International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 4998–5013

Promises and Perilsof Post-Quantum Blockchain

Savita Kumari Sheoran[1], Gayatri[2]
Department of Computer Science & Engineering
Indira Gandhi University Meerpur, Rewari
[1]*savita.sheoran@igu.ac.in*,[2]*gayatri4161@gmail.com*
(*Corresponding author's e-mail:gayatri4161@gmail.com)

Abstract

Recently the Blockchain has predominantly evolved as a powerful technology to address the menaces of privacy, transparency, redundancy and accountability in data transfer over distributed networks. Owing to its weird potential to offer decentralized trust, secure data usage and efficient functioning; it has been successfullydeployed in many critical areas including financial services, e-governance, defence, academics, research, reputation system and smart manufacturing etc. The Blockchain is a special type of distributed ledger which currently relies on hash function and public-key cryptography where information is stored in blocks protected byhash signatures immune toany type of security breaks. Quantum Computing is a recent buzz word encompassing Gover's and Shor's algorithms which promiseto solve the knapsack problems in real time making thefuture of classical key cryptography obsolete. There is an apprehension that Post-Quantum computer will be able to modify the hash signature to compromise the Blockchain security. In such dilemmatic scenario there is an urgent need to develop a Blockchain cryptosystem, resilient towards the potential eavesdropping in Post-Quantum age. This paper aims to explore possibilities of developing such futuristic Post-Quantum information security system along with the promises and perils with regard to the Blockchain technology. A comparative study of public-key Post-Quantum cryptosystem and signing algorithms has been carried to formulate the future research direction in this regime.

Keywords: Blockchain, blockchain security, blockchain cyber security, Post-Quantum cryptosystem.

I. Introduction

Blockchain is a special type of Distributed Transaction Ledgers (DTLs) that was initially developed with cryptocurrency named as Bitcoin [1]. This buzzing technology owes bizarrepropertiessuch as dataprivacy, transparency, decentralization, persistency, anonymity, audit-ability and attack resilienceaverringit a key technology for diverse applications such as e-governance, smart transactions, logistics, online voting, online trading or smart factoriesetc [2].Blockchain store information in data blocks distributed over a network which allow trusted interaction between users through public-key cryptography. The digital signatures generated using the hash function verify the genuineness of user and provides a link for subsequent data blocks in the blockchain. This process is accomplished in two phases *viz.* signing phase and verification phase keeping a unique private key and a public key, where private key is secured secretly while public key is distributed in the blockchain network. In the signing phase users own private key to encrypt the data and sendit to receiver node. The signing algorithm is robust and secure which generate the digital signature using private key of the user. Every blockchain user is associated with a wallet which store private key to generate hash signature [3-4].In verification phase public key of sender is used to validate the signature.Public distributed transaction ledger keepsall the new committed transaction in the blocks and every new committed transaction are appended with previous block. Hash functions generate user address or shorten the size of the public address using SHA-256 and Scrypt algorithm to avoid the forge [5]. Every transaction among the blocks bears a time stamp and hash value link all in chronological order. Every block in the blockchain contains a special minor node to calculate the hash value of its predecessor block in the link. The entry in the blocks are immutable, therefore,any transaction can't be removed, tamperedor tracked back in the present blocks. This astonishing property makes Blockchain most suitable for applications wheremutual trust and honesty is of utmost priority [6].

Bitcoin initially developed by Satoshi Nakamoto in 2009 was the first practical application of Blockchain. It has now surpassed four generations spanning from simple record of financial transactions to smart contacts followed cloud based services and present day smart manufacturing. On the other hand Quantum Computing is newly emerged technology which posses enormous computing capabilities.The Quantum Computers are represented by quantum bits called qubits. It significantly differs from the traditional computer systems in the sense that in contrary to binary system where there can be either 0 or 1 state quantum system may have both 0 and 1 states together. One way quantum computers, gate array quantum computers, topological quantum computers and adiabatic quantum computers are the near commercial varieties of Quantum Computers developed so far. With the development of 'Q System One' by IBM and announcement of Computer Supremacy by Google these efficient and ultra-high processing computers have become a reality.Presently Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Diffie-Hellman (ECDH) Algorithm and Rivest–Shamir–Adleman (RSA) Algorithm are the most popular asymmetric cryptographic algorithms which can't be solved in polynomial time[4][5]. The Quantum Computers operating on the principles of Quantum Physics to perform operation on the data aiming to solve the knapsack or NP hard problem can do this task within polynomial time using Shor's and Grover's algorithms.It offers a new kind of security threat to Blockchain which forces to develop a new public-key cryptosystem and digital signature algorithm that can resist against Quantum Computing. This paper analyzes the development of public key cryptosystem and signing algorithms that can resist quantum attacks and will review the currently developed Post-Quantum cryptography algorithm. This paper will theoretically study this issue and enlist the promises and perils of the most relevant quantum safe cryptosystems. The subsequent section II will deal with theexisting Blockchain. Section III will analyse the most relevant Post-Quantum cryptosystems and will put forward a comparative testimony of it. The section IV will present performance analysis of the Post-Quantum cryptosystem reviewed in this research. The section V will conclude the paper and present the future direction of research in the area under study.

II. Key Concepts in Blockchain

(A) Blockchain Structure

Blockchain stores information about the details of transactions as well as event logs carried out by users. Every transaction in the blockchain is secured, verified and it cannot be removed or backtracked. All the blocks of the blockchain are linked with one another and form a long sequential chain of linked block. Each block stores the hash value of its previous block. Figure1 shows the structure of Blockchain with a sequential link of blocks which contains the complete committed transactions information assuming 'K+1' blocks in blockchain. In the example block 'K-1', 'K' and 'K+1'respectively contains 622F, 727J and 867K hash value.

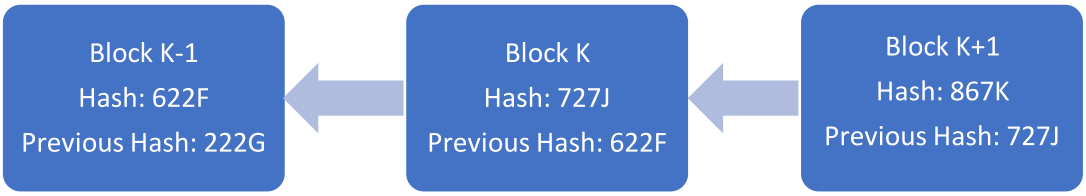


Fig 1: Blockchain Consisting of Continuous Sequence of Blocks

The figure 2 further explains the detail description of the data block presented in figure 1. Each data block of blockchain contains two separate parts in which the first part is Block Header and second part is Transaction Counter. The Block Header contains the information about the Hash value of previous block, Nonce, Number of bits, Timestamp, Markle tree root hash and Block version. The second part of the blockchain stores the transaction data that is in the form of Merkle tree in the current network [8].

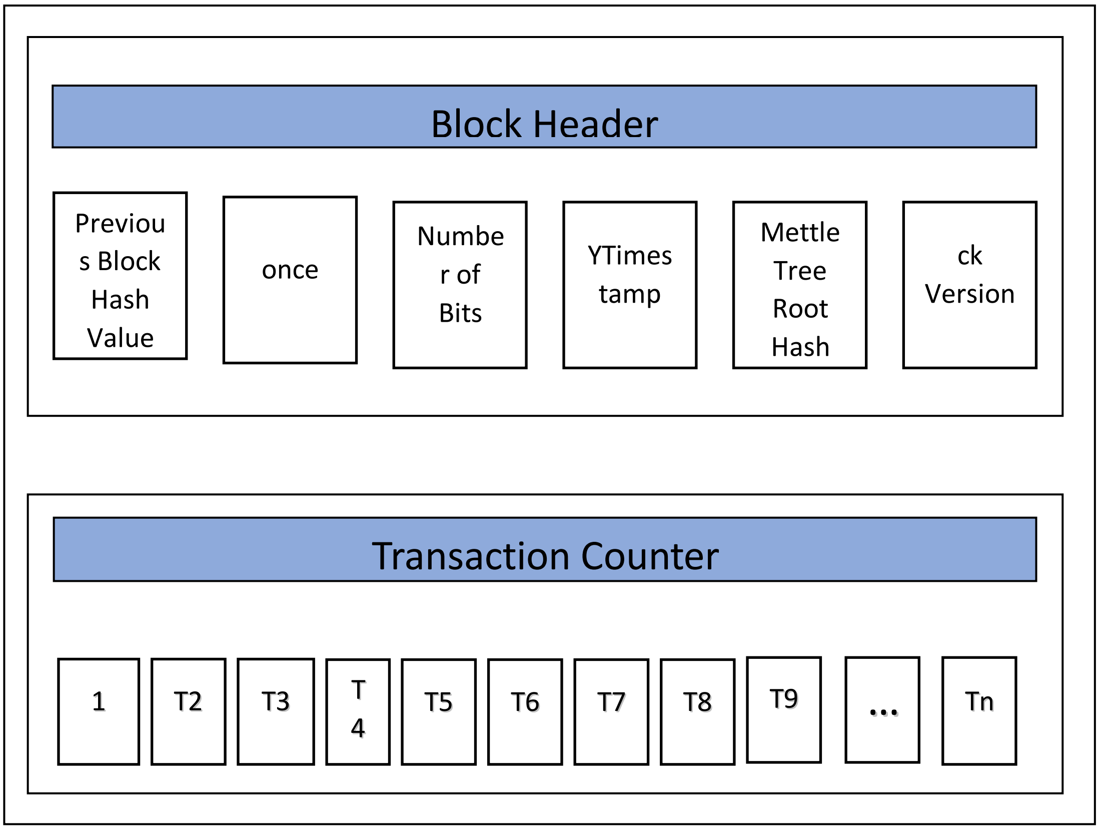


Figure 2: Block Structure in Blockchain

The detailed properties and definitions of variouscomponents ofBlock Header and Transaction Counter are described below:

Block Version: It defines the set of rules which is followed by every block and validates it.
Merkle Tree Root Hash: Every block contains a set of transactions therefore it will help to store the current node as per the type of block and will contain the hash value of the previous block.
Timestamp value: Every transaction has a time stamp. It contains current time of the committed transaction.
Number of bits: Threshold of the block hash that is valid.
Nonce: It is 4-byte filed. The value of nonce starts with 0 and it increase when any hash value is calculated.
Previous block hash value: Each block has a unique hash value. Each block contains the hash value of its predecessor block in the block link.
TX: It contains the detail about the transaction perform by the user.

The transaction counter and data of the transaction is stored in block body. The total number of transaction dependsupon the size of block. Any transaction stored in the block cannot be altered, updated, or removed. The Blockchain has a computational node which is different from the regular nodes and used to perform operations on the nodes such as validation by consensus protocol.

(B) Blockchain Operations

Theblockchain network is decentralized, and each user's is authenticating judged by the address generated by the private key of the user [9]. For instance, while transferring money to the user Y, the user X mandatorily have to sign in using private key. Only after matching the signature, money can be transacted. Figure 3 enunciates the financial transaction through signature verification process.

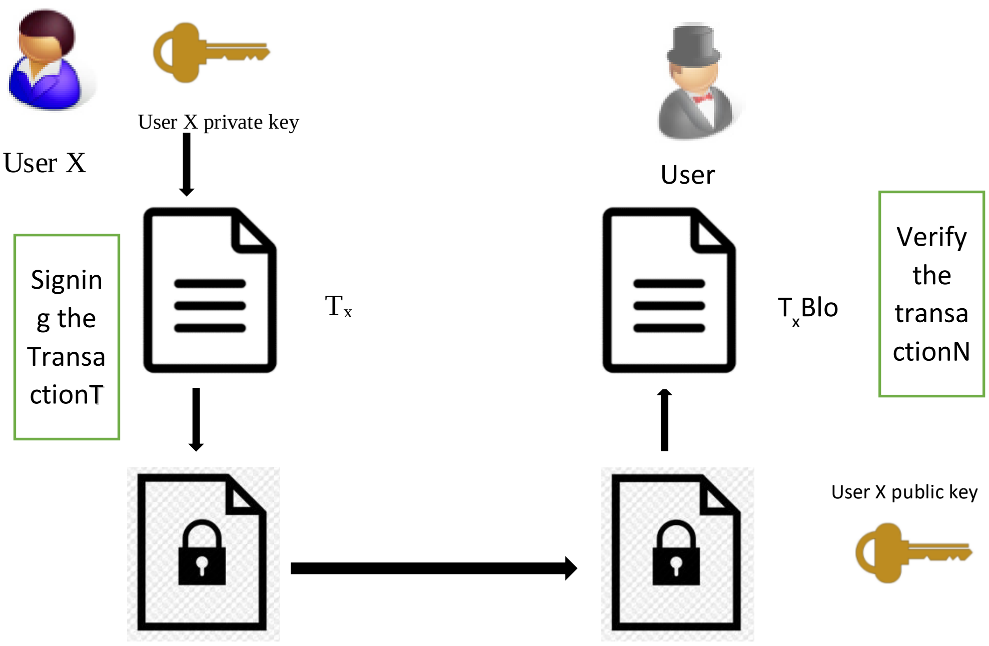


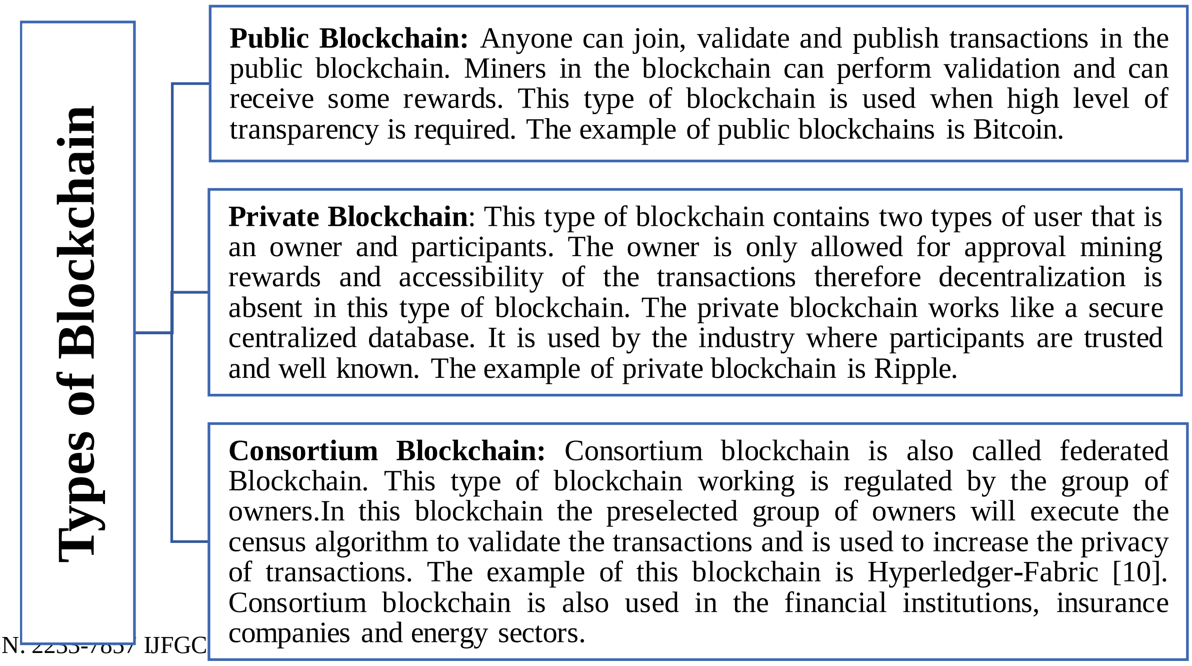
Figure 3: Transaction Verification in Blockchain

The complete process of transaction among users through signature validation is accomplished through following steps:

(a) Firstly the receiver will scan the transaction for validity. It will only accept the valid transactions and may reject the invalidones.
(b) Secondly receiver will check the quantum of amount as per quotation in the delivery address. The transaction with insufficient funds shall be rejected.
(c) Subsequently all valid transactions with sufficient funds shall be credited and debited to the sender and user account respectively.

(C) Types of Blockchain

The Blockchain are generally classified based on the user interaction and data management. Broadly there can be three types of Blockchain *viz.* Public Blockchain, Private Blockchain and Consortium Blockchain. Apart from it, Hybrid Blockchain which is combination of public and private Blockchain, is generally used in many applications. Three basic types of Blockchain are as givenin figure 4 below [10].



Types of Blockchain

Public Blockchain: Anyone can join, validate and publish transactions in the public blockchain. Miners in the blockchain can perform validation and can receive some rewards. This type of blockchain is used when high level of transparency is required. The example of public blockchains is Bitcoin.

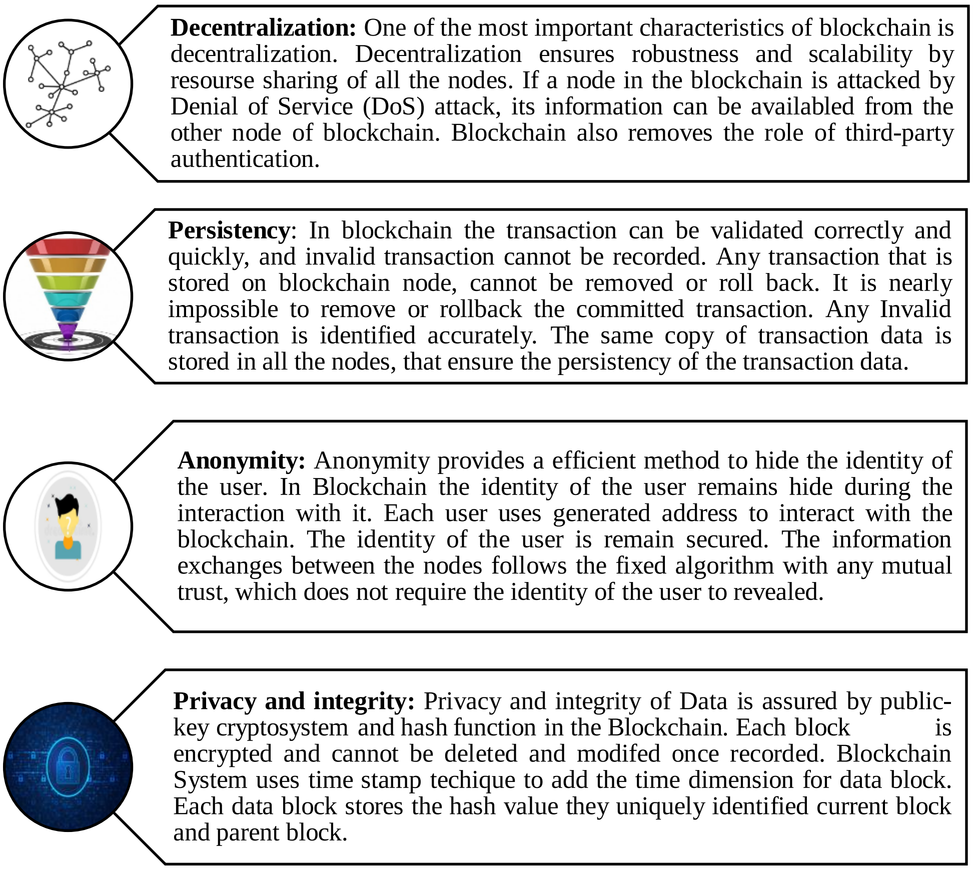
Private Blockchain: This type of blockchain contains two types of user that is an owner and participants. The owner is only allowed for approval mining rewards and accessibility of the transactions therefore decentralization is absent in this type of blockchain. The private blockchain works like a secure centralized database. It is used by the industry where participants are trusted and well known. The example of private blockchain is Ripple.

Consortium Blockchain: Consortium blockchain is also called federated Blockchain. This type of blockchain working is regulated by the group of owners.In this blockchain the preselected group of owners will execute the census algorithm to validate the transactions and is used to increase the privacy of transactions. The example of this blockchain is Hyperledger-Fabric [10]. Consortium blockchain is also used in the financial institutions, insurance companies and energy sectors.

Figure 4: Types of Blockchain

(D) Characteristics of Blockchain

Blockchain posses astonishing feature which make it unique in its applications. Figure 5 represent the main characteristics of Blockchain [13]:



Decentralization: One of the most important characteristics of blockchain is decentralization. Decentralization ensures robustness and scalability by resourse sharing of all the nodes. If a node in the blockchain is attacked by Denial of Service (DoS) attack, its information can be availabled from the other node of blockchain. Blockchain also removes the role of third-party authentication.

Persistency: In blockchain the transaction can be validated correctly and quickly, and invalid transaction cannot be recorded. Any transaction that is stored on blockchain node, cannot be removed or roll back. It is nearly impossible to remove or rollback the committed transaction. Any Invalid transaction is identified accurately. The same copy of transaction data is stored in all the nodes, that ensure the persistency of the transaction data.

Anonymity: Anonymity provides a efficient method to hide the identity of the user. In Blockchain the identity of the user remains hide during the interaction with it. Each user uses generated address to interact with the blockchain. The identity of the user is remain secured. The information exchanges between the nodes follows the fixed algorithm with any mutual trust, which does not require the identity of the user to revealed.

Privacy and integrity: Privacy and integrity of Data is assured by public-key cryptosystem and hash function in the Blockchain. Each block is encrypted and cannot be deleted and modifed once recorded. Blockchain System uses time stamp techique to add the time dimension for data block. Each data block stores the hash value they uniquely identified current block and parent block.

Fig 5: Key Characteristics of the Blockchain

(E) Application Areas

Although first Blockchain application emerge in the form of cryptocurrency, however, within short span of its existence it have spill over many applications domains including insurance, land acquisition, online voting, commodity trading etc. The unique characteristics of the blockchain provide a ground for the new type of business model and handling of transactions [11]. It can improve theperformance of many sector such as banking, finance, e-Governance, healthcare, etc. [12]. The blockchainintegrated with disruptive areas like IoT, AI, Big Data and Industry 4.0 make the industry arrive at a new horizon. Some othermajor application areas of the Blockchain are listed below:

(i) **Land Records, Registration or Ownership [12]**: Land records and registration involves variety entities such as departments, people and third party. With the hike in event of corruption and bribes the land registration and ownership transferhas become a very herculean task. Citizens are suffering of issues pertaining fraud, proxy, tedious process of registration and bribe etc. To overcome the challenges of the land registration, blockchain can be used in the process of authentication of land records and land registration. The Blockchain provide platform where user can upload documents and genuineness of subsequent buyers and seller can be verified without any extra cost.

(ii) **Healthcare [12]**: Blockchain can be used in healthcareto maintain the record of medicine, vaccinations, patients and medical facilities. Today whole world is facing three types of difficulties. The first problematic area is that due to lack of proper database management of the healthcarefake medical certificates which cause a problem before law enforcement agencies. Further misuse of government health care schemes by non-genuine beneficiaries and leftover of appropriate targeted population is a serious problem faced by healthcare sector. Due to non maintenance of extractable database to records of life saving medicine, medical facilities and equipment purchase and selling, stock of vaccination and patients record the scared medical facilities are not used to their full potentials. Another major difficulty is faced by insurance companies while reimbursing the medical bills. These types of problem can be solved by implementing Blockchain system into the healthcare sectorpatient can have easy access to their medical report and healthcare practitioners can have easy track to patient records.

(iii) **Voting [12]:** The use of Blockchainin voting can increase the security and can reduce the potential risk of fraud documentation. In the blockchain network the records of all votes and voters can be verified and reviewed easily. The election administration, voters and candidates will be the acting node of the Blockchain and the voters will use his private key to cast vote.

(iv) **Banking System [12]:** Blockchain technology and Banking system are close to each other. Banking sector higher prone to security and fraud activities and hence require extra-ordinary security. Many countries have implemented Blockchain based customer validation system. It is a distributed ledger system in which transaction can be maintained easily with proper hash value so that all parties can verify and review it. Blockchain technology can also be applied in KYC process, digital baking and online trade and it can speed up the baking process and reduce cost and with bank frauds.

(v) **Supply Chain [12]:**Supply chain management is the innovative area where Blockchain has makes a remarkable entry. Blockchain network can be used in the supply chain to remove the manual works and speeding up the process of raw material, goods and capital. It can be implemented in the supply chain to develop more transparent and accurate end-to-end monitoring and tracking in the supply chain. In the view of this any organization can digitalize the supply chain and create a decentralized persistent record of all the transaction which helps the organization to track assets from inventory to delivery. Blockchain can keep records of all entities of the supply chain to verify the real time records. The blockchain provide increased transparency to the supply chain and this transparency helps in reducing fraud for high values goods.

Apart from it Blockchain is used in various areas where trust and security are required.

III. Literature Review

The Blockchain is still in a naïve stage and not much literature is available in this area. Further its application in Post-Quantum regime is still not explored properly. This section is dedicated to carry out literature review on present status Blockchain and Post-Quantum cryptosystem that is required to handle the promises and perils of such a disruptive technology. Separated review is carried out for public key Post-Quantum cryptosystems and Post-Quantum signing algorithms. For the purpose of literature review the Post-Quantum schemes are categorised as shown in figure 6 below [1-28].

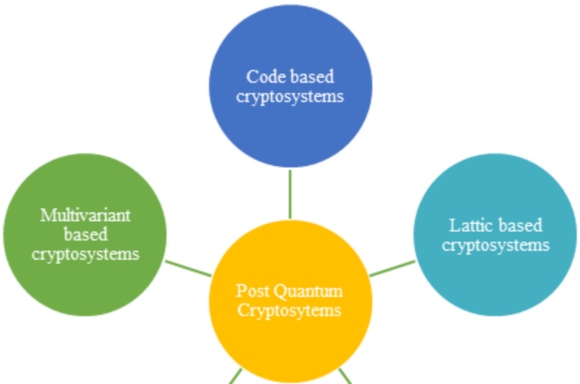

Code based cryptosystems
Multivariant based cryptosystems
Lattic based cryptosystems
Post Quantum Cryptosytems

Figure 6: Classification of Post-Quantum Schemes for Literature Review

(A) Post-Quantum Public-Key Cryptosystem

(i) Multivariate Based Cryptosystems

The multivariate-based cryptosystems system use square matrices which are based on random polynomials equations. The security of this system is based on complexity of multivariate equation which is demonstrated by the NP-Complete and NP-Hard problems [14] which can depend upon the Hidden Field Equations (HFE) and Matsumoto-Imai’s Algorithm (MIA) [15]. The multivariate-based cryptosystems system has two limitations. The first limitation is large key size and another one is Cipher Textoverhead problem [16].

(ii) Lattice Based Cryptosystems

Such systems depends on the lattice which is having set of values in the K-dimensional spaces with periodic structure. The security of the lattice-based cryptosystem depends on the presumed computational hardness of the lattice that have many problems such as Shortest Vector Problem (SVP), Closet Vector Problem (CVP) or Shortest Independent Vector Problem (SIVP). These all are the NP-Hard problems. It is observed that lattice-based cryptosystem is used to speed up the usertransaction and simple in computation.The lattice-based cryptosystem is also having the limitation such as large keys and also involves large chipper text overheads. Some of the popular lattice-based schemes are NewHope [17], NTRU [18], LAC-192 [19], FrodoKEM [20], CRYSTALSKyber [21] and SABER KEM [22]. These lattice-based schemes are based on lattice-based problems such as Learning with Errors (LWE), Polynomial algebra, Ring-LWE and Linder-Peikert LWE (LP-LWE) [23].

(iii) Code Based Cryptosystems

McEliece’s cryptosystem [14] is based on the codebased cryptosystem which support error correction codes. It is fast in encryption and decryption and alsoprovides the advancement. But there are many limitationsof this cryptosystem such as it uses large size of matrices in the encryption or decryption and require space in megabytes. Therefore, it cannot be used in resource constrained devices. To overcome this problem there is need to develop a matrix compression technique. Different codes are used in matrix compression techniques such as Quasi-Cyclic Low-Rank Parity-Check codes (QC-LRPC) [24], Density Parity-Check (LDPC) [25] codes, and specific coding techniques [26]. The NTS-KEM [19] based on McEliece, ROLLO-II [25] based on rank matrix codes with LRPC codes, RQC [27] based on rank Quasi-cyclic codes and HQC [27] based on Quasi-Cyclic and BCH codes are the most popular code-based cryptosystems used in Blockchain cryptography.

(iv) Super-singular Elliptic Curve Isogeny Cryptosystems

Such systemsuse isogeny protocol can stand against quantum attacks and hence uses key sizes are in order of kilobytes [28]. Thelarge key sizes and computational complexity are the main limitations of this system. SIKE [29] is an isogeny-based cryptosystem with128-bit level of security.

(v) Hybrid Based Cryptosystems

Thistype of cryptosystems merges the Pre-Quantum cryptosystems and Post-Quantum cryptosystems [30]. It mayprovide security against quantum attacks. This scheme involves the merger of two complex cryptosystem which may increase computational complexity and causes more energy consumption. An example of hybrid cryptosystem is New Hope cryptosystem merged with X25519 [31]. The CECPQ2 is another hybrid scheme which merge X25519 with HRSS and SXY [30].

The security level, size of private key and size of public key of various Post-Quantum cryptosystem mentioned above are shown in table

Table 1: Security Level, Size of Private and Public keys in Post-Quantum Cryptosystems

Post-Quantum Cryptosystem	Type	Public key (size in bytes)	Private key (size in bits)	Security Level (bits)
NewHope	Lattice based	14,592	29,440	256
NTRU	Lattice based	9,840	12,736	368
FrodoKEM	Lattice based	172,160	344,704	256
CRYSTALSKyber	Lattice based	12,544	25,344	256
SABER KEM	Lattice based	10,496	24,320	388
NTSKEM	Code based	11,357,632	159,376	256
LDPC	Code based	14,976	192	128
ROLLO-II-256	Code based	19,944	320	256
RQC-III	Code based	18,272	320	256
HQC level 5	Code based	127,184	256	256
SIKE	Supersingular elliptic curve based	2992	2640	128
Matsumoto-Imai Cryptosystem	Multivariate	-	-	192
HFE	Multivariate	-	-	192

(B) Post-Quantum Singing Algorithms

(i) Multivariate Based Cryptosystems

In this cryptosystem, trapdoor function [28] use as a private key to generate public key. In this scheme the generated signature is small in size. Multivariate-based signing algorithms are based on variant of HFE, Isomorphism of Polynomials or Matsumoto-Imai's algorithm. Theses algorithms can generate signature whose size is comparable to most popular signing algorithm RSA or ECDSA. Some the popular post quantum signing algorithms have been proposed which are rely on Rainbow like signing scheme and pseudo random quadratic equations. The limitation is these singing schemes are large key size. This problem has been addressed in MQDSS, but it generates the large size signature.

(ii) Code Based Cryptosystems

Code based cryptosystems in signing algorithms are same as McEliece's cryptosystem. The code-based generate short length signature which can be verify very fast. But the key used to generate short length signature are large in size. In [32], it is observed that identification protocol used in Fiat-Shamir transformation [32] outperforms CFS [32]. It is not an absolute secure against quantum attacks.

(iii) Lattice Based Cryptosystems

Lattice based cryptosystem with Short Integer Solution (SIS) are used to reduce key size. The BLISS-B (Bimodal Lattice Signatures B) [33] is one the best schemes which rely on the hardness of the SIS paired with RSA and ECDSA. However it is evident that BLISS-B was attacked in 2016 by side channel attack. A new variant of BLISS-B is also introduced to strength the security but it was attacked by cache attacks. Researchers also introduced some other lattice based scheme such as Bonsai tree based scheme [34], QChain [35], FALCON [34] and qTESLA-p-I [34]. Lattice based schemes use short key as compared to Multivariate based schemes but the generated signature is of large size.

(iv) Hash-Based Signature Schemes

In this scheme the security depends on the hash function. The presented byBernstein et al involing XMSST and SPHICS provide high level security level hash-based signature scheme fall under this category. But it is observed that these schemes are impractical for blockchain. The XNYSS may be implanted as substitute of XMSST [35]. Adaptability towards the Blockchain is major drawback of this scheme.

Table 2 present the comparative study of various schemes based on Post-Quantum signing algorithms.

Table 2: Security Level, Size of Private and Public keys in Post-Quantum Signature Scheme

Algorithm	Scheme type	Public key (bytes)	Private key (bits)	Signature Size (bits)
FALCON	Lattice-based	14344	20368	10184
qTESLA-p-I	Lattice-based	119040	41472	20736
MQDSS	Multivariate-based	368	128	166832
Rainbow	Multivariate-based	13,967,360	10,051,584	1632
GeMSS	Multivariate-based	24,903,680	614,400	576
SPHINCS+ -SHA-256-128f-simple	Hash-Based	256	512	135,808
SPHINCS+ -SHA-256-256f-simple	Hash-Based	512	1,024	393,728
SPHINCS+-Haraka-256f-simple	Hash-Based	512	1,024	393,728
PICNIC2 L5-FS	Hash-Based	512	256	437,856

(C) Post-Quantum Schemes for Blockchain

Data privacy and security in Blockchain canbe achieved by public-key cryptography [37]. The security level provided by public-key cryptography is estimated through bits of security level as shown in table 3. This security level defines how much effort is required to perform brute force attack by a classical computer. For istance the cost of brute force attack on 80bit security level cryptosystem with classical computing is very high (up to millions of dollars). It observed that current security level of the public-key cryptosystem is enough against classical computing attacks. Further it is observed that public-key cryptosystem like 160bit ECDSA can be successfully broken by the 1200-qubit quantum computers [38]. Same scenario is observed in case of RSA algorithm that can be broken by the 2000-qubit quantum computers. Public-key cryptosystems that rely on discrete logarithm and integer factorization can be affects by the quantum computing attacks.

Table 3: Security level of Popular Cryptosystems [4]

Sr. No.	RSA Key Size (bits)	ECDSA Key Size (bits)	Security level
1	1024	192	80
2	2048	224	112
3	3072	256	128
4	7680	384	192

(D) Quantum Attacks on Blockchain

ECDSA algorithm used in blockchain to randomly generate private key $K_{private}$[39-40]. It select the randomly generated point on the eclipse curve 'X' and multiply it with private key $K_{private}$to calculate the point 'Θ' that is corresponding to public key (K_{public}= $K_{private}$ * X). Public key (K_{public}) can be generated only by the known private key ($K_{private}$). It is unidirectional i.e. private key is used to generate public key but reverse is not possible. ShorAlgorithm is based on quantum computing which can generate the private key of any user by using its public key that is distributed on the network [41]. Now, the attackercan use the private key of the existing user to generate the digital signature of that user in the blockchain and can create the unauthorized transaction in it. Most of the cryptographic algorithm such as Hyperelliptic curves, RSA, ECDSA, DSA and Elliptic curves can be break up the security of blockchain by the quantum computing algorithms[42].

Grover search algorithm is also another quantum computing based algorithm [43]. This algorithm can solve the factorization problem of large number and discrete logarithm calculation in polynomial time. Itmakes the brute force attack possible in the current cryptographic algorithm. This algorithm also reduces the security level of the cryptographic algorithms to make the brute force attack possible. Generally, attackers can use this algorithm through two methods. In first method it will search the hash collision to change the entire transactions of blocks in the Blockchain from this way Quantum Computing can break the security of hash function. Therefore, there is a need to increase the output size of the hash function to provide the high level of security. Secondly it can also be used to undermineintegrity of the blockchain [44]. By this algorithm mining in blocks can be accelerated resulting in speeding up the generation of nonce. The table 4 enunciates the security level of the cryptosystemin the light of quantum attacks. The content and data included in the table are taken from the various research articles included with due citation. The table describes the various security levels calculated in contrast of classical computing attack and quantum computing attack.

Sr. No.	Algorithms	Type	Security level in classical computing (bits)	Security level in quantum computing (bits)
1	SHA-256	Hash function	256	128
2	Ethash (Keccak-256, Keccak-512)	Hash function	256	128
3	Scrypt	Hash function	256	128
4	SHA-3 256 [45]	Hash function	256	128
5	Keccak-384	Hash function	384	192

ISSN: 2233-7857 IJFGCN

6	ECDSA	Signature	128	Broken by Shor
7	AES-256	Symmetric Encryption	256	128
8	AES-128	Symmetric Encryption	128	64
9	RSA-1024	Signature, Encryption	80	Broken by Shor
10	RSA-2048	Signature, Encryption	112	Broken by Shor

(E) Development of Post quantum cryptosystem

The development of a Post-Quantum cryptosystem is not a simple task rather it involves various challenges and limitation which should be taken in due consideration at every stage. Various Post-Quantum cryptosystems are developed to resist quantum attack but mostly they are pooron the ground of in large key size, computation complexity and huge power consumption. To develop an efficient Post-Quantum cryptosystem, small key size, lower computational complexity, small signature and energy efficient are some favorable key concepts. Following are the key concepts to developan efficient Post-Quantum cryptosystem and Post-Quantum hash function:

(i) **Small Key Size**: In Post-Quantum scheme we should use small key sizeto interact with Blockchain using private key and public key which are essentially small. It will reduce the storage required to store private and public key. Recently Blockchain is also used in the IoT setup to meet its security challenges. Small key size has less complex computation hence such Blockchain can be used in space and computation constrained networks.

(ii) **Small Signature and Hash Length:** A blockchain maintain a database that store transaction as well as user signature and hash value of block. So large signature and hash length may increase the size of the Blockchain beyond a tolerable limit. To develop the efficient Post-Quantum cryptosystem, the size of the signature and hash length must be small to reduce the requirement of memory storage.

(iii) **Low Computational Complexity:** Post-Quantum scheme needs to be low computational complex due to limitation of hardware in classical computers. The Post-Quantum cryptosystem needs to be optimized in terms of computational complexity.

(iv) **Fast Execution:** The Post-Quantum cryptosystem is very fast in computation and hence can process large amount of transaction in very short time which help in reducingthe computational complexity.

(v) **Low Energy Consumption:**The blockchain used in IoT networks require energy constrained cryptosystem. Post-Quantum scheme need to be energy constrained. It will make the Blockchain more robust.

(F) Perils in Implementation of Quantum Attack Resistant Blockchain

Followings are major perils in designing and developing a Quantum resilient cryptosystem:

(i) **Transition Overhead form Pre to Post-Quantum**: The transition from Pre to Post Quantum age requires a cost-effective mechanism [46]. Many researchers have proposed strategy with hard fork scheme in which the validity of a block is extended when security of blockchain provided by hash function and digital signature is compromised [47]. Stewart et al have proposed a commit-delay-reveal scheme in which user can move to post quantum from pre quantum blockchain [48]. To reduce the overhead of this transition, a cost effective mechanism must be developed.

(ii) **Large Key and Signature Sizes**: the large key size provides better security against quantum attacks. In [49], it is observed that large key size will produce large signature. It is observed that 128-bit security level required for 2688-bit size public key and 384-bit size private make 120-kbit signature. It is a challenge to store the large size keys and signature in blockchain. Some multivariate based Post-Quantum scheme generates short signature but keys that are used for generation and verification of such signature require large memory space.

(iii) **Slow Key Generation**: It is observed that some post quantum scheme limits the process of signing transaction with the same key. It require to generate new key for signing continuously which slows down the transaction process of Blockchain.

(iv) **Standardization**: Multiple projects and initiation are currently analyzing the post quantum scheme to give a standard. The researcher should keep in mind to follow the standard to avoid broken schemes.

(v) **Hardware Limitations**: Blockchain nodes use classical computing hardware for processing. Hardware computability is another perils for the development of Post-Quantum scheme [50].

(vi) **Large Cipher Text Overhead**: Large cipher text overhead is another impediment in the Blockchain development. It may impact the performance of the blockchain adversely by taking huge process time. This issue must tackle by minimizing the cipher text overhead in post quantum scheme.

(vii) **Computational and Energy Efficiency**: It is observed that Post-Quantum cryptosystems require significant execution time. It also requires large storage and computational resources. To development efficient Post-Quantum cryptography it should be kept minimum.

IV. Results and Discussion

The result analysis is carried out on the basis of data presented in Table 1 and Table 2 for public key cryptosystem quantum signing algorithms respectively The average execution time in computed in milliseconds and whole results are presented in two sections.First section describes the average execution time of Post-Quantum public key cryptosystem and second part describe the average execution time of Post-Quantum signing algorithms.

(i) Public Key Cryptosystem Schemes

The comparative results for Post-Quantum public key cryptosystem are presented in figure 7. It is observed that some of the algorithms are performing well in key generation but not perform wellin encryption and decryption. For example the NewHope is effective in key generation as compared to encapsulation and de-capsulation while poor at the front of execution time of key generation in comparison to CRYSTALSKyber, LDPC and HQC. SABER KEM performs better as compared to other algorithms but the implementation overhead is large as compared to others. It is observed that the execution time is large in SIKE. It is observed that SIKE is the slowest cryptosystem scheme as compared to others. NTSKEM suffers from slow key generation in spite of fast encapsulation and de-capsulation. HFE suffers slow de-capsulation. CRYSTALSKyber performs better in all process.

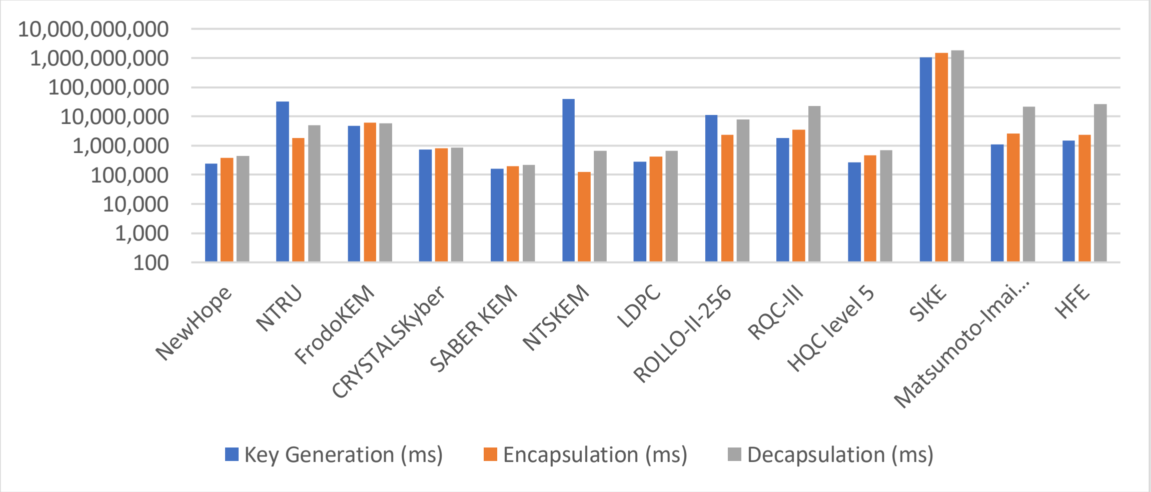


Figure 7: Average Execution Time (ms) of Post-Quantum Public Key Cryptosystem

(ii) Post Quantum Signing schemes

The bar chart of the performance of the Post-Quantum signing algorithm in terms of exertion time in key generation, signing and verification is shown in figure 8. The average execution time is least in FALCON. Rainbow schemes is introduced in signing and verification process but the computational overheard is the limitation of this scheme. PICNICS2 is fast in term of key generation but slowest among all in terms of signing and verification. FALCON, MQDSS, GeMSS, SPHINCS and PICNIC2 are fast in terms of key generation but are slow in signing and verification process, however, it varies with given conditions.

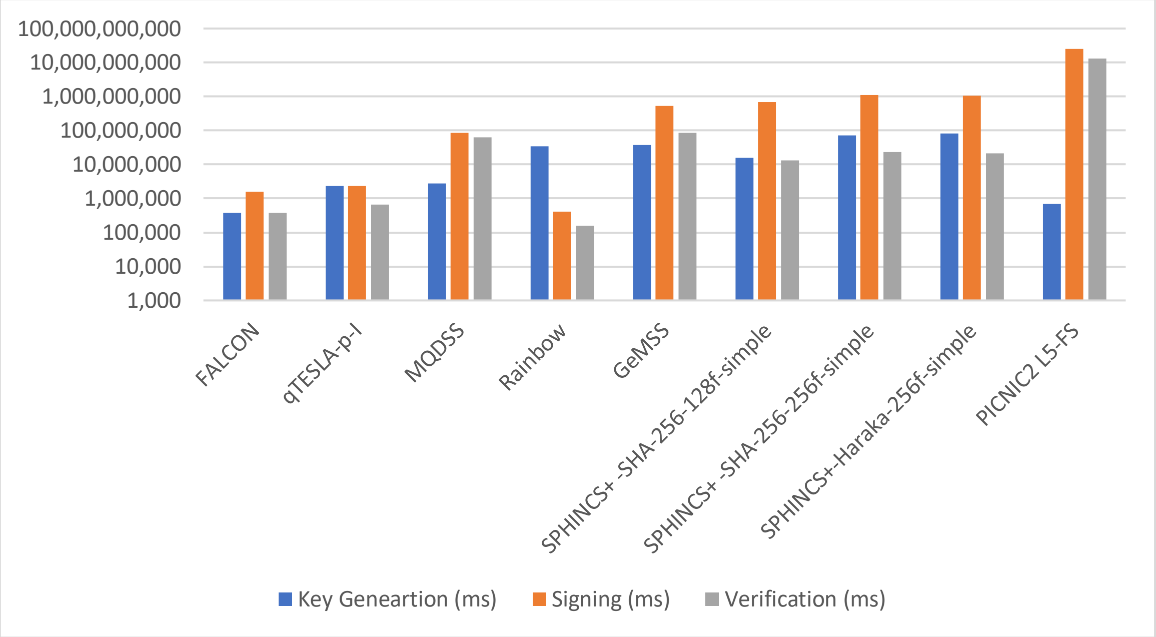


Figure 8: Average Execution Time (ms) in Post-Quantum Signing Cryptosystem

(iii) Key Finding in Result Analysis

On the basis of literature review and result analysis on Blockchain and Post-Quantum cryptosystem this research arrives at following conclusions:

- Post-Quantum cryptosystem are more efficient and Blockchain which could commensurate with such system will sustain in the future.
- There is no single Post-quantum cryptosystem which offerall desired characteristics like small key size, fast key generation, fast signing and verification, short signature sizes, low computational overhead and less energy consumption all together. To develop a universally adoptable Post-Quantum cryptosystem is still a challenge before research community working in this regime of disruptive technologies.
- The recently developed Post-Quantum cryptosystems are not compatible with the existing Blockchain systems. Hardware, computational limitation and implementation cost are the major perils which hinder the direct implementation.
- The code based cryptosystems use large key size hence their implementation is the main overhead while Lattice based schemesprovides most relevant and improved post quantum cryptosystem but the size of key is a main limitation in them. However, compressed key techniques used in lattice-based cryptosystems to increases the employability of this scheme.
- Multivariate based schemes need to be modified on parameters of key size, signing and verification to optimise the large memory size required by them.
- Super singular elliptic curve scheme is required to reduce the signature size. The large keys size and the computational overheard are two main problems in this scheme.

V. Conclusion

This research carried out the literature based theoretical study on the Blockchain and its future in the Post-Quantum age.Various issues, challenges and limitations in development of Post-Quantum cryptosystem are also studied in detail. The paper carried out a broad view of Post-Quantum cryptosystem and signing algorithms which constitute essential ingredients in mitigating quantum attacks fordevelopment of next generation Post-Quantum Blockchain. This study represents the limitations of existing post quantum cryptosystem and key areas where the improvement is required. It is evident from the study that the future of Blockchain is enshrined in Post-Quantum cryptosystem but existing perils in the regime are still hard and need to be mitigated before going ahead. However, this study reaches a conclusive remark on Post-Quantum cryptosystem but more researches need to be carried out through simulation and real time experimentations. As a further study we are planning to implement the these algorithms on suitable test beds to establish more crystal clear evidences for our findings.

References

[1]. B. M. Gupta and S. M. Dhawan, “Blockchain research: A scientometric assessment of global literature during 2010-18,” DESIDOC J. Libr. Inf. Technol., vol. 40, no. 1, pp. 397–405, 2020.

[2]. Q. E. Abbas and J. Sung-Bong, “A Survey of Blockchain and Its Applications,” 1st Int. Conf. Artif. Intell. Inf. Commun. ICAIIC 2019, no. February, pp. 1–3, 2019.

[3]. T. M. Fernandez-Carames 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.

[4]. P. S. Barreto, P. Longa, M. Naehrig, J. E. Ricardini and G. Zanon “Sharper ring-LWE signatures”, Cryptology ePrint Archive, Report 2016/1026, Nov. 2016.

[5]. H. Zhang, F. Zhang, B. Wei, and Y. Du, “Implementing confidential transactions with lattice techniques,” IET Inf. Secur., vol. 14, no. 1, pp. 30–38, 2020.

[6]. W. S. Melo, A. Bessani, N. Neves, A. O. Santin, and L. F. R. C. Carmo, “Using Blockchains to Implement Distributed Measuring Systems,” IEEE Trans. Instrum. Meas., vol. 68, no. 5, pp. 1503–1514, 2019.

[7]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, in Proc. IEEE International Congress on Big Data (BigData Congress), Honolulu, United States, 25-30 June 2017, pp. 557-564.

[8]. G. B. Mermer, E. Zeydan, and Ş. S. Arslan, “An overview of blockchain technologies: Principles, opportunities and challenges,” 26th IEEE Signal Process. Commun. Appl. Conf. SIU 2018, no. May, pp. 1–4, 2018.

[9]. L. Madaan, A. Kumar, and B. Bhushan, “Working principle, application areas and challenges for blockchain technology,” Proc. - 2020 IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2020, pp. 254–259, 2020.

[10]. P. Giungato, R. Rana, A. Tarabella and C. Tricase, “Current trends in sustainability of bitcoins and related blockchain technology”, Sustainability,vol. 9, no. 12, p. 2214, 2017.

[11]. K. Ikeda, Security and Privacy of Blockchain and Quantum Computation, 1st ed., vol. 111. Elsevier Inc., 2018.

[12]. T. M. Fernandez-Carames and P. Fraga-Lamas, “A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories,” IEEE Access, vol. 7, pp. 45201–45218, 2019.

[13]. G. B. Mermer, E. Zeydan, and Ş. S. Arslan, “An overview of blockchain technologies: Principles, opportunities and challenges,” 26th IEEE Signal Process. Commun. Appl. Conf. SIU 2018, no. May, pp. 1–4, 2018.

[14]. D. J. Bernstein, C. Chuengsatiansup, T. Lange, C. van Vredendaal, “NTRU Prime: reducing attack surface at low cost”. In Proceedings of SAC, Ottawa, Canada, Aug. 2017.

[15]. F. Chen, Z. Liu, Y. Long, Z. Liu, N. Ding, “Secure Scheme Against Compromised Hash in Proof-of-Work Blockchain”. In Proceedings of NSS, Hong Kong, China, Aug. 2018.

[16]. R. Shen, H. Xiang, X. Zhang and B. Cai, “Application and Implementation of Multivariate Public Key Cryptosystem in Blockchain”. In Proceedings of Collaborate Com, London, United Kingdom, Aug. 2019.

[17]. E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe, “Post-quantum key exchange - A new hope”. In Proc. USENIX Security Symposium, pp. 327-343, Aug. 2016. [17] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain challenges and opportunities: a survey,” Int. J. Web Grid Serv., vol. 14, no. 4, p. 352, 2018.

[18]. E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe, “Post-quantum key exchange - A new hope”. In Proc. USENIX Security Symposium, pp. 327-343, Aug. 2016.

[19]. NTS-KEM’s documentation for the second round of the NIST Call. Accessed: Aug. 1. 2020. [Online].Available:https://drive.google.com/file/d/1qPsXhK_oXJ88M1ec6pRbvvRKaCMQZfs c/view

[20]. J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe and D. Stehlée, “CRYSTALS – Kyber: a CCA-secure modulelattice- based KEM”. In Proc. IEEE European Symposium on Security andPrivacy, London, United Kingdom, Apr. 2018.

[21]. J.W. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan and D. Stebila “Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE”. In Proceedings of ACM CCS, Vienna, Austria, Oct. 2016.

[22]. J.-P. D’Anvers, A. K. S. S. Roy and F. Vercauteren “Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM”. In Proceedings of Africacrypt, Marrakesh, Morocco, May 2018.

[23]. GeMSS NIST call specification. Accessed: Nov. 2, 2019. [Online]. Available: https://www-polsys.lip6.fr/Links/NIST/GeMSS_specification.pdf.

[24]. ROLLO’s documentation for the second round of the NIST Call. Accessed: Aug. 2, 2020. [Online]. Available: https://pqc-rollo.org/doc/ rollo-specification_2019-04-10.pdf

[25]. H. Jiang, Z. Zhang and Z. Ma, “Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model”. In Proceedings of PQCrypto, Chongqing, China, May 2019.

[26]. M. Baldi, P. Santini and G. Cancellieri, “Post-quantum cryptography based on codes: State of the art and open challenges,” in Proc. AEIT International Annual Conference, Cagliari, Italy, Sep. 2017.

[27]. C. Aguilar-Melchor, O. Blazy, J.-C. Deneuville, P. Gaborit and G. Zémor, “Efficient encryption from random quasi-cyclic codes,” IEEE Transactions on Information Theory, vol. 64, no. 5, pp. 3927-3943, Feb. 2018.

[28]. C. Peng, J. Chen, S. Zeadally, and D. He, “Isogeny-Based Cryptography: A Promising Post-Quantum Technique,” IT Prof., vol. 21, no. 6, pp. 27–32, 2019.

[29]. SIKE’s documentation for the second round of the NIST Call. Accessed: Nov. 2, 2019. [Online]. Available: https://sike.org/files/SIDH-spec.pdf.

[30]. Y. Qassim, M. E. Magana, and A. Yavuz, “Post-quantum hybrid security mechanism for MIMO systems,” 2017 Int. Conf. Comput. Netw. Commun. ICNC 2017, pp. 684–689, 2017.

[31]. I. Stewart, D. Ilie , A. Zamyatin , S. Werner, M. F. Torshizi and W.J. Knottenbelt, “Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack,” Royal Society Open Science, vol. 5, no. 6, June 2018.

[32]. D. Unruh, “Post-quantum security of Fiat-Shamir”. In Proceedings of ASIACRYPT, Hong Kong, China, Nov.-Dec. 2017.

[33]. P. Pessl, L. G. Bruinderink and Y. Yarom, “To BLISS-B or not to be -Attacking strong Swan’s Implementation of Post-Quantum Signatures”,in Proc. ACM SIGSAC Conference on Computer and Communications Security, Dallas, United States, Oct.-Nov. 2017..

[34]. Z. Liu, K. Nguyen, G. Yang and H. Wang, “A Lattice-Based Linkable Ring Signature Supporting Stealth Addresses”. In Proceedings of ESORISCS, Luxembourg, Sep. 2019.

[35]. H. An and K. Kim, “QChain: Quantum-resistant and Decentralized PKI using Blockchain”. In Proceedings of SCIS 2018, Niigata, Japan, Jan. 2018.

[36]. D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P.Schwabe and Z. Wilcox-O’Hearn, “Sphincs: practical stateless hash-based signatures,” in Proc. EUROCRYPT, Sofia, Bulgaria, Apr. 2015.

[37]. K. Ikeda, "Security and Privacy of Blockchain and Quantum Computation," Advances in Computers, vol. 111, pp. 199-228, May 2018

[38]. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, 1997.

[39]. M. Baldi, P. Santini, and G. Cancellieri, "Post-quantum cryptography based on codes: State of the art and open challenges," 2017 AEIT Int. Annu. Conf. Infrastructures Energy ICT Oppor. Foster. Innov. AEIT 2017, vol. 2017-January, pp. 1–6, 2017.

[40]. V. Clupek, L. Malina, and V. Zeman, "Secure digital archiving in post-quantum era," 2015 38th Int. Conf. Telecommun. Signal Process. TSP 2015, pp. 622–626, 2015.

[41]. I. Mustafa et al., "A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications," IEEE Access, vol. 8, pp. 99273–99285, 2020.

[42]. W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," IEEE Access, vol. 6, pp. 5393–5401, 2017.

[43]. F. M. Ablayev, D. A. Bulychkov, D. A. Sapaev and A. V. Vasiliev, "Quantum-Assisted Blockchain," Lobachevskii Journal of Mathematics, vol. 39, no. 7, pp. 957-960, Sep. 2018.

[44]. D. Arora, S. Gautum, H. Gupta, B. B Bhushan, "Blockchain-based Security Solutions to Preserve Data Privacy and Integrity", International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). doi:10.1109/icccis48478.2019.8974503, 2019.

[45]. M. Cherkaoui Semmouni, A. Nitaj and M. Belkasmi, "Bitcoin Security with Post Quantum Cryptography". In Proceedings of NETYS, Marrakech, Morocco, June 2019.

[46]. H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: a survey," Int. J. Web Grid Serv., vol. 14, no. 4, p. 352, 2018.

[47]. M. Sato and S. Matsuo, "Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography," in Proc. International Conference on Computer Communication and Networks, Vancouver,Canada, July-Aug. 2017.

[48]. I. Stewart, D. Ilie , A. Zamyatin , S. Werner, M. F. Torshizi and W.J. Knottenbelt, "Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack," Royal Society Open Science, vol. 5, no. 6, June 2018.

[49]. Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, and V. Soukharev, "A post-quantum digital signature scheme based on supersingular isogenies," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10322 LNCS, pp. 163–181, 2017.

[50]. Y. Xinyi, Z. Yi., "Technical Characteristics and Model of Blockchain" 10th International Conference on Communication Software and Networks, ICCSN 2018 (2018).