A Survey on Consensus Algorithms in Blockchain based on Post Quantum Cryptosystems

1st Jisha Mary Jose
Research Scholar, CSE
Indian Institute of Information Technology, Kottayam
India
jisham.phd2119@iiitkottayam.ac.in
ORCID: 0000-0002-9729-6009

2nd Panchami V
Assistant Professor, CSE- Cyber Security
Indian Institute of Information Technology, Kottayam
India
panchamam036@iiitkottayam.ac.in
ORCID: 0000-0002-9297-6929

2022 5th International Conference on Computational Intelligence and Networks (CINE) | 978-1-6654-6465-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/CINE56307.2022.10037353

***Abstract*—Blockchain is a distributed, decentralized ledger mechanism with a various features. It is used in diverse applications nowadays,from financial sector to password management. It does not have any central tool to validate and verify the transactions, yet every transaction in the Blockchain is secured and verified. This is achieved because of a consensus algorithm in the network. Latest study reports show that emergence of quantum computing will impact the overall safety of Blockchain and its internal working. Attacks using Grover's and Shor's algorithm can threaten the hashing and public key schemes in cryptography. It will force a complete redesign of the Blockchain systems to withstand quantum attacks. So there is a need to develop quantum-safe Blockchain systems. Consensus mechanisms like Proof of Work (PoW) and Signing algorithms like Elliptic Curve Cryptography used in Blockchain can be modified to overcome quantum attacks. Here a comparative study and analysis of different consensus algorithms developed using post-quantum cryptosystems are done, which can be implemented in Blockchain systems to make them quantum safe.**

***Index Terms*—Blockchain, Consensus, Quantum computing, Cryptography, Post-Quantum systems**

I. Introduction

Blockchain can be defined as a chain of blocks, used to store digital data (transactions) in an an open distributed ledger [1]. A block is chained with the next one using a cryptographic hash of the block. Each block contains transaction data, a timestamp, and hash of the previous block. It is a disruptive technology and is making a huge impact on the modern Internet era. Although the initial purpose of introducing Blockchain technology was to act as the backbone of the digital cryptocurrency Bitcoin and prevent issues like double spending problem, now it has become widely popular for implementing applications which require features like immutability and decentralization [4]. The innovative idea here is that Blockchain guarantees the exactness and safeness of transaction data and guarantees trust without any trusted third party. So the ultimate aim of Blockchain systems is to record and distribute data without any modifications. Nowadays, Blockchain is used in various fields like the Internet of Things (IoT), the banking sector, healthcare, supply chain systems etc, for handling data. Blockchain has many versions namely: Blockchain 1.0 is the implementation of the cryptocurrency Bitcoin, Blockchain 2.0 is the concept of smart contracts and Blockchain 3.0 is the usage of Decentralized Apps (DApps). The prime advantage of using Blockchain in these applications is that it saves time and money and gives added security. Some of the other characteristics of Blockchain include [2]:

- Transparency
- Immutability
- Decentralization
- Anonymity
- Programmable
- Integrity

Different types of Blockchain are available today, as shown in Fig 1, which include Public Blockchain- they are permission-less and can be used by anyone without any restriction, Private Blockchain- they are permissioned chains used in organizations or enterprises where only limited participants are there, Consortium Blockchain-they are semi-decentralized i.e., the chain is run by multiple organizations, Hybrid Blockchain-it is a combination of public and private Blockchain systems.

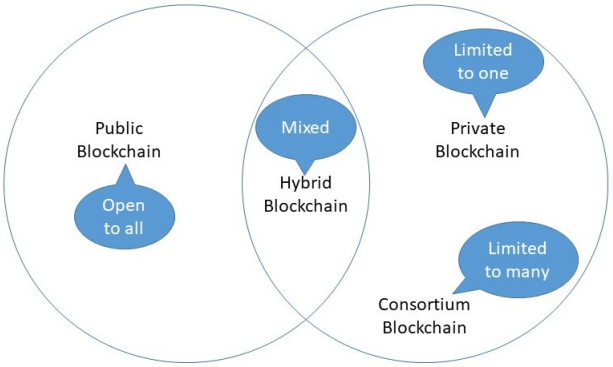

Fig. 1. Types of Blockchain

II. Background Study

A. Blockchain node

Once a transaction or event log is stored in a Blockchain, it cannot be removed or altered. This immutability property makes Blockchain systems suitable for many applications. A Blockchain node is an entity that can perform operations

on the network. A Blockchain miner is a type of node that performs validation of transactions stored on the chain. Since it's a decentralized network, it leads to serious distrust among the nodes when handling transaction data [4]. To ensure the smooth workflow and reliability of the overall network, nodes on the network need to perform certain negotiations using different protocols to achieve a consensus.

B. Consensus algorithms

In a distributed, decentralized network trust among the nodes is very important. Each time a node wants to add any data onto the network, every other node must agree, i.e., a consensus must be reached. This is mainly because in such decentralized systems there are no pre-assigned trusted third parties. So in such kind of networks say for example Blockchain networks, negotiations are made using certain algorithms and they are collectively known as consensus algorithms. These consensus algorithms also make sure that attacks like double spending do not occur, ensure fairness, security etc.

It is an algorithm employed in Blockchain systems to decide which node on the network is allowed next to append a new block onto the chain [5]. Consensus algorithms are also required to validate the transactions happening on the nodes of the network so that they can be updated on the chain i.e. the ledger. The most widely used consensus technique in Blockchain systems is Proof of Work (PoW). But different Blockchain architectures use different other consensus algorithms as well, depending on their requirements. Some of the commonly available algorithms are:

- Proof of Stake
- Proof of Existence
- Proof of Exercise
- Byzantine Fault Tolerance
- Proof of Luck
- Proof of Importance
- Proof of Elapsed Time
- Delegated Acyclic Graph

The consensus algorithms make the Blockchain versatile in nature and hence they play a major role in the proper working of Blockchain systems. They have undergone various changes and improvements over time so that we can ensure the stable working of the corresponding Blockchain in which it is used. We can evaluate the technical level of a consensus mechanism using different aspects:

- Consistency
- Security
- Scalability
- Resources used
- Performance

The consensus protocols used in Blockchain technology can be categorized into two main types. The first type is the proof-based consensus protocols which are based on certain computations, and are often used in permission-less Blockchains [11]. The most famous proof-based consensus protocol is Proof-of-Work (PoW) used in Bitcoin. The second type is the vote-based consensus protocols which are based on certain communications. and are often used in permissioned Blockchains. A common example of vote-based consensus is offered by the Byzantine fault tolerance algorithm.

The use of consensus algorithms can relatively solve the issue of trust in decentralized networks. But the process can be affected by many undesired factors like malicious behaviour of nodes, processing error of nodes, denial of service from nodes, delayed actions from nodes etc. So in the effective working of a distributed network like a Blockchain system the role of the consensus algorithm is vital [6].

C. Byzantine Generals Problem

The method to reach a consensus among the peer nodes of a Blockchain network is considered to be a Byzantine Generals problem. It is based on an old concept where suppose 10 generals from Byzantine want to attack a country. The attack will be successful only if majority of the generals i.e., more than 5 of them attack at the same time. But some of the generals may be traitors, and they won't attack.So reaching a consensus in such an untrustworthy situation will be a challenge. The main reason for a similar scenario in Blockchain networks is that the system is a decentralized [12].

D. Quantum Computing

Cryptography is a very important entity in communication as well as data storage systems. Recent developments made in quantum computing pose a serious threat to cryptography systems. They can provide a huge amount of parallel computing power that can be used to easily break the mathematical foundations of basic cryptography. The security characteristics of Blockchain depend primarily on asymmetric key cryptography and hashing functions [7]. Since Blockchain technology relies on these concepts of cryptography for providing a decentralized and trustful network, it will also be seriously impacted by the advent of quantum computing.

In particular, the consensus model used in Blockchain systems can be compromised by the use of quantum systems [8]. For example, a quantum computer will attack a Bitcoin's hash function SHA256, thereby to attack its PoW consensus model. This can reduce the complexity of the algorithm from O(N) (traditional attack method) to $O(\pi/4\sqrt{10N})$, thereby making it easier to compromise the security of the Blockchain.

E. Post Quantum Cryptography

Post-quantum cryptography is hence the need of the hour. This research area is widely discussed and studied nowadays. Especially NIST calls for proposals of post-quantum public key cryptosystems in a periodic fashion, and it's currently in the second round. There are various initiatives for developing post quantum Blockchains going on as well [3].

Post-quantum cryptosystems can be broadly classified as shown in Fig 2:

Code-based systems means they make use of error correction codes like McEliece's system or low-density parity check

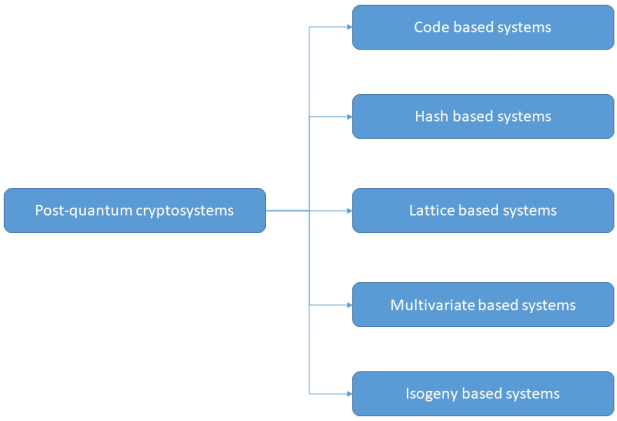

Fig. 2. Classification of post quantum systems

codes(LDPC), quasi-cyclic low rank parity check codes(QC-LRPC) etc to achieve quantum resistance. Hash-based systems make use of the security of the hash functions employed like one-way functions, Merkle scheme etc for quantum safeness. Lattice-based systems make use of lattices and hardness of lattice based problems like Shortest Vector Problem(SVP), Closest Vector Problem(CVP) etc. Multivariate-based systems solve a given system of multivariate equations like MQ problem to achieve quantum resistance. Isogeny-based systems are based on the isogeny protocol for ordinary elliptic curves. There is also a Hybrid-based system which combines pre-quantum and post-quantum cryptosystems but is not popular much.

These post-quantum cryptography systems can be used to enhance the security of existing Blockchain networks by either modifying the working of consensus algorithms or the signing algorithms [9]. The steps to modify the working are shown in Fig 3.

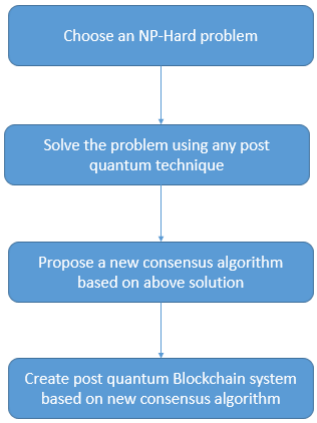

Fig. 3. Workflow of post quantum systems

Initially we need to choose an NP-Hard problem which is difficult to solve in polynomial time. Then solve that problem using either of the post-quantum techniques like for example multivariate quadratic equations. Based on the solution that we get, modify an existing consensus algorithm like PoW or propose a new consensus technique. Based on this new consensus algorithm, a Blockchain system can be built, which will be thus a post-quantum Blockchain system. [10]

In the next section, a review of some of the modified consensus algorithms used in Blockchain systems is done. The algorithms are classified based on the post-quantum technique that they have incorporated.

III. Quantum Safe Consensus Algorithms in Blockchains

A. An Efficient Blockchain Consensus Algorithm Based on Post-Quantum Threshold Signature

In this paper [13], to build a quantum safe consensus algorithm they have first created a threshold signature scheme based on an NP-hard problem. The problem is to solve quadratic equations in a finite field. The signature generated using this method will be used in implementing the consensus algorithm, thereby making the Blockchain itself quantum safe. The process for reaching a consensus in this paper includes different steps like the election of a leader node, generation of a new block, data validation, and updating of the chain. A consensus is reached in this new method if more than one and a half nodes sign the new block generated based on the post-quantum threshold signature. The security and efficiency of the threshold signature-based Blockchain is higher compared to the traditional Blockchain which is based on RSA and Elliptic curve systems.

B. On the Construction of a Post Quantum Blockchain for Smart City

In this paper [14], a post-quantum consensus algorithm is proposed to make the Blockchain quantum safe. They have replaced the SHA256 hashing scheme used in the traditional consensus algorithm with an NP-Hard problem. It also employs a dynamic DAA (Difficulty Adjustment Algorithm) compared to original consensus schemes so that the difficulty of computations will change dynamically for blocks rather than in a fixed pattern. All these not only ensure quantum safeness but also supports memory mining. To create lightweight transactions in this system, an identity-based post-quantum signature is inserted into a transaction process. The consensus algorithm introduces the problem of solving Multivariate Quadratic Equations (QE), which is an NP-hard problem. A system of multivariate quadratic equations with m equations in n variables over a finite field Fq is used here.

C. A New Proof of Work for Blockchain Based on Random Multivariate Quadratic Equations

In this paper [15], a modified consensus algorithm is proposed, which is based on solving a set of random multivariate quadratic equations over GF(2). For this they have used a NP-hard problem called the MQ problem. Initially there are a system of m quadratic polynomial equations in several

variables over a finite field F. When a block is to be mined a node first calculates multiple hash values using an equation and assigns each hash to the coefficients of the multivariate polynomials and dump excess ones. The mining task will then find a vector which is random in nature and proceed with the consensus scheme. This modified consensus algorithm achieves properties like intrinsic hardness property, solution public verifiability property, homogeneous hardness property, difficulty adjustability property etc all of which are achieved due to the NP-Hardness of the random MQ problem used. In Table I a comparison of the three multivariate based quantum safe consensus algorithms is done.

D. GSCS: General Secure Consensus Scheme for Decentralized Blockchain Systems

In this paper [16], an improved consensus mechanism called GSCS is proposed. It implements techniques like serial mining puzzle (SMP) and mining credibility system (MCS) to resist quantum attacks. Since the consensus algorithm thus developed is quantum safe , the Blockchain implemented using the same will also be quantum safe. SMP is a novel mining puzzle technique that can resist resource coalition i.e, prevent usage of mining pools. It also prevents outsourced mining and parallel mining i.e., mining power cannot be taken from multiple CPUs. MCS is introduced into GSCS to prevent the involvement of any bogus participants. The entire sequence of participants mining actions is indirectly recorded in a Blockchain, which reflects each participant's actual credibility. MCS then evaluates the mining actions and quantifies the credibility-based mining difficulty.

E. Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem

In this paper [17], an asymmetric consensus mechanism based on a computationally hard problem is used. It works on the concept that generation of the 'proof' is made difficult or memory intensive, and verification of the 'proof' is made easier. This is done so as to achieve ASIC (Application Specific Integrated Circuit) resistance. The generalized birthday problem or k-XOR problem, which searches for a set of n-bit strings that XOR to zero is used here. The strings are generated using a PRNG function, like a hash function in counter mode. Algorithm binding method is used to prevent cost amortization and to prove that parallel implementations are restricted by memory bandwidth.

F. Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic

In this paper [18], a new consensus algorithm has been proposed which combines an unconditionally secure signature (USS) scheme and the YAC (Yet Another Consensus) algorithm. USS are used to overcome the quantum threat by using hashing techniques to create the signatures. YAC is a vote-based consensus protocol unlike PoW which is a proof-based one. The modified consensus protocol is named as QSYAC (Quantum Secured YAC). The basic construction of the protocol is as follows: The Toeplitz hash message authentication code is used as the base of the USS scheme, and a signature is created. The keys and strings used in the signature scheme are exchanged using a Quantum Key Distribution (QKD) mechanism, which makes the overall method quantum safe. This new signature called TGS (Toeplitz Group Signature) created, replaces the public key signature used in original YAC and thus QSYAC protocol is created.

G. Lattice Based Proof of Work for Post Quantum Blockchains

In this paper [19], a new consensus algorithm is proposed using lattice systems called the LPoW (Lattice-PoW) and it is based on solving the Hermite-SVP (Shortest Vector Problem) in the Euclidean norm to a small approximation factor which is an NP-Hard problem. The main aim of the authors here; was to make the conventional hash-based PoW quantum safe by using the lattice problem which is hard to solve but easy to verify. The solution to the problem used here is achieved using different algorithms and they have used heuristic lattice sieves which have the best quantum complexity. The parameters of LPoW are easily fine-tunable to adjust the difficulty factor for example, increasing the dimension of the lattice affects the computational resources required to solve the consensus algorithm. So higher the dimension more difficult to solve.

H. ECCPoW: Error Correction Code based Proof-of-Work for ASIC Resistance

In this paper [20], a new consensus protocol Error-Correction Code PoW (ECCPoW) is proposed which combines the low-density parity-check decoder and a hash function. The newly constructed consensus algorithm is applied to Bitcoin. This method mainly tries to resolve the issue of centralization of mining process in Blockchain due to the emergence of ASICs.

IV. Challenges

The main challenge faced by all of the above discussed methods is the proper selection of an NP-Hard problem so that resistance to quantum attacks can be achieved. Other challenges that can occur are memory constraints related to mining, the latency of the transactions, achievement of ASIC resistance etc.

V. Comparison and Evaluation

In this section, a comparative study of the different consensus algorithms is done based on various factors. In Table II a summary of the post-quantum systems and techniques used in different modified consensus algorithms is given. In Table III an overall evaluation of the technical level of different post-quantum consensus algorithms is done. In Fig 4 the usage popularity off different post-quantum cryptosystems to modify consensus algorithms are given. We can see that Isogeny based systems and hybrid systems are not used for modifying consensus algorithms.

TABLE I
COMPARISON OF MULTIVARIATE SCHEMES

Techniques	Generation of coefficients	No: of Variables	Solution technique
Threshold signature [13]	Unbalanced Vinegar & Oil scheme	m,n and n=2m	Gauss Jordan elimination
Multivariate quadratic equations [14]	PRNG & SHA-256	m,n and n=m	Grobner basis algorithm
MQ problem [15]	SHA-256 or SHA-512	m,n and n=m+8	Hash function

TABLE II
COMPARISON OF QUANTUM SAFE CONSENSUS METHODS

New Consensus algorithm	Post quantum system	Technique used	Blockchain	Modification of
Yi et al. [13]	Multivariate based	Threshold signature	Yes	PoW
Chen et al. [14]	Multivariate based	Multivariate quadratic equations	Yes	PoW
Ding et al. [15]	Multivariate based	MQ problem	Yes	PoW
Wang et al. [16]	Hash based	SMP & MCS	Yes	PoW
Biryukov et al. [17]	Hash based	Generalised Birthday Problem	No	PoW
Sun et al. [18]	Hash based	Toeplitz Signature	Yes	BFT
Behnia et al. [19]	Lattice based	Hermite SVP Problem	Yes	PoW
Jung et al. [20]	Code based	Low Density Parity Check Decoder	Yes	PoW

TABLE III
EVALUATION OF QUANTUM SAFE CONSENSUS ALGORITHMS

New Consensus algorithm	Consistency	Security	Scalability	Efficiency	Resources used	Quantum resistant
Yi et al [13]	Yes	Yes	Same as PoW	Moderate	Moderate	Yes
Chen et al. [14]	Yes	Yes	Same as PoW	High	Moderate	Yes
Ding et al. [15]	Yes	Yes	Same as PoW	High	Moderate	Yes
Wang et al. [16]	Yes	Yes	Same as PoW	Moderate	Moderate	Yes
Biryukov et al. [17]	Yes	Yes	Same as PoW	Moderate	High	No
Sun et al. [18]	Yes	Yes	Same as BFT	Moderate	Moderate	Yes
Behnia et al. [19]	Yes	Yes	Same as PoW	High	Low	Yes
Jung et al. [20]	Yes	Yes	Same as PoW	Moderate	Moderate	No

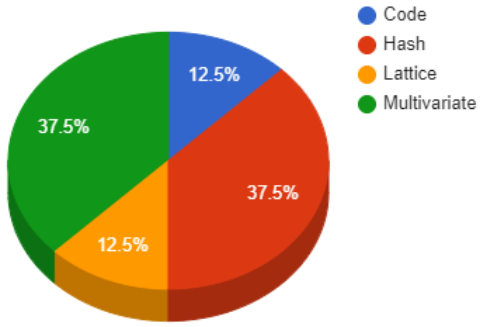

Fig. 4. Popularity of consensus using post quantum systems

VI. CONCLUSION

Blockchain is an upcoming technology and is used in many applications. The consensus mechanism used in Blockchain is closely associated with its application scenario as well. The consistency and security of consensus algorithms have to be ensured in the upcoming quantum computing era. A review of different quantum-safe consensus algorithms is conducted here so that the best method can be chosen to create quantum-safe Blockchains. We can make a common observation that almost all have tried to modify the PoW algorithm. Based on the analysis study we can conclude that almost all schemes are good candidates out of which lattice schemes are more suitable for developing post quantum consensus algorithms, as they have the advantage of using fewer resources and ensure better performance. Other features like security, scalability and consistency are ensured in almost all schemes. Similar to consensus algorithms, another way to make Blockchain systems quantum resistant is to use quantum-safe digital signatures. Studies have shown that lattice schemes can be used to develop post quantum signature schemes as well, which have reduced key size compared to other methods and thus may also be incorporated into Blockchain systems.

REFERENCES

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. SSRN Electronic Journal [Internet]. 2008; doi:10.2139/ssrn.3977007
[2] Sanka AI, Irfan M, Huang I, Cheung RCC. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. Computer Communications [Internet]. 2021 Mar;169:179–201. doi:10.1016/j.comcom.2020.12.028
[3] Bernstein DJ, Lange T. Post-quantum cryptography. Nature [Internet]. 2017 Sep;549(7671):188–94. doi:10.1038/nature23461
[4] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo K-KR. A systematic literature review of blockchain cyber security. Digital Communications and Networks [Internet]. 2020 May;6(2):147–56. doi:10.1016/j.dcan.2019.01.005
[5] Bhutta MNM, Khwaja AA, Nadeem A, Ahmad HF, Khan MK, Hanif MA, et al. A Survey on Blockchain Technology: Evolution, Architecture and Security. IEEE Access [Internet]. 2021;9:61048–73. doi:10.1109/access.2021.3072849
[6] Belotti M, Bozic N, Pujolle G, Secci S. A Vademecum on Blockchain Technologies: When, Which, and How. IEEE Communications Surveys; Tutorials [Internet]. 2019;21(4):3796–838. doi:10.1109/comst.2019.2928178

[7] Tamil Selvi K, Thamilselvan R. Post-Quantum Cryptosystems for Blockchain. Quantum Blockchain [Internet]. 2022 Jul 15;173–200. doi: 10.1002/9781119836728.ch7
[8] Kearney JJ, Perez-Delgado CA. Vulnerability of blockchain technologies to quantum attacks. Array [Internet]. 2021 Jul;10:100065. doi:10.1016/j.array.2021.100065
[9] Fernandez-Carames TM, Fraga-Lamas P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access [Internet]. 2020;8:21091–116. doi:10.1109/access.2020.2968985
[10] Dey N, Ghosh M, Chakrabarti A. Quantum Solutions to Possible Challenges of Blockchain Technology. Lecture Notes on Data Engineering and Communications Technologies [Internet]. 2022;249–82. doi:10.1007/978-3-031-04613-1_9
[11] Ferdous MS, Chowdhury MJM, Hoque MA. A survey of consensus algorithms in public blockchain systems for crypto-currencies. Journal of Network and Computer Applications [Internet]. 2021 May;182:103035. doi:10.1016/j.jnca.2021.103035
[12] Zhang C, Wu C, Wang X. Overview of Blockchain Consensus Mechanism. Proceedings of the 2020 2nd International Conference on Big Data Engineering [Internet]. 2020 May 29; doi:10.1145/3404512.3404522
[13] Yi H, Li Y, Wang M, Yan Z, Nie Z. An Efficient Blockchain Consensus Algorithm Based on Post-Quantum Threshold Signature. Big Data Research [Internet]. 2021 Nov;26:100268. doi:10.1016/j.bdr.2021.100268
[14] Chen J, Gan W, Hu M, Chen C-M. On the construction of a post-quantum blockchain for smart city. Journal of Information Security and Applications [Internet]. 2021 May;58:102780. doi:10.1016/j.jisa.2021.102780
[15] Ding J. A New Proof of Work for Blockchain Based on Random Multivariate Quadratic Equations. Applied Cryptography and Network Security Workshops [Internet]. 2019;97–107. doi:10.1007/978-3-030-29729-9_5
[16] Wang J, Ding Y, Xiong NN, Yeh W-C, Wang J. GSCS: General Secure Consensus Scheme for Decentralized Blockchain Systems. IEEE Access [Internet]. 2020;8:125826–48. doi:10.1109/access.2020.3007938
[17] Biryukov A, Khovratovich D. Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. Ledger [Internet]. 2017 Apr 28;2:1–30. doi:10.5195/ledger.2017.48
[18] Sun X, Sopek M, Wang Q, Kulicki P. Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic. Entropy [Internet]. 2019 Sep 12;21(9):887. doi:10.3390/e21090887
[19] Behnia R, Postlethwaite EW, Ozmen MO, Yavuz AA. Lattice-Based Proof-of-Work for Post-Quantum Blockchains. Data Privacy Management, Cryptocurrencies and Blockchain Technology [Internet]. 2022;310–8. doi:10.1007/978-3-030-93944-1_21
[20] Jung H, Lee H-N. ECCPoW: Error-Correction Code based Proof-of-Work for ASIC Resistance. Symmetry [Internet]. 2020 Jun 9;12(6):988. doi:10.3390/sym12060988