IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 8 June 2023, accepted 12 July 2023, date of publication 18 July 2023, date of current version 24 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3296559

SURVEY

Fortifying the Blockchain: A Systematic Review and Classification of Post-Quantum Consensus Solutions for Enhanced Security and Resilience

JORÃO GOMES JR.[1], (Member, IEEE), SAJJAD KHAN[1], (Member, IEEE), AND DAVOR SVETINOVIC[1,2], (Senior Member, IEEE)

[1]Department of Information Systems and Operations Management, Vienna University of Economics and Business, 1020 Vienna, Austria
[2]Center for Cyber-Physical Systems, Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, United Arab Emirates

Corresponding author: Davor Svetinovic (dsve@acm.org)

This research has been supported in part by ASPIRE under the ASPIRE Virtual Research Institute Program, Award Number VRI20-07. ASPIRE is part of the Advanced Technology Research Council located in Abu Dhabi, UAE.

ABSTRACT The inherent security and computational demands of classical consensus protocols are often presumed impervious to various forms of attack. However, quantum computing advancements present considerable threats to the assumed attack resistance of classical security strategies currently deployed within blockchain systems. Adopting consensus algorithms fortified with post-quantum security measures can significantly enhance traditional blockchains' privacy and security dimensions. Notable advantages of such post-quantum solutions in blockchain consensus include accelerated transaction verification, clarified mining authorship, and resilience against quantum attacks. Yet, a comprehensive analysis of the implications of post-quantum solutions for blockchain consensus is notably absent in the existing scholarly discourse. This paper aims to bridge this gap by systematically reviewing Post-Quantum Blockchain Consensus (PQBC). The four primary contributions of this study are (i) a systematic approach to presenting a comprehensive overview of PQBC, (ii) the systematic selection and analysis of 29 key studies from an initial pool of 1192 papers, (iii) a critical review of methods, enhancements to security, scalability, trust, and privacy, as well as the evaluation employed for PQBC, and (iv) a discussion of primary gaps and prospective directions for future PQBC research.

INDEX TERMS Blockchain, consensus protocol, post-quantum, privacy, security.

I. INTRODUCTION

Consensus protocols (e.g., proof of work and proof of stake) are used in blockchain applications, such as Bitcoin and Ethereum, to establish an agreement between the network nodes ensuring that the information distributed is accurate and consistent [1]. However, one of the most significant limitations of classical consensus protocols is its reliance on high computational resources to solve a mathematical puzzle [2], [3]. Generally, it is assumed that blockchain networks are attack resistant due to the high cost of computational resources. Double-speeding attacks, 51% control attacks, and malicious user attacks are examples of attacks that consensus protocols must be resistant to [4], [5], and [6].

Motivated by the innovative advancements in the field of quantum computing, the existing classical security measures adopted by blockchains are susceptible to various attacks. The fact that quantum approaches can generate faster computation can influence the classical consensus approaches and make the cryptographic methods vulnerable and less secure [7]. Moreover, the existing cryptographic algorithms might be outdated in the coming years due to quantum computing [8]. Studies have shown that classical cryptographic algorithms used in blockchain applications such as Rivest & Shamir & Adleman (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Diffie-Hellman (ECDH), or Digital Signature Algorithm

The associate editor coordinating the review of this manuscript and approving it for publication was Tiago Cruz.

(DSA) can be broken using post-quantum cryptographic methods [9].

Quantum algorithms are becoming a threat to classical blockchain consensus. Grover's [10] and Shor's [11] algorithms are examples of algorithms that benefit from the advancements in quantum computing. Such algorithms have the computational power to impact blockchain applications. A quantum computer using Grover's algorithm can execute Proof-of-Work much faster than classical computers [7], [10]. Since consensus protocols are essential to make the network secure and consistent, it is necessary to ensure that blockchain consensus protocols must be able to resist quantum attacks and also use the power of quantum computers to improve the classical consensus.

Post-quantum cryptography can significantly improve the privacy and security of conventional blockchains. These approaches can improve security and speed up transaction verification for blockchain applications [12]. Post-quantum blockchain consensus (PQBC) equipped with quantum cryptographic methods is an emerging research field that analyses conventional approaches and presents novel solutions based on quantum approaches for blockchain consensus protocols [13], [14], [15], [16]. However, with the growth of the solutions for PQBC, there is a lack of studies analyzing post-quantum solutions in blockchain consensus protocols, how they have been addressed, and the improvements of security, scalability, trust, and privacy (SSTP).

This work aims to fill this gap, presenting a systematic review for PQBC applying a systematic method for the review process. In contrast to the usual literature review process, a systematic review is designed to reduce bias and provide a reliable picture of the current state of the art in a specific research field . Through a predefined protocol, this sort of study follows precise and strict methodological steps to select and analyze relevant papers [17], [18]. Therefore, this systematic literature review's objective and main contribution is to identify, categorize and analyze PQBC solutions and the impact of these solutions for SSTP in order to understand this research topic in a fair, accurate, and auditable way.

The contributions of this paper are:

1) The use of a systematic method to provide an overview of methods, challenges, and evaluations of PQBC;
2) A collection of 29 papers systematically selected from 1162 papers;
3) An analysis of improvements and impacts of PQBC for SSTP;
4) Main gaps and future directions for PQBC.

The remainder of this paper is structured as follows: Section II presents the background. Section III presents the related work. Section IV describes the conduction of the review protocol followed in this paper. Section V presents the answer to the research questions and the discussion about it. Section VI presents some threats to the validity of this review. At last, Section VII presents our concluding remarks and future directions.

II. BLOCKCHAIN CONSENSUS OVERVIEW

Undoubtedly, Blockchain technology has laid the foundation of trust among distributed peers. Consensus algorithms are the key component to form the basis of immutability, trustworthiness, validation, decentralization, and synchronization of the distributed ledger technology. However, consensus algorithms were introduced in 1970 to tackle the Byzantine Generals' Problems by avoiding false information propagation between two or more parties and devising a successful strategy or avoiding failures. This section describes the evolution of consensus algorithms. To present the advancements of the consensus protocols over time, the algorithms are divided into three major groups: Byzantine Fault Tolerant Consensus (BFT Consensus), Nakamoto's Consensus, and PQBC. This section presents an overview of each of them.

A. FIRST GENERATION: BFT CONSENSUS

Generally, consensus means that individual participants agree to a certain state of a system or data values in the system. With the emergence of distributed systems, consensus algorithms were adopted to tackle fault tolerance. Fault tolerance in a distributed computing environment might arise from various reasons, such as malware injection, process failures due to adversarial interference or influence, and physical device capture. [19] lays out the foundation of process failure as Byzantine fault-tolerant (BTF) in distributed computing by formalizing the problem as the Byzantine general problems.

In distributed computing, a process is termed as BFT if the participants agree to (i) Termination; (ii) Agreement; (iii) Validity; and (iv) Integrity, by satisfying the condition $N \geq 3F+1$, where F presents the number of the Byzantine process. However, it is challenging to achieve consensus due to the asynchronous nature of distributed computing environments. In this view, the problem of asynchronous networks and to accomplish the basic requirements of the consensus in the distributed computing environment, [20] developed a partially synchronous consensus algorithm. The Cosmos Tendermint blockchain adapts an extended version of this protocol for the block finalization process.

In terms of practicality, Practical BFT (PBFT) is one of the most well-known consensus protocols in distributed computing. It is based on state machine replication and BFT consensus protocol [21]. A detailed description of distributed consensus protocols is given for [22]. Interested readers are referred to the tutorial to read details about the protocols. Despite the advancements in the distributed consensus protocols, these protocols failed to achieve consensus in a completely decentralized environment. Moreover, the distributed consensus environment entities must reveal their identities to reach an agreement.

B. SECOND GENERATION: NAKAMOTO's CONSENSUS

Consensus between participants in a truly decentralized environment was achieved as participants could validate transactions without trusted third-party or centralized servers with

the inception of the Bitcoin blockchain. The identity of participants was also secure, as the participants in the Bitcoin blockchain used pseudonymous identities rather than revealing their identities. Contrary to the classical consensus algorithms where the state of values with each node was validated using a central server, Nakamoto's consensus validates the values by storing and updating replicas of the blockchain structure on all nodes in the blockchain [23]. With each node able to update the blockchain, the problem of double-spending might occur, where an entity might want to double-spend the same amount in two transactions. Hence, the concept of Proof of Work (PoW) was introduced to avoid such malicious intent by the decentralized participants.

PoW is a probabilistic-decentralized consensus protocol that ensures the legitimacy of a transaction before appending it to the blockchain. The idea is to solve a puzzle by computing a value (nonce) less than a target value to claim a reward. Hence, imposing a high computational cost to partake in the verification process. Despite the groundbreaking work of eliminating trusted third parties or centralized servers, Nakamoto's consensus algorithm is confronted with several issues. In a decentralized environment, nodes attempting to reach consensus result in forks and orphaned blocks in the blockchain. As a result, a huge amount of computational and energy resources are wasted [24]. Similarly, the algorithm failed to achieve scalability in processing a very low number of transactions per block [25]. Moreover, the algorithm is based on the assumption that most of the nodes are honest. Hence, if more than 50% of the nodes collude, various attacks, such as selfish mining or eclipse attacks, are possible. As the blockchain is public, the probability of such attacks cannot be ignored as nodes can join the network.

To overcome some of the limitations of the PoW consensus algorithm, various improved algorithms such as Proof of Stake, Proof of Elapsed Time, and Proof of Authority were proposed to complement the consensus algorithm in decentralized environments [26]. In one way or another, these consensus algorithms are confronted with the risk of centralization, failing to scale in transaction processing, etc. Besides that, advances in quantum computation emerged as a new threat to Nakamoto's consensus. Quantum safety must be added to stand consensus since quantum computers are already a threat to several research fields.

The Nakamoto consensus is still used nowadays and is playing a key role in blockchain applications. However, it can be time-consuming for blockchain applications, even though they have evolved a lot since the first launch of bitcoin [14]. The efficiency of the current blockchain systems is much lower than traditional distributed database systems because of the time-consuming decentralized consensus [14]. For this reason, a third generation of blockchain consensus is emerging: PQBC.

C. THIRD GENERATION PQBC

The advance on quantum computers creates a huge expectation of how computers can solve computationally challenging problems [27]. Grover's and Shor's algorithms are examples of algorithms that benefit from the advance of quantum computing [28]. Such algorithms have the computational power to impact blockchain applications. A quantum computer can use Grover's algorithm to execute Proof-of-Work faster than classical computers [7], [10]. Moreover, common algorithms used in blockchain applications such as RSA, ECDSA, ECDH, or DSA can be broken using Shor's algorithm [9].

In this view, PQBC came as the next step to improve consensus protocols. Most of the PQBC solutions use the principles of quantum physics to improve the classical consensus generation or to propose a novel PQBC. Quantum measurement, quantum entanglement, and quantum random numbers are approaches used for PQBC to create a trust and secure channel to archive consensus among peers in blockchain applications. Besides that, PQBC try to be safe against the threats of quantum attacks [29]. However, it is hard to understand the actual impacts of PQBC since it is a new field of research and only a few works presented solutions for PQBC.

III. RELATED LITERATURE

This section presents the related literature to this work. We discuss similar research on consensus protocols and quantum cryptography methods in PQBC solutions.

The authors in [30] discussed the advantage of quantum computing in PoW mining and several use cases on how quantum PoW can be as profitable as classical PoW mining. In [9], a study is presented on post-quantum blockchains. The authors discussed pre- and post-quantum cryptographic methods and their resistance to post-quantum attacks. In similar research, [31] present an overview of quantum consensus algorithms. The authors describe how the solution for quantum networks can reach agreements among their peers. The authors also pointed out that it is necessary to perform an in-depth evaluation of how quantum consensus can impact blockchain and distributed ledger.

Reference [32] highlighted post-quantum blockchains' security and privacy threats. The authors also discussed a voting mechanism for post-quantum blockchains. Reference [33] discussed quantum synchronization and key distribution in strengthening the security and efficiency of blockchains. Reference [34] present the vulnerability of blockchain to quantum attacks. The authors analyzed blockchain-based cryptocurrencies and their risk to quantum computers. The research revealed that Bitcoin's consensus (PoW) is vulnerable to Grover algorithm-based attacks.

In [35], the authors reviewed and presented a theoretical framework of identity authentication in quantum Blockchain. The proposed framework integrates quantum public key infrastructure with quantum blockchain technology to authenticate identity. However, this work does not cover the technological aspects of PQBC in improving conventional blockchains' security, scalability, trust, and privacy.

TABLE 1. Research question list.

	Research questions
RQ1	What are the main solutions for PQBC?
RQ2	What is the impact and how effective are PQBC in improving SSTP?
RQ3	How PQBC solutions has been evaluating the improvements in SSTP?
RQ4	What are the key challenges that hinder the adoption of PQBC and future directions?

After this brief overview, it is possible to conclude that the literature is improving consensus protocols to be quantum resistant. It is necessary to ensure that consensus protocols can resist quantum attacks. Also, use the power of quantum computers to improve the classical protocols since consensus is an essential step in making blockchain applications secure and consistent. This is of critical importance in complex security and anonymity protection applications, e.g., [36], [37], [38], and [39]. However, no work gathers the main approaches and challenges for PQBC and present an overview of this field. This work came to fill this gap systematically.

IV. PROTOCOL DEFINITION AND CONDUCTION

A protocol was adopted for the execution of the systematic review to reduce the bias and make the study reproducible. The process used in this paper was based on the same protocol presented by [17]. We detail all steps taken to elaborate the research protocol in this section. The planning process consisted of the following steps: (i) Definition of the research questions; (ii) Selection of the relevant search terms; (iii) Definition of the exclusion criteria; (iv) Selection of the research repositories.

This research aims to identify and understand what is being developed for the PQBC field. The research objectives were defined according to the research questions. Research questions (RQs) aim to categorize and create an overview of the literature, discovering covered topics in the research area [17]. The RQs of this work are presented in Table 1.

The scope was defined using the PICOC method (Population, Intervention, Comparison, Outcome, and Context) [40] based on the research objectives. The PICOC method helps identify relevant keywords from the objectives associated with each entry. It is possible to define the search terms, keywords, and synonyms that must be used to find the relevant papers for this research. Table 2 describes the PICOC elements and the search terms defined for each PICOC element. The search terms were defined using papers to control the results [13], [14], [15], [16]. The selected terms appeared in the control papers, generating evidence about the correctness of the search string.

A logical query string was created using the selected terms. Each PICOC element was separated by an *AND*, and each synonym term was separated by an *OR*. The search string can be represented as follows:

(blockchain OR "distributed ledger" OR bitcoin OR ethereum) AND (consensus OR "proof of work" OR "proof of stake") AND (method OR technique OR algorithm OR approach OR protocol OR model OR mechanism) AND (quantum)

Unrelated works to the research's purpose can still be found, even the search terms used for this study were extracted from the PICOC field analysis and control papers used. Some exclusion criteria (EC) were chosen to exclude these works during the process and are presented in Table 3.

The databases chosen to execute the search string were Google Scholar,[1] ACM Digital Library,[2] IEEE Digital Library,[3] ISI Web of Science,[4] ScienceDirect,[5] and Scopus.[6] The following steps were performed to determine the databases based on which the research would be carried out [41]: (i) The database can perform searches using logical expressions or similar mechanisms; (ii) The database allows searches to be made to encompass all text or just specific fields (e.g., title, abstract)[7]; (iii) The database must be available at the researcher's institution.

The review was conducted by executing the search string in each scientific repository. We first excluded all the duplicate papers (EC1). We used *Parsif.al*[8] to organize the papers and remove the duplicates. The filtering of papers was performed using the remaining exclusion criteria (EC2 - EC6). The first exclusion was based on reading the title and abstract of the papers. Papers that did not have relevance for this review were excluded. The next stage was reading the introduction and conclusion of each paper in the previous step. The remaining papers were completely read and analyzed according to the research questions. Finally, we performed the snowballing step. This step aims to find relevant papers not returned by the search string by looking at the works cited in the references of the accepted papers. In the last two stages, besides the exclusion criteria, the quality of the paper was also taken into account before the questions were raised to exclude the papers that did not have answers to the research questions. Figure 1 presents the protocol conduction.

In the first step of the protocol, 1162 papers were obtained through the set of the five scientific repositories, where 979 papers were by Google Scholar, 76 papers by Scopus, 64 papers by ACM Digital Library, 36 papers by IEEE Digital Library, 5 paper by ScienceDirect, and 2 papers by ISI Web of Science. First, we excluded 56 duplicated papers. The remaining papers were analyzed through title and abstract reading, where 963 papers were excluded. The 144 papers selected in the second phase had their introduction and con-

[1] https://scholar.google.com/
[2] https://dl.acm.org/
[3] http://ieeexplore.ieee.org
[4] http://www.isiknowledge.com
[5] https://www.sciencedirect.com/
[6] http://www.scopus.com
[7] As Google Scholar does not have native metadata feature filtering but has a massive collection of scientific papers, we used a script that performs the abs-title-key filter using the HTML of the pages and Regular Expressions. The script is freely available and can be accessed at https://github.com/joraojr/gscholar-review-filter
[8] http://parsif.al

TABLE 2. PICOC and Search terms definition.

Element	Description	Search terms
Population (P)	Blockchain applications	blockchain, distributed ledger, bitcoin, ethereum
Intervention (I)	Consensus protocols	consensus, proof of work, proof of stake
Comparison (C)	*Not defined*	-
Outcome (O)	Solutions	method, technique, algorithm, approach, protocol, model, mechanism
Context (O)	Quantum computing	quantum

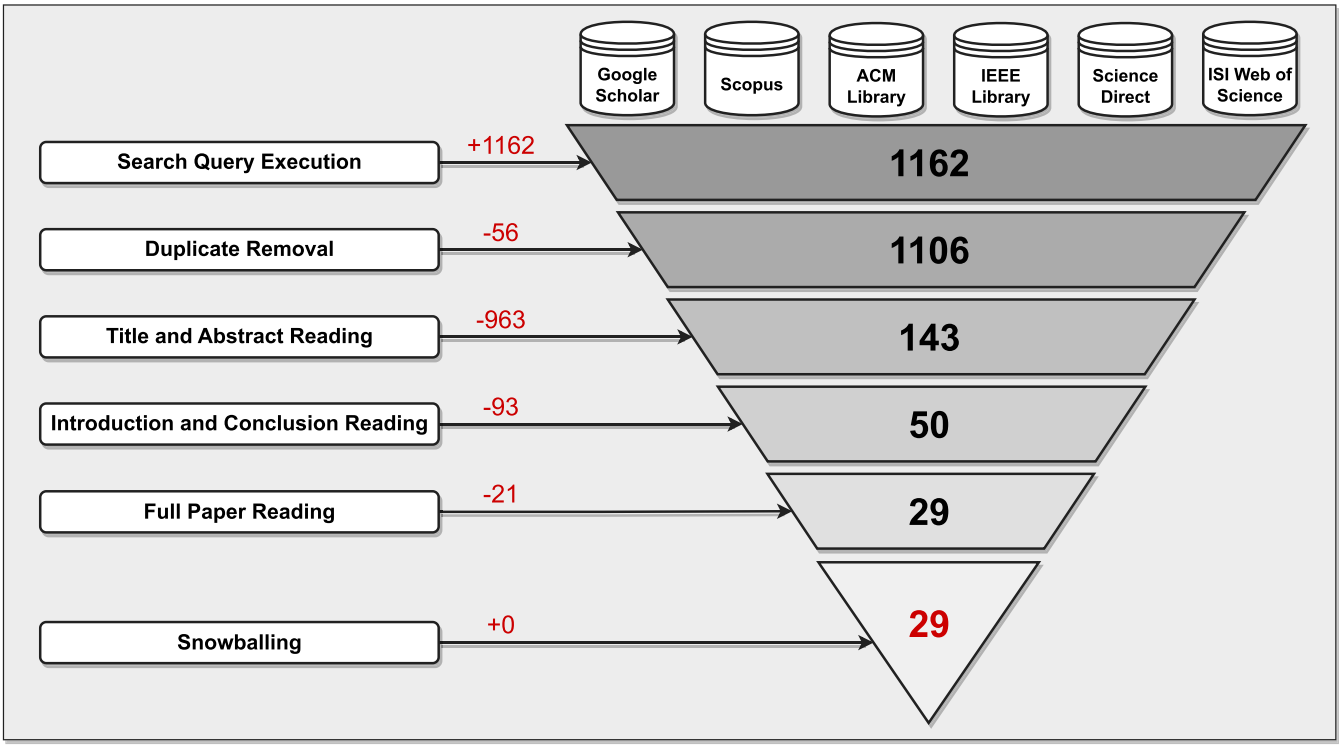

FIGURE 1. Systematic review conduction.

clusion read. Based on the exclusion criteria, at the end of this stage, 50 papers remained. The 29 papers (2.50% of the initial papers) were selected after reading the full text and applying the exclusion criteria. Finally, the forward snowballing step was performed, but no new papers were added in this stage. In this paper, 29 papers were mapped and analyzed in the end. This protocol was performed in January 2023. The accepted papers list can be found in Table 4.

V. SYSTEMATIC REVIEW REPORT

In this section, we provide the answers to the research questions outlined in Section IV, organized into sub-sections. The emergence of PQBC as a research area began in 2018 with the publication of the first work on the topic. Since then, published papers have increased significantly, indicating a growing interest among researchers. This trend can be visualized in Figure 2.

A. RQ2 – WHAT ARE THE MAIN SOLUTIONS FOR PQBC?

This section presents the main information regarding PQBC solutions. First, we describe the solutions used to create new PQBC. Next, we explain the common steps used for PQBC.

TABLE 3. Exclusion criteria.

	Exclusion Criteria
EC1	Duplicates
EC2	Papers that do not present a solution for Blockchain Consensus Protocol
EC3	Papers without post-quantum computing solutions
EC4	Papers not written in English
EC5	Papers that are not available in full text.
EC6	Grey literature[a]

[a] We consider the papers published without a peer review as grey literature, such as pre-prints, technical reports, and others.

TABLE 4. Full list of papers.

ID	REF	ID	REF	ID	REF	ID	REF	ID	REF
1	[14]	2	[16]	3	[15]	4	[13]	5	[42]
6	[43]	7	[44]	8	[45]	9	[46]	10	[47]
11	[48]	12	[49]	13	[50]	14	[2]	15	[51]
16	[52]	17	[53]	18	[54]	19	[55]	20	[56]
21	[57]	22	[30]	23	[58]	24	[35]	25	[59]
26	[60]	27	[29]	28	[61]	29	[62]		

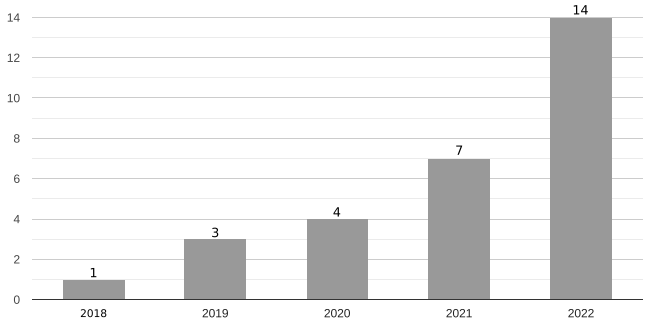

FIGURE 2. Number of publications over the years.

The solutions for PQBC can be divided into two major groups: (i) proposing a novel consensus protocol based on quantum computation and (ii) improving classical consensus to be quantum resistant. Both approaches aim to make blockchain consensus quantum-safe and improve the security of these protocols. We found and mapped 6 PQBC solutions and summarized the steps to PQBC solutions to achieve consensus. The following subsections describe each of them and how the works have been applying these solutions for PQBC.

1) QUANTUM RANDOM NUMBER-BASED CONSENSUS

Random numbers are important in blockchain applications [43]. Ensure that the number generated is random and cannot be reproducible; it is important to the security of the applications. Once the source to generate the random number is discovered, it is possible to rewrite all the information. However, in theory, it is only possible to generate random numbers under certain quantum physical processes that are completely true random (e.g., the collapse process of quantum states) [43]. In this view, quantum random numbers came as a novel way to ensure the numbers generated are random, unpredictable, and verifiable.

Some works created a quantum random number-based consensus by applying the quantum random number concept to PQBC. Reference [43] proposed improving PBFT by applying verifiable quantum random number (vQRN). vQRN is used to improve the randomness and fairness of the PBFT, and any node in the blockchain can judge whether the QRN is valid or not. References [44], [45], and [53] lies on asynchronous BFT. In the BBA proposed by the authors, the BBA will consume quantum-safe new common random coins generated by quantum random numbers. These coins are used to reconstruct the shared secrets in the consensus protocol. The coins have the same function as the nonces in PoW.

2) QUANTUM ENTANGLEMENT AND QUANTUM MEASUREMENT-BASED CONSENSUS

Quantum entanglement occurs when a quantum system generates a set of tiny particles that share quantum states. However, this new entanglement state only exists together, and it is impossible to recreate these particles independently. In other words, a quantum entanglement state exists if and only if it is impossible to represent the quantum entanglement state as a product vector of qubits. Assuming that $|\alpha\rangle$ and $|\beta\rangle$ are two qubits states and $|\Psi\rangle$ is an entanglement state that happened based on $|\alpha\rangle$ and $|\beta\rangle$, $|\Psi\rangle$ is only an entanglement state if it respects the restriction of Equation 1.

$$|\Psi\rangle \neq |\alpha\rangle \otimes |\beta\rangle \tag{1}$$

Quantum measurement is used to probabilistically predict the result in a quantum environment. Linear algebra operations are used to perform it. According to [16], to perform a quantum measurement, three steps are necessary: (i) determining measurement bases; (ii) collapse of the state vector; (iii) evaluation of the initial state. In the first step, the measurement bases perform the spectral decomposition of the states (input state), and a set of eigenvectors are defined to perform the quantum measurement (different bases can generate different quantum entanglement states). The second step has performed the measurement, and the state will collapse into one certain eigenvector with a certain probability (this stage is random and irreversible). In the last step, the evolution of states between the collapsed input states against the original states is evaluated. In a nutshell, as presented by [55], a quantum measurement can be described by the set of measurement operators $\{M_m\}_{0\leq m\leq n}$ under the restrictions of Equations 2 and 3.

$$M_m = |m\rangle\langle m|, 0 \leq m \leq n \tag{2}$$

$$\sum_{n}^{m=0} M_m^{+} M_m = I \tag{3}$$

Applying the quantum measurement and quantum entanglement concepts to PQBC, some works created quantum entanglement and quantum measurement-based consensus. Reference [16] used quantum measurement to generate random numbers and perform the quantum zero-knowledge proof proposed by the authors. In other words, the nonce generation is based on this quantum measure and added to the blockhead. The quantum measure is based on a photon sequence. Reference [51] proposed a new quantum protocol for solving the multivalued Byzantine consensus problem using entangled states. Each general firstly receives a list of equal lengths that none of the other peers know, and based on this list, n generals can reach a consensus against the t generals that are not trustable (where $t < n/3$). Reference [55] proposed a new consensus mechanism based on quantum measurement and teleportation. The quantum teleportation in this paper is used to transmit an unknown quantum state using the qubits of the sender and receiver entangled through a quantum-safe channel. Reference [52] presented a quantum blockchain using multiparty entanglement of quantum-weighted hypergraph states. The quantum measure is applied in the consensus step to verify the information is consistent and can be added to the blockchain (if 1 is accepted; otherwise, the process is aborted, and the peer is identified as untrustworthy).

3) QUANTUM KEY DISTRIBUTION-BASED CONSENSUS

Quantum key distribution creates a secure channel where the peers can share secret keys. The peers in the network only know these keys. The quantum channel created by quantum key distribution is a security method based on quantum cryptography schemes.

Reference [2] proposed a consensus protocol entitled Quantum-Secured YAC (QSYAC) that is a combination of an unconditionally secure signature scheme (Toeplitz Group Signature – TGS) and the Yet Another Consensus (YAC) algorithm. The digital signature scheme is based on quantum key distribution. The authors assume that a quantum network will be used to distribute private keys between participants. In this quantum network, the nodes are connected by quantum channels, which form a quantum key distribution.

4) QUANTUM DISTRIBUTED PROCESSING-BASED CONSENSUS

Quantum distributed processing assumes that quantum computers will be faster than classical ones. So, using distributed systems based on quantum computation will be secure against quantum attacks. However, the principles of quantum entanglement, quantum measure, quantum key distribution, and quantum random number generation are used in distributed processing. The main goal of quantum distributed processing is to be secure and safe against quantum computers.

Reference [46] proposed the general secure consensus scheme (GSCS), an improved version of PoW based on quantum distributed processing. The nodes in the network need to solve multiple mini-parallel mining puzzles to achieve consensus. The verification of all the mini-mining puzzles must be performed to create a new block. Reference [50] presented TensorFlip, a deterministic lottery quantum consensus mechanism. The proposed consensus is fully decentralized and with round complexity of $O(1)$. The protocol employs a quantum-distributed protocol to achieve the consensus. Quantum entanglement and quantum measures are used as part of the protocol.

5) LATTICE-BASED CONSENSUS

The lattice-based solutions are designed to be post-quantum safe and built over basis vectors and lattices. Basis (B) is a set of vectors $b_1, b_2, .., b_k \subset \mathbb{R}^n$ and a lattice (L) is the set of all integer combinations of basis vectors [15], [56]. According to [56], a lattice can be mathematically defined as (Equation 4):

$$L(B) = \left\{ \sum_{n}^{i=1} x_i \cdot b_i : x_i \in \mathbb{Z} \right\} = \left\{ B \cdot x : x \in \mathbb{Z}^n \right\} \quad (4)$$

Applying the lattice concept to PQBC, some works created Lattice-based Consensus. Reference [15] propose an improvement of the PoW consensus using Lattice-based. The entitled Lattice-Based PoW (LPoW) is based on the Hermite-SVP problem and, according to the authors, has fast verification and adjustable difficulty. LPoW has a hard puzzle to solve, but the verification is easy and makes the LPoW faster than the original PoW. The advantage of SVP is to produce a faster algorithm than Grove's algorithm. Similarly, [56] also improved PoW with lattice-based consensus; however, it solved using Closest Vector Problem (CVP). Reference [49] combines PoW and Signature Protocol of Number Theory Research Unit (NTRUSIgn). Based on the NTRUSign the puzzle of PoW is replaced by a signature-based approach. The signature is considered quantum-resistant because it is based on a lattice puzzle. Finally, [47] combines lattice-based and Verifiable Random Function (VRF). The approach is called k-times LB-VRF, where k denotes a particular public-secret key pair generated by the key generation and is used to create at most k VRF outputs.

6) MULTIVARIATE POLYNOMIALS EQUATIONS-BASED CONSENSUS

Multivariate polynomials equations are mathematical expressions where you have to sum powers over more than one variable. Multivariate polynomial equations are supposed to be secure against both quantum computer attacks and standard attacks [14]. A general formula for multivariate polynomials equation is presented in Equation 5, and an example of multivariate equations with 2 variables and power of 2 is present in Equation 6.

$$f(x) = \sum_{i_1=0}^{m} \sum_{i_2=0}^{m} \cdots \sum_{i_n=0}^{m} \alpha_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \quad (5)$$

$$f(x, y) = \alpha_{22} x^2 y^2 + \alpha_{21} x^2 y + \alpha_{12} x y^2 + \alpha_{11} xy + \alpha_{10} x + \alpha_{01} y + \alpha_{00} \quad (6)$$

Reference [14] proposed a post-quantum threshold signature scheme based on an NP-hard problem. The authors used multivariate quadratic equations in a finite field, considered secure when a powerful quantum computer emerges. The proposed signature has six steps: A group leader is selected randomly, and the signature is used among the n users in the group. Private keys are generated by the group leader and broadcast to the n users securely. Public keys are generated based on the private keys by the group leader. At least t users among n users can generate a valid signature for a message, which n users sign. The group leader is the only one who can verify the signature to know who signs the signature. References [13] and [42] presented a consensus architecture similar to PoW. However, instead of using the SHA256 to find the hash value that meets the requirements, the authors propose using multivariate quadratic equations to replace the SHA256 in PoW consensus (solve and verification steps).

7) PQBC STEPS

The steps to PQBC solutions to achieve consensus can be divided into 4 major steps: leader election, block generation, block validation, and chain update. Figure 3 presents an overview of the steps for PQBC.

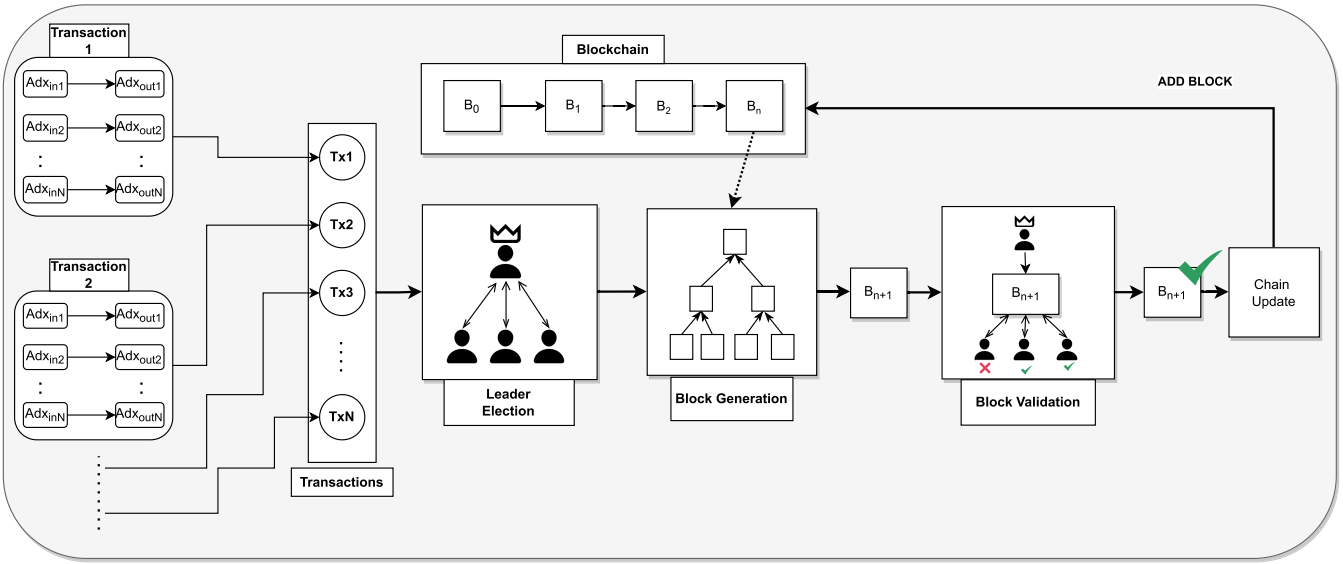

FIGURE 3. PQBC steps.

First, in the leader election step, the blockchain participants decide who will be the block leader. The block leader will lead the block generation. Puzzle-based, steak-based, and random-based approaches are the most commonly used to define the block leader.

Second, in the block generation step, miners create a valid block. Most of the work consists of the package of the transactions, the generation of new hashes, and then broadcasting the new block to peer verification. Some information about the previous block (B_n) is also necessary to generate the new block (B_{n+1}).

Third, in the block validation step, the block leader broadcaster the block to the peers and gets the verification flag of all of them. Supposing those N peers exist in the blockchain and T is a threshold number defined by the blockchain where $1 \leq T \leq N$, at last, T peers must accept the block to continue the protocol. The block creation will be rejected if less than T peers accept the block.

Finally, in the chain update step, the new block (B_{n+1}) is appended to the blockchain, and the chain is updated to the new version.

B. RQ2 – WHAT IS THE IMPACT AND HOW EFFECTIVE ARE PQBC IN IMPROVING SSTP?

This section presents the impacts of PQBC solutions over SSTP.

1) CLASSICAL VS. QUANTUM RANDOM NUMBERS

To resist quantum attacks, the authors used Verifiable Random Function (VRF) with two algorithms based on quantum hard problems [47]. In the first algorithm, a non-zero vector with a uniform distribution is determined with multi-properties. Whereas, in the second, a distribution is obtained using a multi-criteria approach. The approach is effective in avoiding secrets from being leaked. However, the approach can only generate a fixed number of VRF outputs.

To resist quantum attacks, the authors used Verifiable Random Function (VRF) with two algorithms based on quantum hard problems [47]. In the first algorithm, a non-zero vector with a uniform distribution is determined with multi-properties. Whereas, in the second, a distribution is obtained using a multi-criteria approach. The approach is effective in avoiding secrets from being leaked. However, the approach can only generate a fixed number of VRF outputs. In [58], a quantum-safe VRF is proposed using XMSS signature scheme. XMSS comprises three algorithms mainly used for key generation using certain security parameters, signing, and verification. The proposed VRF algorithm is tested in the Algorand setting using different instances to verify correctness, uniqueness, and randomness while achieving low memory and computational cost. The authors claim to have outperformed lattice-based VRF in terms of scalability. However, the work incurs a high communication cost for key updates or in the event of losing the key and joining or leaving the network

Post-quantum blockchain must be able to resist various attacks such as double spending, hash cracking, and disturbing block generation intentionally. To mitigate the hashing and double spending attacks, quantum probabilistic polynomial algorithms can provide security of private keys against eavesdropping, forging, repudiation, etc. [54]. The delegated-PoS-based voting mechanism for block generation can be effective in identifying participants that intentionally disturb the block generation mechanism. Moreover, the presence of semi-honest participants can resist security attacks in a post-quantum blockchain.

2) QUANTUM ENTANGLEMENT AND QUANTUM MEASUREMENT

Quantum measurement is an effective way to determine if a system is in a state of attack. If the system is in some

eigenstate, different entities with the same set of photons will yield the same result. Entities might verify each other using zero-knowledge proof. Unconditional security can be an effective way to secure post-quantum blockchains consensus (such as man-in-the-middle attacks etc.) [16]. Moreover, the use of mathematical puzzles can be a weak strategy to secure PQBC. In this work, the authors state that quantum randomness, quantum measurement, and zero-knowledge proof can resist 51% attack in post-quantum blockchains.

Unconditional secure signatures can resist quantum attacks in PQBC. Toeplitz hash with one-time pad encryption is effective for message transfers by fulfilling security requirements such as unforgeability, transferability, and non-repudiation [2]. The only drawback of such schemes is they can be designed for a fixed-length message. Unconditional secure signatures schemes combined with Byzantine fault-tolerant consensus are able to resist quantum attacks in PQBC.

Quantum computing can outperform the hashing power of classical PoW [52]. In classical PoW, the hash of blocks is stored only in the previous and next blocks. Hence, quantum computing can significantly change the hash in recent most blocks. In order to complement the security of classical PoW, the hash of the blocks can be stored in n-peers using weighted entanglement states to resist quantum attacks.

Various attacks such as intermediaries, interception or re-transmission, and quantum measurement attacks can be detected using quantum teleportation [55]. In this process, information about a state is forwarded using the classical and quantum channels to the users. Then quantum state measurements can be used to detect the various attacks. However, the process relies on the presence of a quantum secure transmission protocol for secret key distribution between the users. As the quantum states cannot be cloned, therefore it's impossible for attackers to eavesdrop or forge secret codes. Moreover, consensus algorithms designed using such schemes provide unconditional security which does not rely on hash algorithms in classical blockchains consensus [59] Quantum entanglement can also be used to refrain malicious nodes from broadcasting false information in the network. The authors in [61] used a two-phase quantum Byzantine agreement to detect and report malicious reports. This work used a trusted third party to store the state of malicious nodes and requires honest nodes to validate the node as malicious or honest using a trust value and dual signature scheme. However, such schemes may incur a high communication cost if the number of participating nodes is higher.

Semi-trusted parties can detect compromised messages in Byzantine agreement problems [51]. Trusted parties can prepare and verify entangled states. To verify that messages are not compromised, multi-criteria measurements are used to measure the results of messages for each general. Moreover, the entangled states are mixed with decoy particles in the preparation and verification process. However, to avoid attacks in such settings, the trusted parties have to be neutral. The authors used a mechanism for censorship-resistance consensus in post-quantum blockchains using one-time used coins [44], [45], [53]. It also leverages concurrent pre-processing using these coins for the next using asynchronous weak secret sharing. The method relies on the presence of honest participants for the secret sharing in an asynchronous PQBC.

3) QUANTUM DISTRIBUTED PROCESSING

Serial Mining puzzles can effectively reduce the risk of centralization and post-quantum attacks [46]. The authors present a serial mining puzzle that involves solving and verification serially and cannot be done in parallel. The verification stage is a multi-criteria process for miners to verify unverified blocks. Moreover, the authors introduced a credibility-based mining scheme to reward or penalize miners. The mining difficulty changes for miners based on credibility level.

4) LATTICE-BASED

Lattice-based signatures are effective in resisting post-quantum attacks. The signatures are based on SIS problems that are np-hard problems [57]. SIS problem aims to find a non-zero vector with multi properties using a uniform random matrix with multi parameters. The authors used a hybrid of two algorithms to generate the keys to verify a message to resist message attacks in the PQBC.

Probabilistic lattice-based signatures schemes can complement the transaction verification process in PQBC [49]. In this work, the authors assume that lattice-based signature schemes are quantum resistant. The schemes mainly rely on calculating the distance between the signature and the coded message. It is only effective in determining whether a signature is authentic.

5) MULTIVARIATE POLYNOMIALS EQUATIONS

The existing consensus algorithms have a verification process with a time complexity of O(n) approximately. Moreover, the verification requires $O(n^2 * m * n)$. The use of heuristic and lattice-based algorithms can sufficiently reduce the mining cost. However, such algorithms might incur an exponential memory cost.

The computational complexity of the existing hashing algorithms in PoW consensus will decrease from O(n) to $1/(N)^{(1/2)}$ in PQBC [15]. Such computational capability can weaken the attack resistance of the existing hashing algorithms. To increase the efficiency of these algorithms, multivariate quadratic equations based can be used to increase the attack resistance of such algorithms. The work also proposes a post-quantum transaction processing mechanism for the PQBC. However, it creates additional communication and computation overheads as the process requires witnesses to sign an additional block and store the headers on decentralized storage. The authors perform a simulation of a blockchain using the proposed PQBC. Theoretically, the proposed mechanism can scale the Transaction Processing Speed (TPS) of the existing algorithms up to three times as compared to PoW.

The authors proposed to divide the block verification and to minimize the impact of malicious nodes influencing leader election. Malicious nodes might partake in the election process with multiple private keys. Hence, an effective way to minimize such attacks is to have private elections for each step of the block proposal, generation, verification, etc. using post-quantum random numbers.

Consensus is one of the most resource and computationally-intensive processes. Therefore, its efficiency is low as compared to traditional data storage schemes such as distributed databases, etc. The introduction of a post-quantum threshold can increase the performance of the current consensus in blockchain application [14]. Post-quantum threshold signature requires more than 50% parties to sign the new blocks. This work introduces the use of managers and nodes to sign the new blocks. The selection of nodes for each block must be random. The underline assumption for such a design is: if the threshold signature for signing the new blocks is based on 51% then it is very difficult to overcome such a scheme. RSA and Elliptic curve-based schemes are considered weak for the PQBC algorithms.

C. RQ3 – HOW PQBC SOLUTIONS HAS BEEN EVALUATING THE IMPROVEMENTS IN SSTP?

There are different approaches to evaluating consensus protocols. This section describes how the works have evaluated the new PQBC against the classical consensus.

1) VERIFIABILITY

PQBC solution must be evaluated in terms of verificability [15], [43], [47]. One of the key points for blockchain applications is the verifiability of the transactions and blocks created. Once the consensus is reached and a new block is added to the chain, the verification of the information added to the chain must be easily verifiable.

2) COMPLEXITY AND COMPATIBILITY

PQBC solutions must be evaluated in terms of algorithm complexity level [43], [56]. Asymptotic analysis is performed to compare two or more different types of algorithms. The lower the complexity, the better the algorithm is.

3) FAIRNESS

PQBC solutions must be evaluated in terms of fairness [43], [46]. As any new peer can join the blockchain and propose a new block, it is necessary to ensure that the block creation was performed fairly. The probability of some peers working unfairly toward the blockchain or avoiding a coalition being created must be evaluated for the new solution. Besides that, the randomness and unpredictability of the algorithm must be one key point of evaluation to ensure that the solutions are unpredictable and irreversible.

4) SCALABILITY AND LATENCY

PQBC solutions must be evaluated in terms of scalability and latency level [2], [14], [15], [43], [46], [47], [49], [51]. Evaluation of how fast the PQBC reach an agreement and a new block is generated and added to the main chain. The latency of novel consensus based on quantum solution tend to be lower than the classical ones.

5) LIVENESS AND CORRECTNESS

PQBC solutions must be evaluated in terms of liveness and correctness [2], [43], [44], [45], [46], [53]. Even if an unusual event happens, the PQBC must guarantee that the best output for the network will be achieved. The best output has a degree of correctness that provides the probability of the consensus itself fixed from a novel event (e.g. fork resolution, two or more honest users adding a new block at the same time, etc.).

6) RESOURCE SAVING

PQBC solutions must be evaluated in terms of resource saving [16], [46], [55]. Some of the classical consensus protocol demands high consumption of computing resources (e.g. PoW) and the novel PQBC solution must evaluate how much their approaches improve the resource savings. For example, it is expected that PQBC be faster than a classical computer, save energy, and not consume too many computing resources.

D. RQ4 – WHAT ARE THE KEY CHALLENGES THAT HINDER THE ADOPTION OF PQBC AND FUTURE DIRECTIONS?

This section presents the limitations and future directions for PQBC.

1) VERIFIABILITY

Quantum algorithms do not solve the problems (undecidable problems) that are not solved by a classical computer, but it solves them faster than classical algorithms [56]. With PQBC, transaction verification, and confirmation criteria must be revised. In the current blockchains, it is assumed that a transaction is confirmed with a block size of six. In theory, rebuilding the previous six blocks is not possible. However, the regeneration's problems must be investigated in PQBC to confirm transactions.

Post-quantum signing mechanism must satisfy basic security requirements such as binding and non-re-usability: users are unable to change signatures from one block to another. Publicly verifiable with anonymity: their signatures must be publicly verifiable without revealing their identity. Eligibility and self-tallying: users must only sign if they are eligible, and signed blocks must be summed publicly.

2) COMPLEXITY AND COMPATIBILITY

Compatibility of quantum blockchains or blockchains empowered by quantum consensus algorithms with the conventional blockchains. Compatibility in terms of miners, leaders selection, and transaction verification. Compatibility must be satisfied for all the existing and new clients in the blockchain

3) FAIRNESS

Post-quantum random number can significantly complement attack resistance in the PQBC. An effective way to improve PQBC is to break down the block generation and verification process between various parties such that a party gets one step using quantum numbers generation.

PQBC have the power to reduce the creation of a coalition. The power of post-quantum computers can allow honest miners to solve puzzles faster than the classical protocols. For instance, with sufficient computing power, it is possible to split one entire puzzle into a series of mini-puzzles. This prevents one malicious miner create a block alone, once creating a new block will be necessary to solve all the small parts. The honest miners will be able to take control of the block creation again.

4) SCALABILITY AND LATENCY

Scalability is an issue with the conventional as well as post-quantum blockchains. In the existing architectures, the transaction processing speed is 7. With PQBC the speed can scale up to 20-50 theoretically. However, such TPS is still very low.

With PQBC, an efficient signing mechanism is required that not only scales in transaction processing capability but also in terms of secure signing. Shor's algorithm is able to decode the existing digital signature schemes in blockchains.

5) MIGRATING FROM CLASSICAL TO QUANTUM SECURE TECHNOLOGY

One of the biggest issues in PQBC is the interactions of existing classical blockchains with quantum-empowered blockchains. One way to enable interactions between the two is to migrate all the assets and coins from a classical blockchain to quantum empowered blockchain using a quantum-empowered hard fork in the existing blockchain. However, such a scheme will require proof of burn on the classical blockchains [60].

6) LIVENESS AND CORRECTNESS

An important issue in the PQBC is its recovery mechanisms in the event of forks. Malicious participants with computational power can intentionally launch double-spending attacks. In such events, what can be the recovery mechanism of the PQBC. PQBC are supposed to have high computational power, therefore, the probability of having forks is relatively high in PQ blockchains as compared to the existing one.

7) RESOURCE SAVING

A quantum cryptocurrency miner can potentially be a faster and more energy-saving option. Quantum computers will require fewer clock cycles, a lot less energy, and dissipate a lot less heat in order to mine the same amount of cryptocurrency as classical computers could mine [30].

VI. THREATS TO VALIDITY

This systematic review aimed to present an overview of PQBC. However, some limitations can treat the validity due to the nature of the systematic literature review process itself. There might be bias regarding the number of researchers selecting the papers. Despite reviewing the overall process and aiming to mitigate this threat to validity, the first and second authors were able to reproduce this process to reduce the possibility of bias. Removing papers not written in English and those in gray literature, for example, can also affect the accuracy of the conclusions, even though the review covered 29 research papers systematically. Besides, some exclusion criteria could be more flexible. However, this review aimed at papers that explained the main process of PQBC solutions and was discussed in detail, even though some influential works in the area might have been lost during the selection process. Besides that, the systematic literature review process tends to be reproducible. Thus, it is relatively straightforward for any new researcher to repeat, validate, and extend a systematic literature review.

Furthermore, errors can be inserted in the protocol definition and the search string might not contain all the relevant keywords. It might cause the loss of some valuable studies. To mitigate this, other researchers reviewed the review planning presented in Section IV, and the search string was evaluated using control papers to ensure the results. The papers appeared in the results, generating evidence about the search string correctness.

At last, not all the electronic databases were considered in this paper, e.g., EI Compendex. So, relevant studies might not be added to the selection of this review. However, this research relies on the representative repositories selected to answer the research questions. Besides relevant electronic databases such as Scopus and IEEE, we also used Google Scholar to reduce the probability of relevant studies are not indexed in our selection. Google Scholar presents a good recall of papers however, it is not the best option to be used alone for systematic review [63]. We believe that the selected electronic databases together with Google Scholar were enough to obtain an overview of the PQBC solutions.

VII. CONCLUSION

Consensus protocol is an important mechanism used by blockchain applications. The consensus is used to ensure that peers can work together in a distributed environment, making it a confident and secure network. The exponential increase of solutions based on quantum computation came as a new threat to classical blockchain consensus since they cannot resist quantum attacks. Post-quantum cryptography can significantly improve conventional blockchains' security, scalability, trust, and privacy (SSTP). So, research in PQBC turned into a new goal for blockchain research.

This work presented a systematic review for PQBC though four research questions (RQ). The systematic report described the main PQBC solutions (RQ1), the impact of these solutions for SSTP (RQ2), how they have been

evaluated (RQ3), and the future steps for PQBC (RQ4). Our findings show that six solutions for PQBC have been implemented by the research works and four main steps are performed for PQBC to archive consensus. Besides that, the solutions for PQBC are effective in improving SSTP in terms of verifiability, liveness, correctness, latency, etc. However, there is a lack of studies dealing with privacy in PQBC. In future work, we intend to implement a PQBC based quantum measurement and zero-knowledge proof to improve the privacy of block leader election.

REFERENCES

[1] A. S. Almasoud, F. K. Hussain, and O. K. Hussain, "Smart contracts for blockchain-based reputation systems: A systematic literature review," *J. Netw. Comput. Appl.*, vol. 170, Nov. 2020, Art. no. 102814.

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

[3] D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," *J. Netw. Comput. Appl.*, vol. 215, Jun. 2023, Art. no. 103633.

[4] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.

[5] M. H. U. Rehman, A. M. Dirir, K. Salah, E. Damiani, and D. Svetinovic, "TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8485–8494, Dec. 2021.

[6] X. Xiang, J. Cao, and W. Fan, "Decentralized authentication and access control protocol for blockchain-based e-health systems," *J. Netw. Comput. Appl.*, vol. 207, Nov. 2022, Art. no. 103512.

[7] M. D. Noel, O. V. Waziri, M. S. Abdulhamid, and A. J. Ojeniyi, "Stateful hash-based digital signature schemes for Bitcoin cryptocurrency," in *Proc. 15th Int. Conf. Electron., Comput. Comput. (ICECCO)*, Dec. 2019, pp. 1–6.

[8] R. Benkoczi, D. Gaur, N. Nagy, M. Nagy, and S. Hossain, "Quantum Bitcoin mining," *Entropy*, vol. 24, no. 3, p. 323, Feb. 2022.

[9] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

[10] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, 1996, pp. 212–219.

[11] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.

[12] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *J. Netw. Comput. Appl.*, vol. 182, May 2021, Art. no. 103035.

[13] J. Chen, W. Gan, M. Hu, and C.-M. Chen, "On the construction of a post-quantum blockchain," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Jan. 2021, pp. 1–8.

[14] H. Yi, Y. Li, M. Wang, Z. Yan, and Z. Nie, "An efficient blockchain consensus algorithm based on post-quantum threshold signature," *Big Data Res.*, vol. 26, Nov. 2021, Art. no. 100268.

[15] R. Behnia, E. W. Postlethwaite, M. O. Ozmen, and A. A. Yavuz, "Lattice-based proof-of-work for post-quantum blockchains," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, J. Garcia-Alfaro, J. L. Muñoz-Tapia, G. Navarro-Arribas, and M. Soriano, Eds. Cham, Switzerland: Springer, 2022, pp. 310–318.

[16] X.-J. Wen, Y.-Z. Chen, X.-C. Fan, W. Zhang, Z.-Z. Yi, and J.-B. Fang, "Blockchain consensus mechanism based on quantum zero-knowledge proof," *Opt. Laser Technol.*, vol. 147, Mar. 2022, Art. no. 107693.

[17] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.

[18] F. W. Neiva, J. M. N. David, R. Braga, and F. Campos, "Towards pragmatic interoperability to support collaboration: A systematic review and mapping of the literature," *Inf. Softw. Technol.*, vol. 72, pp. 137–150, Apr. 2016.

[19] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[20] C. Dwork, N. Lynch, and L. Stockmeyer, "Consensus in the presence of partial synchrony," *J. ACM*, vol. 35, no. 2, pp. 288–323, Apr. 1988.

[21] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Operating Syst. Design Implement.*, 1999, pp. 173–186.

[22] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.

[23] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[24] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: An energy-efficient blockchain proof-of-work consensus algorithm," *Comput. Netw.*, vol. 214, Sep. 2022, Art. no. 109118.

[25] A. E. Azzaoui, P. K. Sharma, and J. H. Park, "Blockchain-based delegated quantum cloud architecture for medical big data security," *J. Netw. Comput. Appl.*, vol. 198, Feb. 2022, Art. no. 103304.

[26] S. Khan, M. B. Amin, A. T. Azar, and S. Aslam, "Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability," *IEEE Access*, vol. 9, pp. 116672–116691, 2021.

[27] S. Kumari, M. Singh, R. Singh, and H. Tewari, "A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for IoT devices," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109327.

[28] S. Mukherjee, "A Grover search-based algorithm for the list coloring problem," *IEEE Trans. Quantum Eng.*, vol. 3, pp. 1–8, 2022.

[29] C. Peng, H. Xu, and P. Li, "Redactable blockchain using lattice-based chameleon hash function," in *Proc. Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS)*, Jul. 2022, pp. 94–98.

[30] D. A. Bard, J. J. Kearney, and C. A. Perez-Delgado, "Quantum advantage on proof of work," *Array*, vol. 15, Sep. 2022, Art. no. 100225.

[31] M. Marcozzi and L. Mostarda, "Quantum consensus: An overview," 2021, *arXiv:2101.04192*.

[32] K. Sentamilselvan, P. Suresh, G. K. Kamalam, and H. Muthukrishnan, "Security threats and privacy challenges in the quantum blockchain: A contemporary survey," in *Quantum Blockchain: An Emerging Cryptographic Paradigm*. Wiley, Aug. 2022, pp. 293–316.

[33] W. Cui, T. Dou, and S. Yan, "Threats and opportunities: Blockchain meets quantum computation," in *Proc. 39th Chin. Control Conf. (CCC)*, Jul. 2020, pp. 5822–5824.

[34] S. Holmes and L. Chen, "Assessment of quantum threat to Bitcoin and derived cryptocurrencies," Cryptol. ePrint Arch., Paper 2021/967, 2021. [Online]. Available: https://eprint.iacr.org/2021/967

[35] Z. Yang, T. Salman, R. Jain, and R. D. Pietro, "Decentralization using quantum blockchain: A theoretical analysis," *IEEE Trans. Quantum Eng.*, vol. 3, pp. 1–16, 2022.

[36] A. Wahrstätter, J. Ernstberger, A. Yaish, L. Zhou, K. Qin, T. Tsuchiya, S. Steinhorst, D. Svetinovic, N. Christin, M. Barczentewicz, and A. Gervais, "Blockchain censorship," 2023, *arXiv:2305.18545*.

[37] A. Wahrstätter, J. Gomes, S. Khan, and D. Svetinovic, "Improving cryptocurrency crime detection: CoinJoin community detection approach," *IEEE Trans. Dependable Secure Comput.*, early access, Jan. 20, 2023, doi: 10.1109/TDSC.2023.3238412.

[38] T.-H. Chang and D. Svetinovic, "Improving Bitcoin ownership identification using transaction patterns analysis," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 9–20, Jan. 2020.

[39] Y. Wehbe, M. A. Zaabi, and D. Svetinovic, "Blockchain AI framework for healthcare records management: Constrained goal model," in *Proc. 26th Telecommun. Forum (TELFOR)*, Nov. 2018, pp. 420–425.

[40] M. Petticrew and H. Roberts, *Systematic Reviews in the Social Sciences: A Practical Guide*, vol. 6. Malden, MA, USA: Blackwell Publishing, 2006, pp. 304–305.

[41] C. Costa and L. Murta, "Version control in distributed software development: A systematic mapping study," in *Proc. IEEE 8th Int. Conf. Global Softw. Eng.*, Aug. 2013, pp. 90–99.

[42] J. Chen, W. Gan, M. Hu, and C.-M. Chen, "On the construction of a post-quantum blockchain for smart city," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102780.

[43] P. Wang, W. Chen, S. Lin, L. Liu, Z. Sun, and F. Zhang, "Consensus algorithm based on verifiable quantum random numbers," *Int. J. Intell. Syst.*, vol. 37, no. 10, pp. 6857–6876, Oct. 2022.
[44] S. Dolev and Z. Wang, "SodsBC/SodsBC++ & SodsMPC: Post-quantum asynchronous blockchain suite for consensus and smart contracts," in *Proc. Int. Symp. Stabilizing, Saf., Secur. Distrib. Syst.* Cham, Switzerland: Springer, 2021, pp. 510–515.
[45] S. Dolev and Z. Wang, "SodsBC: Stream of distributed secrets for quantum-safe blockchain," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 247–256.
[46] J. Wang, Y. Ding, N. N. Xiong, W.-C. Yeh, and J. Wang, "GSCS: General secure consensus scheme for decentralized blockchain systems," *IEEE Access*, vol. 8, pp. 125826–125848, 2020.
[47] M. F. Esgin, V. Kuchta, A. Sakzad, R. Steinfeld, Z. Zhang, S. Sun, and S. Chu, "Practical post-quantum few-time verifiable random function with applications to algorand," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Cham, Switzerland: Springer, 2021, pp. 560–578.
[48] J. Seet and P. Griffin, "Quantum consensus," in *Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE)*, Dec. 2019, pp. 1–8.
[49] B. Mi, Y. Weng, D. Huang, Y. Liu, and Y. Gan, "A novel PoW scheme implemented by probabilistic signature for blockchain," *Comput. Syst. Sci. Eng.*, vol. 39, no. 2, pp. 265–274, 2021.
[50] A. Ahuja, "TensorFlip: A fast fully-decentralized computational lottery for cryptocurrency networks," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2021, pp. 246–253.
[51] Q.-B. Luo, K.-Y. Feng, and M.-H. Zheng, "Quantum multi-valued Byzantine agreement based on d-dimensional entangled states," *Int. J. Theor. Phys.*, vol. 58, no. 12, pp. 4025–4032, Dec. 2019.
[52] S. Banerjee, A. Mukherjee, and P. K. Panigrahi, "Quantum blockchain using weighted hypergraph states," *Phys. Rev. Res.*, vol. 2, no. 1, Mar. 2020, Art. no. 013322.
[53] S. Dolev, B. Guo, J. Niu, and Z. Wang, "SodsBC: A post-quantum by design asynchronous blockchain framework," Cryptol. ePrint Arch., Paper 2020/205, 2020. [Online]. Available: https://eprint.iacr.org/2020/205
[54] W. Wang, Y. Yu, and L. Du, "Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm," *Sci. Rep.*, vol. 12, no. 1, pp. 1–12, May 2022.
[55] X. Wen, Y. Chen, W. Zhang, Z. L. Jiang, and J. Fang, "Blockchain consensus mechanism based on quantum teleportation," *Mathematics*, vol. 10, no. 14, p. 2385, Jul. 2022.
[56] A. Endurthi, P. Yarra, S. Gavireddy, and U. Polishetty, "Closest vector problem-based proof of work mechanism for post-quantum blockchain," in *Innovations in Computer Science and Engineering*. Cham, Switzerland: Springer, 2022, pp. 215–220.
[57] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2019.
[58] M. Buser, R. Dowsley, M. F. Esgin, S. K. Kermanshahi, V. Kuchta, J. K. Liu, R. C.-W. Phan, and Z. Zhang, "Post-quantum verifiable random function from symmetric primitives in pos blockchain," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2022, pp. 25–45.
[59] H. Wang and J. Yu, "A blockchain consensus protocol based on quantum attack algorithm," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–6, Aug. 2022.
[60] S. B. Far, A. I. Rad, and M. R. Asaar, "Goodbye Bitcoin: A general framework for migrating to quantum-secure cryptocurrencies," in *Proc. 30th Int. Conf. Electr. Eng. (ICEE)*, May 2022, pp. 512–517.
[61] X. Gao, J. Xu, and J. Fan, "A novel quantum Byzantine consensus protocol based on malicious node prevention mechanism," in *Proc. Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS)*, Jul. 2022, pp. 202–205.
[62] Q. Li, J. Wu, J. Quan, J. Shi, and S. Zhang, "Efficient quantum blockchain with a consensus mechanism QDPoS," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3264–3276, 2022.
[63] M. Gusenbauer and N. R. Haddaway, "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google scholar, PubMed, and 26 other resources," *Res. Synth. Methods*, vol. 11, no. 2, pp. 181–217, Mar. 2020.

JORÃO GOMES JR. (Member, IEEE) received the B.Sc. degree in exact sciences and the B.Sc. and M.Sc. degrees in computer science from the Federal University of Juiz de Fora (UFJF), Brazil, in 2018, 2019, and 2021, respectively. He is currently pursuing the Ph.D. degree in economic and social sciences with the Vienna University of Economics and Business (WU). He was a Data Scientist with EtherCity and a Research and Development Technical Manager with "RECMEM–Recommendation of Educational Media," sponsored by the Brazilian National Research and Educational Network (RNP). He is a Teaching and Research Associate with WU. His research interests include data mining, information retrieval, cybersecurity, and complex networks.

SAJJAD KHAN (Member, IEEE) received the B.S. degree in computer science from the University of Peshawar, Khyber Pakhtunkhwa, Pakistan, in 2012, and the M.S. degree in computer science from COMSATS University Islamabad, Pakistan, in 2019. He was a Research Associate with the Comsens Research Laboratory. He is currently with the Institute for Distributed Ledgers and Token Economy, Vienna University of Economics and Business, Vienna, Austria. His research interests include blockchain interoperability, distributed computing, and decentralized federated learning, with a special focus on security, privacy, and trust.

DAVOR SVETINOVIC (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Waterloo, Waterloo, ON, Canada, in 2006. He was with TU Wien, Austria, and Lero—the Irish Software Engineering Center, Ireland. He was a Visiting Professor and a Research Affiliate with MIT, USA, and the MIT Media Laboratory, MIT. He is currently a Professor of computer science with the Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, and the Department of Information Systems and Operations Management, Vienna University of Economics and Business, Austria, (on leave), where he is also the Head of the Institute for Distributed Ledgers and Token Economy and the Research Institute for Cryptoeconomics. He has extensive experience working on complex multidisciplinary research projects. He has published over 95 papers in leading journals and conferences. His research interests include security, privacy, trust, decentralized systems, blockchain, and software engineering. His career has furthered his interest and expertise in developing advanced research capabilities and institutions in emerging economies. He is a Lifetime Senior Member of ACM. He is an Affiliate of the Mohammed Bin Rashid Academy of Scientists. He is a highly cited researcher in blockchain technology.