}$; identity

permutation is referred to as id. One can define new quantum states with the help of the hidden permutation π as $|\Phi^{\sigma}_{\pi,s}\rangle$. For each $\sigma \in S_y$, $\pi \in \mathcal{K}^x_y$, $s \in \mathbb{Z}_y$ and the state $|\Phi^{\sigma}_{\pi,s}\rangle$ represented as:

$$|\Phi^{\sigma}_{\pi,s}\rangle = \frac{1}{\sqrt{x}} \sum_{t=0}^{x-1} \omega_x^{st} |\sigma \pi^t\rangle \tag{3}$$

where $\omega_x = e^{2\pi j/m}$.

The QSCD_{cyc} is a classification problem for x quantum state ensembles $\{\rho_{\pi}^{(0)}(y)^{\otimes k(y)}\}_{y\in N}, ..., \{\rho_{\pi}^{(x-1)}(y)^{\otimes k(y)}\}_{y\in N}$, where $\rho_{\pi}^{(s)}(y)$ and any arbitrary polynomial k denotes the mixed state $\frac{1}{y!}\sum_{\sigma\in S_y} |\Phi^{\sigma}_{\pi,s}\rangle\langle\Phi^{\sigma}_{\pi,s}|$ for each $\pi \in \mathcal{K}^x_y$. Instead of k, the framework uses k-QSCD_{cyc} when k is fixed. QSCD_{cyc}, the new problem, has cryptographic characteristics as well. And π will be a trapdoor of QSCD_{cyc}.

Given that QSCD_{cyc} employs a permutation π (order $x \geq 2$), it is very much possible to encrypt $\log x$ bits into the states $\rho_{\pi}^{(0)}, \ldots \rho_{\pi}^{(x-1)}$. For each fixed σ, the Generalised controlled π-test is sufficient to create a method which decrypts $|\Phi^{\sigma}_{\pi,s}\rangle$ to s.

If k is any polynomial and quantum algorithm $\mathcal{C}$ solves k-QSCD_{cyc} with a nonzero benefit for a uniformly random permutation $\pi \in \mathcal{K}^x_y$ in polynomial time, that is, there exist $s, s' \in \mathbb{Z}_y$, and a polynomial p, for indefinitely large numbers $y \in N$,

$$\underset{\pi,\mathcal{C}}{Pr}[\mathcal{C}(\rho_{\pi}^{(s)}(y)^{\otimes k(y)} = 1] - \underset{\pi,\mathcal{C}}{Pr}[\mathcal{C}(\rho_{\pi}^{(s')}(y)^{\otimes k(y)} = 1] > \frac{1}{p(y)} \tag{4}$$

where π will be selected randomly from $\mathcal{K}^x_y$. Hence, there exists a quantum algorithm $\mathcal{B}$ that can solve k-QSCD_{cyc} in polynomial time with non-negligible advantages.
The quantum state $\rho_{\pi}^{(s)}$ for π and s, used as an encryption key in QSCD_{cyc}, is generated by a multi-bit quantum PKC algorithm.

3.1.2 $\rho_{\pi}^{(s)}$-Generation algorithm

The $\rho_{\pi}^{(s)}$-generation algorithm can be created using the approximate Fourier transformation [44]. Figure 6 represents a four-bit Fourier transformation circuit for $\rho_{\pi}^{(s)}$ generation. The step is as follows:

Step 1: Utilise the Fourier transformation over the cyclic group $\{id, \pi, \pi^2, \cdots, \pi^{(x-1)}\}$ to efficiently approximate π to F_{π}.

$$F_{\pi}|\pi^s\rangle = \frac{1}{\sqrt{x}} \sum_{t=0}^{x-1} \omega_x^{st} |\pi^t\rangle \tag{5}$$

Step 2: Apply uniform random permutation $\sigma \in S_y$ to the resulting state $F_{\pi}|\pi^s\rangle$.

Step 3: Finally, the desired state $\rho_{\pi}^{(s)}$ is achieved.

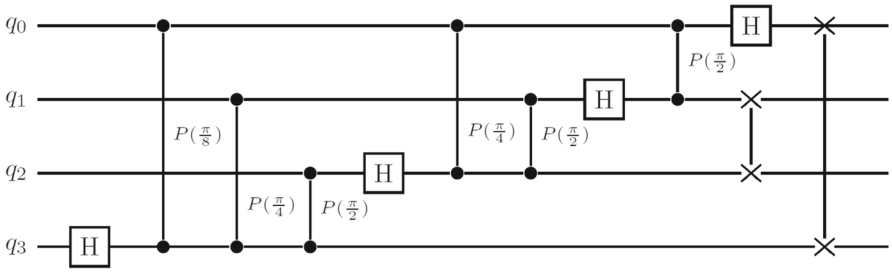

Fig. 6 A four-bit circuit for Quantum Fourier Transformation

3.2 Transaction signing process

There are three parties involved in signing a deal, as depicted in Fig. 7. The transaction is signed by node S, and it is verified by node V. The node T serves as a trusted authority and the system's private key generator. It is assumed that the trusted party generates the key, but it only holds the secret key, as mentioned in *Step 1* of Sect. 3.3 (key generation phase). Figure 7 represents the transaction signing process used to sign and verify the transaction. This trustworthy node T is the blockchain's most reliable block, never disclosing the private key to anyone. Node S is ready to transmit a transaction message encoded as a bit string $\mathcal{T}$ $(t_1,\ t_2, \cdots, t_y)$, $t_i \in \{0,\ 1\}$. It requests node V's encryption key from node T to sign the transaction message $\mathcal{T}$. On receiving the key, it signs $\mathcal{T}$ and sends it to node V for verification. Node V verifies the $\mathcal{T}$ using π received from the node T.

3.3 Key generation phase

The following steps are included in the key generation phase:

Step 1: As the secret key, node S chooses an odd permutation $\pi \in \mathcal{K}_y$, where bit string length $y \in_r L$. The quantum private key (QPrK) π is subsequently written in the blockchain using B92 QKD protocol [15]. The (ID, π) pair is held privately by node T, where ID is node S identity code.

Step 2: To obtain the public key $|PK\rangle = \otimes_{i=1}^{y} \rho_{\pi}^{i+}$, node S uses the $\rho_{\pi}^{(s)}$ generation algorithm (multiple bit).

Step 3: The node S has a key pair $(|PK\rangle, \pi)$.

3.4 Signing phase

Step 1: Node S receives the encryption key $(\rho_{\pi}^{(0)},\ \rho_{\pi}^{(1)}, \cdots, \rho_{\pi}^{(x-1)})$ from the trusted node T.

Step 2: In order to obtain the bit string $t : \pi(\mathcal{T}) = t$, node S performs a cyclic permutation through π operations on $\mathcal{T}$, where the $t = (t_1,\ t_2, \cdots, t_n)$, $t_i \in \{0,\ 1\}$.

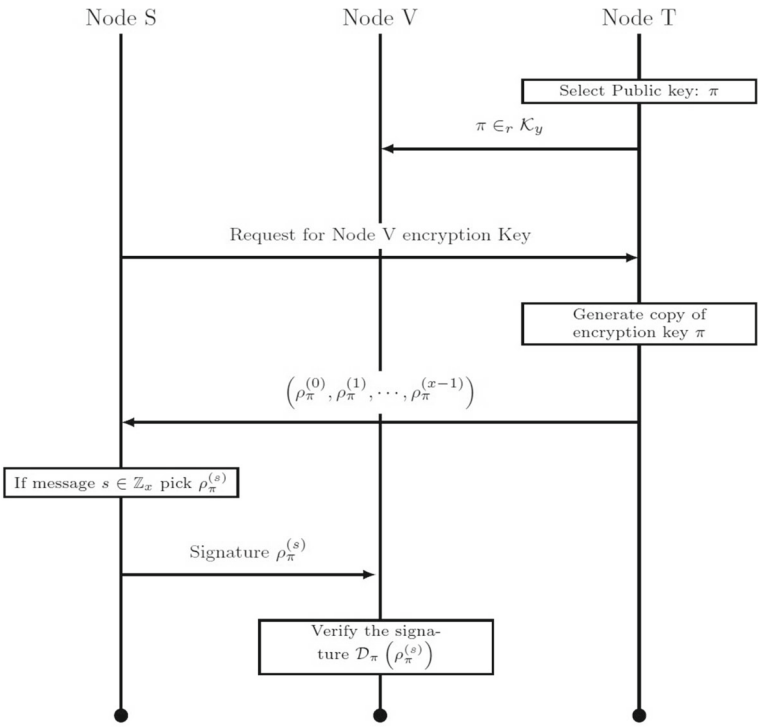

Fig. 7 Transaction signing and verification in quantum blockchain

Step 3: Node S encrypts t as a quantum sequence: $\rho = \otimes_{i=1}^{y} \rho_\pi^i$, where $\rho_\pi^i = \begin{cases} \rho_\pi^+ & \text{if } t_i = 0 \\ \rho_\pi^- & \text{if } t_i = 1 \end{cases}$

Step 4: Signer node S prepares $\mathcal{D}$ decoy particles $\{(\mathcal{D} \gg 2m)$, where $\mathcal{D} \in_r (|0\rangle, |1\rangle, |+\rangle, |-\rangle)\}$. To check eavesdropping it randomly insert $\mathcal{D}$ into $|\rho\rangle|PK\rangle$ to get sequence $|\rho'\rangle|PK'\rangle$. Then, it will send $\{\mathcal{T}, \text{ID}, |\rho'\rangle, |PK'\rangle\}$ to verifier node V.

Step 5: After receiving $\{\mathcal{T}, ID, |\rho'\rangle, |PK'\rangle\}$ by node V, node S reveal the $\mathcal{D}$ position to node V.

Step 6: Node V removes the decoy particles once it verifies there is no eavesdropping in the communication and finally hold $\{\mathcal{T}, ID, |\rho\rangle, |PK\rangle\}$ by eliminating the decoy particle $\mathcal{D}$.

3.5 Verifying phase

Step 1: Node V replaces $|PK\rangle$ to $|PK_\mathcal{T}\rangle$ based on $\mathcal{T}$, where $|PK_\mathcal{T}\rangle = \otimes_{i=1}^{y} \rho_{\pi,m}^i$ and where $\rho_{\pi,\mathcal{T}}^i = \begin{cases} \rho_\pi^+ & \text{if } t_i = 0 \\ \rho_\pi^- & \text{if } t_i = 1 \end{cases}$

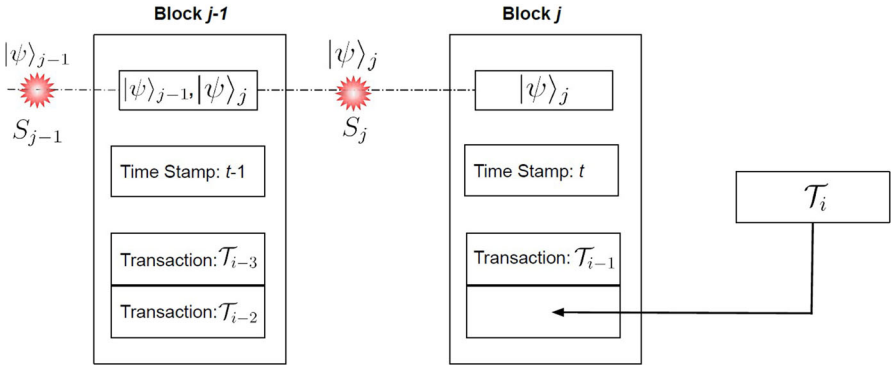

Fig. 8 Message $\mathcal{T}$ will be packed into the block created by the current verifier node

Step 2: Node V prepares $\mathcal{D}$ decoy particles $\{(\mathcal{D} \gg 2m)$, where $\mathcal{D} \in_r (|0\rangle, |1\rangle, |+\rangle, |-\rangle)\}$ and randomly insert $\mathcal{D}$ into $|\rho\rangle|PK_{\mathcal{T}}\rangle$ to obtain the sequence $|\rho''\rangle|PK''_{\mathcal{T}}\rangle$ to check eavesdropping in the system. And send $\{\text{ID}, |\rho''\rangle, |PK''\rangle\}$ to the trusted node T.

Step 3: After receiving $\{\text{ID}, |\rho''\rangle, |PK''\rangle\}$ by node T, node V reveals the $\mathcal{D}$ position to node T. Node T checks these particles corresponding base if any error is obtained, the signature generation phase will restart; otherwise, the next step will be carried out.

Step 4: Node T removes the decoy particles and recovers $\{|\rho\rangle, |PK_{\mathcal{T}}\rangle\}$ by eliminating the decoy particle $\mathcal{D}$.

Step 5: Node recovers private key π based on the ID, and send private key π to node V.

Step 6: On receiving the private key π, node V obtains the bit string $\mathcal{T}'$ by distinguishing $\rho^i_{\pi,\mathcal{T}}$ where $\mathcal{T}'_i = \begin{cases} 0 & \text{if } \rho^i_{\pi,\mathcal{T}} = \rho^+_\pi \\ 1 & \text{if } \rho^i_{\pi,\mathcal{T}} = \rho^-_\pi \end{cases}$. The π permutation is performed on $\mathcal{T}'$ to obtain $t' = \pi(\mathcal{T}')$.

Step 7: If $t' = t$ the signature is accepted by the node V. Hence, the signature is verified by the node V.

3.6 Packaging the transaction into blockchain

As trustworthy signature verifiers, the QSYAC verifier codes should be used. The generated $\mathcal{T}$ transaction information is accurate. If more than $\frac{2}{3}$ verifier nodes accept the signature, $\mathcal{T}$ will be packed into the block created by the current verifier node, as seen in Fig. 8, else $\mathcal{T}$ is deleted by the current verifier node.

At the time of packaging the transaction into blockchain, classical information is stored in the newly entangled quantum state $|\psi\rangle = \frac{|0\rangle + e^{i\theta p}|1\rangle}{\sqrt{2}}$ where p is used to represent the classical information. The blockchain is based on entanglement for chaining. The data are stored in the previous block, as one pair of entangled qubits is stored in the previous block. A network of nodes that validate and verify transactions

keeps decentralisation in place. Each node keeps a copy of the blockchain and uses a consensus process to determine the ledger's current state. By using a consensus process, all nodes are guaranteed to see the blockchain consistently, and no single node can change the ledger. Due to the entangled block in the blockchain, if any single node tries to change the information, it will affect all other blocks in the blockchain as the correlation between the entangled qubits gets altered.

4 Security analysis and comparisons

This section presents an extensive security analysis as well as a comparison of current relevant work using QBC. It also highlights their similarities and differences through Table 1.

4.1 Security analysis

The security analysis of the proposed QBC revolves around three key aspects. In the first aspect, information-theoretic security is considered as shown in Theorem 1, which means that any asymmetric quantum encryption is considered secure when the quantum ciphertexts exhibit computational indistinguishability. Secondly, the data on the QBC are linked together through quantum entanglement to form a chain, and it also serves as a decentralised and distributed ledger. The immutability of information inside this framework must be ensured. The consistency and unforgeability of transactions are the third aspect of security in the QBC. Making sure that all nodes concur on the legality and integrity of transactions becomes crucial because there is no involvement of a third party to validate transactions and achieve consensus among nodes.

Theorem 1 *Indistinguishability of quantum cyphertext. Any adversary $\mathcal{E}$ with unlimited quantum computational capabilities cannot computationally distinguish cyphertext from any block.*

Proof Let's take two computationally indistinguishable quantum ensembles ρ_1 and ρ_2. Let the following equation be satisfied for every positive polynomial $P(.)$, every probabilistic polynomial algorithm A, and positive large number n:

$$|P_r(A(\rho_1) = 1) - P_r(A(\rho_2) = 1)| < \frac{1}{P(n)}, \tag{6}$$

where $P_r(.)$ is the probability.

The cyphertext in the blockchain is $\rho_\pi^+(n)$ and $\rho_\pi^-(n)$, which provides $\rho_1 = \rho_\pi^+(n)^{\otimes P(n)}$ and $\rho_2 = \rho_\pi^-(n)^{\otimes P(n)}$. Now, apply these value in Eq. 6 and prove:

$$\begin{aligned} &|P_r(A(\rho_\pi^+(n)^{\otimes P(n)}) = 1) - P_r(A(\rho_\pi^-(n)^{\otimes P(n)}) = 1)| \\ &\qquad < \frac{1}{P(n)}. \end{aligned} \tag{7}$$

Assume we have an algorithm A_l that uses probabilistic polynomials, which results in:

$$|P_r(A_l(\rho_\pi^+(n)^{\otimes P(n)}) = 1) - P_r(A_l(\rho_\pi^-(n)^{\otimes P(n)}) = 1)| \geq \frac{1}{P(n)}. \tag{8}$$

It means that, to solve the $QSCD_{\text{cyc}}$ problem, we have an effective technique for differentiating signature cyphertexts $\rho_\pi^+(n)$ from $\rho_\pi^-(n)$. However, as demonstrated by Kawachi et al. [32], due to the hardness of $QSCD_{\text{cyc}}$ problems, problem Eq. (8) cannot be solved in polynomial time. As a result, our blockchain can be said to have quantum information-theoretic security. □

Theorem 2 *Given an adversary $\mathcal{E}$ with unlimited quantum power, the provided QBC is untemperable, and if he tampers any quantum block, he will be detected.*

Proof A quantum block consists of a quantum state $|\psi\rangle = \frac{|0\rangle + e^{i\theta_p}|1\rangle}{\sqrt{2}}$. The classical information is stored in the quantum state and represented as p, related to the phase of state $|\psi\rangle$. As each node is connected through the entanglement, they can generate corresponding quantum information and form a chain. If any $\mathcal{E}$ wants to temper the k^{th} block in the QBC, he can do it by measuring the state of the quantum block. As the block is chained through entanglement, measuring one block can collapse the entanglement state of another block. This causes the whole blockchain to collapse without revealing any information to the adversary. In case $\mathcal{E}$ tries to change the phase of the blockchain, the adversary needs a perform the quantum operation on the k^{th} block. All quantum operations are reversible; hence, each node can easily determine if any block in the blockchain has been tempered by measuring it. □

Theorem 3 *Signature Non-Forgeability, for any adversary $\mathcal{E}$ equipped with unlimited quantum computational capabilities, the probability of their ability to successfully forge a legitimate signature is considered negligible.*

Proof Let a signer create the public key $|PK\rangle$ and transaction information $\mathcal{T}$ before using the private key to create the signature $|\rho_1\rangle$. With the use of $\mathcal{T}$ and the signer's private key, an attacker wishes to create a false signature, which makes $|\rho_1\rangle \neq |\rho_2\rangle$. Because the output of the $\rho_\pi^+(n)$ generation procedure is unique and we have $|\rho_1\rangle = |\rho_2\rangle$, the signature algorithm discussed above in section "Signing and verification of transactions" states that the signatures cannot be forged. □

Blockchain is secure in the era of quantum computers because TGS provides absolute security against forging, non-transferability, and repudiation. Even an opponent with infinite computing power cannot forge the digital signature of an honest user. As a result, the threat that quantum computers pose to blockchain is no longer an issue.

4.2 Security analysis of quantum secure yet another consensus (QSYAC) Protocol

Assume that there are $4\mathcal{F}+1$ peer nodes in total, $3\mathcal{F}+1$ peer nodes are honest, and $\mathcal{F}$ peer nodes are dishonest. By contradiction, one can establish the theorem by assuming

that in the same round, distinct blocks from $\mathcal{B}_i$ and $\mathcal{B}_j$ are accepted by o_i and o_j. The majority of votes for $\mathcal{B}_i$ have been cast for o_i, and for $\mathcal{B}_j$, o_j has obtained the majority of votes. In other words, minimum $3\mathcal{F}+1$ votes are cast for $\mathcal{B}_i$, and $3\mathcal{F}+1$ votes are cast for $\mathcal{B}_j$. This disproves the notion that only $\mathcal{F}$ peer nodes are dishonest because minimum $2\mathcal{F}$ peer nodes have voted twice.

4.3 Scalability

Real-world QBC scalability depends on developments in algorithm optimisation, quantum networking, framework design, and hardware design. This study provides a scalable framework which uses QSYAC protocol. If there are n peer nodes, the proposed peer node will send $n-1$ message to the peer nodes who will vote. During the decision-making process, the voting peer nodes can send at most n messages. As a result, QSYAC has $O(n^2)$ communication complexity. As a result, the QSYAC protocol is scalable and scales unquestionably far better than the quantum-secured blockchain QB consensus protocol.

4.4 Security analysis of blockchain

This section provides a security analysis based on different parameters of the blockchain, like blockchain creation, the signing process and security against possible attacks.

4.4.1 Security of block creation

Blocks are generated using consensus algorithms, and each consensus algorithm has a different level of security. In this procedure, the three principal breaking-protocol assaults that fit the malicious adversary concept are: (1) instances of double spending [2], (2) attacks that quickly decode the hash value in a short time [45], and (3) nodes that purposefully interfere with block generation [17]. Then, the paper describes how the proposed blockchain is resilient to these attacks in the block generation process under the scenario of an evil opponent.

Double-spending attacks are possible when attacker nodes secretly create a different blockchain to falsify data in blocks. When the computational force is greater, it results in a high attack success rate. When one node's computational power exceeds 50% of the entire blockchain framework's computing power, the success rate reaches 100%. However, because this attack relies on unnecessary computational power for the proposed algorithm, it can be protected against using blockchain technology.

A unique attack based on a quantum computer is one that quickly decrypts the hash value. The Grover algorithm [46] can be cracked by a quantum computer via quadratic acceleration, making quantum computer-equipped nodes the dominant nodes in blockchain networks. However, because this assault still relies on computational power, the proposed framework can protect against it.

As seen in "Blocks generated by QSYAC" Section, some nodes in blockchain frameworks may actively prevent blocks from being created. Blockchain frameworks

can capture malicious behaviour in the QSYAC protocol, and these records can affect the node's election results. The proposed blockchain framework can also fend against this assault because a node's chance of being chosen as a witness is less when it exhibits more bad behaviours.

4.4.2 Security of the signing process

Eavesdropping, forgery, repudiation, and interception are examples of malicious attacks that could be utilised in this procedure. Then, using the example of a malicious adversary, the paper explains how the blockchain could fend off these attacks.

Private keys Security: Private key security should be guaranteed in two methods. First, it establishes that no quantum algorithm can efficiently distinguish between signature cyphertexts $\rho_{\pi}^{(s)}$, as discussed in the section on "Quantum information-theoretical security". Therefore, if there is no private key π [32], no quantum algorithm can decode the signer's private keys.

Second, the attacker only has a chance $\frac{\sqrt{2^y}}{y!}$ to gain the private keys since they are chosen from the set of values between $\mathcal{K}_y$ and $\mathcal{K}_y = \frac{y!}{\sqrt{2^y}}$ (notice that $y!$ has a far stronger divergence than $\sqrt{2^y}$). As a result of the relatively low success rate of brute force assaults in this situation, attacker-generated random signatures have little chance of being successful.

Security of eavesdropping: The B92 [15] protocol can be used to prevent eavesdropping, as was already indicated. Eavesdropping may cause quantum states to collapse because quantum states are distinct from one another and cannot be copied. The verifier could identify any eavesdropping by monitoring decoy states using the second checkout process in B92 [15]. The no-cloning theorem [47] in quantum also says that it is impossible to eavesdrop by copying signatures.

Security against signature forgery: Before utilising the private key to create the signature $|\rho_1\rangle$, a signer generates the public key $|PK\rangle$ and transaction metadata T. T is used to generate a phoney signature where $|\rho_1\rangle \neq |\rho_2\rangle$ using the signer's private key. The signatures cannot be forged, in accordance with the signature algorithm stated, because the outcome of the $\rho_{\pi}^{(s)}$ generating approach is unique, and it has $|\rho_1\rangle = |\rho_2\rangle$.

In the second method, a signer creates the public key $|PK\rangle$ and transaction information T_1. To ensure that the signature of T_2 passes verification, an attacker would like to alter the signer's transaction metadata so that $T_2 = T_1$. Attackers without access to the signer's private keys are unable to generate a legally acceptable signature under the security of the private keys discussed in Section "Security of private keys". Information about transactions can't, therefore, be faked. In conclusion, it is impossible to perform the aforementioned forging techniques.

4.4.3 Security analysis of blockchain under chosen plaintext attack

Consider a scenario where a single network administrator, node T, who serves as a trusted third party, is connected to a sizable network of "ordinary" users, some of whom

may be malicious against other users. All of these parties can conduct polynomial-time quantum algorithms. The administrator (let's say node T) can deliver information (both quantum and classical bits) to each user through this channel precisely and securely. This communication channel is safe and authenticated. Financial limitations are more likely to drive regular people to rely on inexpensive but unsafe means for regular communication with other users. A malicious person (say, Eve) may eavesdrop on the communication via such an unsecured channel. Anyone seeking to interact with node V must first get a decryption key (π) and an encryption key ($\rho_{\pi+}$) from node T. The decryption key is then transmitted by node T to node V over a secure channel.

Assume that node T is an honest node, node S, wants to send a secure single-bit message to node V. It begins by requesting node T's encryption key ρ_{π}^{+} from node V. Node S encrypts its secret message into either ρ_{π}^{+} state or ρ_{π}^{-} state as an encrypted message and delivers it to node V via an unsafe quantum channel using this key. Eve intercepts node S's ciphertext to listen in on his secret message ρ. Eve can request multiple copies of the keys from node T as she is also a part of the network. To try and determine what information is contained in node S's secret message, Eve utilises a quantum approach on the ciphertext ρ and multiple encryption key ρ_{π}^{+} obtained from node T.

Eve can only collect node S's ciphertext and node V's encryption key in a traditionally chosen plaintext attack. In this case, it is a straightforward generalisation of this classical instance because Eve only acquires copies of a quantum state acting as an encryption key and a quantum state representing node S's encrypted message.

In this case, the keys for each user must be created and distributed by the administrator. A scenario like this has frequently been employed in the real-world implementation of classical Public-Key Cryptography Standards (PKCs); for instance, a government organisation may be permitted to manage those users' keys in the capacity of a third party. It is worth noting that node T only distributes decryption keys across the secure channel once during key setup. Even if they don't provide any additional secret information, each user can communicate their conversations securely to others multiple times using their unique decryption keys. On the other hand, symmetric secret-key cryptography (SKCs) calls for users to exchange private keys. As a result, even in this circumstance, one can benefit from the asymmetry of keys in many-to-many communication that PKCs have over SKCs.

4.5 Comparison among similar quantum blockchain scheme

At present, there exist some quantum-based blockchain schemes. This section provides a comparison between the proposed scheme and some of the existing schemes Refs. [20, 36], and [43]shown in Table 1. The proposed scheme used the QSYAC consensus method, using quantum voting more fairly to select the node than the schemes in Refs. [20, 36], and [43]. Selecting the respective node through the quantum voting takes $O(n)$ time complexity. All other compared schemes Refs. [20, 36], and [43] have the same time complexity $O(n)$. The scheme used in Refs [20, 36], and [43] used entanglement for the chaining. But for entanglement, there must be two minimum qubits generated from the same source. If the third qubit wants to entangle with an already entangled pair,

Table 1 Comparison among proposed scheme and other quantum blockchain schemes

Comparison basis	Proposed Scheme	Scheme in Ref [36]	Scheme in Ref [20]	Scheme in Ref [43]
Consensus mechanism	QSYAC	QDPoS	Relative phase consensus	Relative phase consensus
Consensus time complexity	$O(n)$	$O(n)$	$O(n)$	$O(n)$
Chain structure	Entanglement	Weighted graph state	Entanglement	Weighted graph state
QKD protocol used	B92	N/A	N/A	N/A
Undeniability of nodes	Yes	Yes	N/A	N/A
Information stored in single node	n-classical bit	n-classical bit	n-classical bit	n-classical bit
Resource loss during the consensus process	no	no	N/A	n qubit
Byzantine fault tolerance	yes	yes	N/A	No
Resource require to generate a block	2 qubit in bell state	1 qubit	1 qubit	1 qubit
Transaction verification complexity	$O(n^2)$	$O(n^2)$	$O(n^2)$	N/A
Resistant to hash rate attack	Yes	Yes	Yes	Yes
Resistant to double-spending attack	Yes	N/A	N/A	N/A
Resistant to signature forgery	Yes	N/A	N/A	N/A

it will have some effect on the correlation of the previous entangled qubit pairs. But all the schemes Refs in [20, 36], and [43] try to entangle with the already entangled qubit, which affects the correlation among the entangled pair, which causes information loss from the block. To avoid this issue, the proposed scheme contains two entangled qubits in each block except the first and the last node in the blockchain, as shown in Fig. 5. In contrast with other schemes in which nodes independently produce blocks, leading to a less resilient blockchain system, the suggested technique demonstrates improved efficiency. It is not necessary to transmit extra quantum information on an individual basis in this system since block information shared during the consensus process is classical. This property speeds up the creation of quantum blocks. On the other hand, the scheme in Refs. [20], and [43] requires quantum states to be sent across quantum channels in order to be verified, which requires the use of n qubits individually.

Furthermore, a major obstacle to the security of blockchains is the lack of QKD in the methods described in Refs. [20, 36], and [43]. The QBC may be vulnerable to data manipulation, illegal access, and other issues explained in Sect. 4.4 if QKD-based key distribution is not implemented. However, our proposed scheme addresses these challenges effectively by utilising the B92 QKD protocol, ensuring robust key distribution and enhancing the security of the QBC.

In the proposed scheme, the TGS signature scheme is used to provide absolute security against forging repudiation and non-transferability. Similar to the other scheme in Ref [36], this scheme also achieves the undeniability of the transactions. It uses a similar approach to asymmetric cryptography, where the signature of the node is verified by any node which has the public key. The sender sends a signed message to the participating node, which takes two-way communication and provides the transaction time $O(n^2)$, which is similar to Refs [36], and [20].

Furthermore, the proposed scheme provides security against hash rate attacks, double-spending attacks and signature forgery. The schemes in Refs [20, 36], and [43] consider providing security against the hash rate attack. Hence, the proposed scheme is much more useful science it uses the correct way of entanglement to provide chain structure. Finally, the risk of information loss in the schemes Ref [20, 36], and [43] is more compared to the proposed scheme.

5 Description

Scope: Using the concepts of quantum mechanics, QBC provides improved security by using cryptographic algorithms like QBA [7, 8], QSYAC [10] that are immune to quantum attacks. Additionally, it enables faster transaction processing and increased scalability due to inherent parallelism. Furthermore, QBC guarantees more effective consensus processes that are resistant to quantum adversaries, enabling complex and safe transactions. Quantum-resistant solutions are essential to preserving data integrity and asset security since quantum computing threatens existing blockchain protocols. Despite challenges, QBC holds promise for applications in the Internet of Things, financial, and healthcare sectors and offers more functionality and security than classical blockchain platforms.

Impact: Theoretically, quantum blockchain can lead to breakthroughs in smart contracts, cryptography, and consensus techniques [7, 8, 10] by utilising the principles of quantum computing. While effective consensus techniques and quantum smart contracts allow for sophisticated and safe transactions, quantum-resistant algorithms improve security against quantum attacks.
Practically, quantum blockchain offers enhanced security, faster transaction processing, and increased scalability. Data integrity is protected by quantum-resistant cryptographic techniques, and scalability and transaction processing are accelerated by inherent parallelism. However, reliable quantum-resistant solutions and improvements in the infrastructure supporting quantum computing are needed for practical application.

Challenges: A comprehensive analysis of integrating quantum technology into blockchain systems involves evaluating the current state and future prospects of quantum computing. Shor's [14] and Grover's algorithms [22], prominent in quantum computing, present challenges and opportunities for classical blockchain systems. Shor's algorithm, which is well known for its ability to factor huge numbers quickly, threatens the security of conventional blockchains by undermining popular cryptographic protocols like RSA, whose security depends on the difficulty of factoring large numbers. Grover's approach, on the other hand, provides a quadratic speedup for unstructured search issues, which may affect the robustness of traditional proof-of-work systems by lowering the computational difficulty of locating a legitimate nonce during the hashing process. Even if these quantum algorithms are dangerous in theory, research is still done on how to use them on large-scale quantum computers. Although the practical implementation on large-scale quantum computers is still investigated, it is imperative to overcome issues related to scalability and real-world deployment constraints. Efforts in the blockchain field are directed towards investigating quantum cryptographic algorithms and bolstering security measures against quantum attacks. This study introduces a framework aimed at resolving issues in classical blockchain systems and mitigating risks posed by quantum computing. In Sect. 4.5, various challenges in existing research are addressed and compared.

Limitations: The security of the proposed QBC relies on a quantum-one-way function-based quantum digital signature technique. Block creation is powered by voting and the QSYAC [10] algorithm, while key exchange takes place via the B92 protocol. However, a few limitations are identified in these methods: First, the one-time nature of the signature method is suitable for one use, prompting the need for a more effective quantum signature. Second, despite the security of the B92 protocol against quantum attacks, the possibility of man-in-the-middle attacks and interception persists, with recent attacks posing risks to key distribution. In addition, its flexibility to integrate with current blockchain frameworks and adjust to new quantum technologies also makes it a viable alternative for promoting the use of QBC in a variety of real-world contexts, such as the supply chain, healthcare, and finance industries.

6 Conclusion

This paper suggests a QBC algorithm based on the $QSCD_{cyc}$ method that signs transaction data using a quantum one-way function and produces blocks using QSYAC. The fairness, effectiveness, and the blockchain framework's security can be strengthened by voting and punishing the bad actions of QSYAC and QKD. This paper analysed and discussed the security of the proposed framework. The cost of several operations and transactional activities can be reduced due to the secure environment offered by the QBC. It must be kept in mind that the honest node T has more influence on the network. Consequently, the requirement for a trustworthy node may make decentralisation less effective. Future research could focus on creating quantum signatures that do not require a reliable node. Using more secure QKD methods to guarantee safe communication between nodes can solve the problem of needing a reliable node. Quantum private computing also presents the possibility of creating QBCs and improving blockchain application security. Implementing strong security measures, interacting with regulatory agencies for compliance, optimising quantum algorithms like quantum signature and QKD, and focusing on interoperability solutions are the key to overcoming obstacles in the implementation of quantum private computing for blockchain. These tactics enable the efficient and secure incorporation of quantum technology into blockchain applications.

Author Contributions Mandeep Kumar created all of the tables and drafted the paper, and all the figures have been generated by Bhaskar Mondal. Both authors worked together on simulations, literature reviews, and proofreading.

Funding The authors hereby state that no organisation provided any financial support, either in full or in part.

Data availability During the research, no data were produced that could be disclosed. There isn't any code to share.

Declarations

Conflict of interest The authors have disclosed no personal or financial conflicts of interest about this article.

Ethical approval The article does not contain any investigations involving humans or animals. Therefore, ethical approval is not required.

References

1. Wüstenfeld, J., Geldner, T.: Economic uncertainty and national bitcoin trading activity. North Am. J. Econ. Financ. **59**, 101625 (2022)
2. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Review, 21260 (2008)
3. Jakobsson, M., Juels, A.: In: Preneel, B. (ed.) Proofs of Work and Bread Pudding Protocols(Extended Abstract), pp. 258–272. Springer, Boston (1999)
4. King, S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August 19(1), (2012)
5. Larimer, D.: Delegated proof-of-stake (dpos). Bitshare whitepaper **81**, 85 (2014)

6. Muratov, F., Lebedev, A., Iushkevich, N., Nasrulin, B., Takemiya, M.: Yac: Bft consensus algorithm for blockchain. arxiv 2018. arXiv preprint arXiv:1809.00554
7. Fitzi, M., Gisin, N., Maurer, U.: Quantum solution to the byzantine agreement problem. Phys. Rev. Lett. **87**(21), 217901 (2001)
8. Weng, C.-X., Gao, R.-Q., Bao, Y., Li, B.-H., Liu, W.-B., Xie, Y.-M., Lu, Y.-S., Yin, H.-L., Chen, Z.-B.: Beating the fault-tolerance bound and security loopholes for byzantine agreement with a quantum solution. Research **6**, 0272 (2023)
9. Tan, C., Xiong, L.: Dposb: Delegated proof of stake with node's behavior and borda count. In: 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), pp. 1429–1434 (2020). IEEE
10. Sun, X., Sopek, M., Wang, Q., Kulicki, P.: Towards quantum-secured permissioned blockchain: signature, consensus, and logic. Entropy **21**(9), 887 (2019)
11. Amiri, R., Abidin, A., Wallden, P., Andersson, E.: Efficient unconditionally secure signatures using universal hashing. In: International Conference on Applied Cryptography and Network Security, pp. 143–162 (2018). Springer
12. Miller, V.S.: Use of elliptic curves in cryptography. In: Conference on the Theory and Application of Cryptographic Techniques, pp. 417–426 (1985). Springer
13. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
14. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994). IEEE
15. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
16. Stucki, D., Brunner, N., Gisin, N., Scarani, V., Zbinden, H.: Fast and simple one-way quantum key distribution. Appl. Phys. Lett. **87**(19), 194108 (2005)
17. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179 (1984)
18. Xin, X., Wang, Z., Yang, Q.: Quantum signature scheme based on hadamard and h π/4 operators. Appl. Opt. **58**(27), 7346–7351 (2019)
19. Yi, H.: A post-quantum blockchain notary scheme for cross-blockchain exchange. Comput. Electr. Eng. **110**, 108832 (2023)
20. Qu, Z., Zhang, Z., Zheng, M.: A quantum blockchain-enabled framework for secure private electronic medical records in Internet of medical things. Inf. Sci. **612**, 942–958 (2022)
21. Xu, S., Ning, J., Ma, J., Huang, X., Deng, R.H.: K-time modifiable and epoch-based redactable blockchain. IEEE Trans. Inf. Forensics Secur. **16**, 4507–4520 (2021)
22. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, pp. 212–219 (1996)
23. Wu, X., Li, Q., Li, Z., Yang, D., Yang, H., Pan, W., Perkowski, M., Song, X.: Circuit optimization of Grover quantum search algorithm. Quantum Inf. Process. **22**(1), 69 (2023)
24. Li, X., Xu, J., Fan, X., Wang, Y., Zhang, Z.: Puncturable signatures and applications in proof-of-stake blockchain protocols. IEEE Trans. Inf. Forensics Secur. **15**, 3872–3885 (2020). https://doi.org/10.1109/TIFS.2020.3001738
25. Sayeed, S., Marco-Gisbert, H.: Assessing blockchain consensus and security mechanisms against the 51% attack. Appl. Sci. **9**(9), 1788 (2019)
26. Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., Secundo, G.: Blockchain technology for bridging trust, traceability and transparency in circular supply chain. Inf. Manage. **59**(7), 103508 (2022)
27. Sunmola, F., Burgess, P.: Transparency by design for blockchain-based supply chains. Procedia Comput. Sci. **217**, 1256–1265 (2023)
28. Wang, B., Lin, Z., Wang, M., Wang, F., Xiangli, P., Li, Z.: Applying blockchain technology to ensure compliance with sustainability standards in the PPE multi-tier supply chain. Int. J. Prod. Res. **61**(14), 4934–4950 (2023)
29. Cao, X.-Y., Li, B.-H., Wang, Y., Fu, Y., Yin, H.-L., Chen, Z.-B.: Experimental quantum e-commerce. Sci. Adv. **10**(2), 3258 (2024)
30. Yin, H.-L., Fu, Y., Li, C.-L., Weng, C.-X., Li, B.-H., Gu, J., Lu, Y.-S., Huang, S., Chen, Z.-B.: Experimental quantum secure network with digital signatures and encryption. Natl. Sci. Rev. **10**(4), 228 (2023)

31. Vyvlecka, M., Jehle, L., Nawrath, C., Giorgino, F., Bozzio, M., Sittig, R., Jetter, M., Portalupi, S.L., Michler, P., Walther, P.: Robust excitation of c-band quantum dots for enhanced quantum communication. arXiv preprint arXiv:2305.13273 (2023)
32. Kawachi, A., Koshiba, T., Nishimura, H., Yamakami, T.: Computational indistinguishability between quantum states and its cryptographic application. J. Cryptol. **25**(3), 528–555 (2012)
33. Xie, Y.-M., Lu, Y.-S., Weng, C.-X., Cao, X.-Y., Jia, Z.-Y., Bao, Y., Wang, Y., Fu, Y., Yin, H.-L., Chen, Z.-B.: Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. PRX Quantum **3**(2), 020315 (2022)
34. Fesquet, F., Kronowetter, F., Renger, M., Chen, Q., Honasoge, K., Gargiulo, O., Nojiri, Y., Marx, A., Deppe, F., Gross, R., et al.: Perspectives of microwave quantum key distribution in the open air. Phys. Rev. A **108**(3), 032607 (2023)
35. Zhou, L., Lin, J., Xie, Y.-M., Lu, Y.-S., Jing, Y., Yin, H.-L., Yuan, Z.: Experimental quantum communication overcomes the rate-loss limit without global phase tracking. Phys. Rev. Lett. **130**(25), 250801 (2023)
36. Li, Q., Wu, J., Quan, J., Shi, J., Zhang, S.: Efficient quantum blockchain with a consensus mechanism QDPoS. IEEE Trans. Inf. Forensics Secur. **17**, 3264–3276 (2022)
37. Wang, W., Yu, Y., Du, L.: Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. Sci. Rep. **12**(1), 1–12 (2022)
38. Bera, S., Gupta, S., Majumdar, A.: Device-independent quantum key distribution using random quantum states. Quantum Inf. Process. **22**(2), 109 (2023)
39. Hu, L.-W., Zhang, C.-M., Li, H.-W.: Practical measurement-device-independent quantum key distribution with advantage distillation. Quantum Inf. Process. **22**(1), 77 (2023)
40. Ye, C.-Q., Li, J., Chen, X.-B., Hou, Y., Dong, M., Ota, K.: Circular mediated semi-quantum key distribution. Quantum Inf. Process. **22**(4), 170 (2023)
41. Kobler, J., Schöning, U., Torán, J.: The graph isomorphism problem: its structural complexity. Springer, Berlin (2012). https://doi.org/10.1007/978-1-4612-0333-9
42. Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv preprint arXiv:quant-ph/0105032 (2001)
43. Banerjee, S., Mukherjee, A., Panigrahi, P.K.: Quantum blockchain using weighted hypergraph states. Phys. Rev. Res. **2**(1), 013322 (2020)
44. Kitaev, A.Y.: Quantum measurements and the abelian stabilizer problem. arXiv preprint arXiv:quant-ph/9511026 (1995)
45. Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., Trushechkin, A.S., Yunusov, R.R., Kurochkin, Y.V., Lvovsky, A., Fedorov, A.K.: Quantum-secured blockchain. Quantum Sci. Technol. **3**(3), 035004 (2018)
46. Long, G.-L.: Grover algorithm with zero theoretical failure rate. Phys. Rev. A **64**(2), 022307 (2001)
47. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Phys. Today **54**(2), 60 (2001)