Integration of Quantum Computing and Blockchain Technology: A Cryptographic Perspective

Srivastava Tanya, Bhushan Bharat, Bhatt Saurabh, Haque A. K. M. Bahalul

DOI: 10.1007/978-981-19-0924-5_12

Integration of Quantum Computing and Blockchain Technology: A Cryptographic Perspective

Tanya Srivastava

Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, India.

2019622455.tanya@ug.sharda.ac.in

Bharat Bhushan

Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, India.

bharat_bhushan1989@yahoo.com

Saurabh Bhatt

Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, India.

2019002150.saurabh@ug.sharda.ac.in

AKM Bhalul Haque

Software Engineering, LENS, LUT University, Lappeenranta, 53850, Finland

bahalul.haque@lut.fi

Abstract: Blockchain is a computational data structure that provides open and distributed and decentralized public ledger technology that has many promising applications. Blockchain applies block structure linked with each other to store and verify data and provides trust-worthy consensus mechanism for the synchronization of changes in data which results in a tamper-proof digital platform. Blockchain has many approaches for security services which includes integrity assurance, confidentiality, resource provenance and access control list. Blockchain is an emerging technology and believed to be employed in diverse interactive system of the internet. The goal of this paper is to give a detailed overview on the blockchain technology such as its background,

architecture and properties. Further, it describes the quantum level vulnerabilities of different popular blockchains in-use and the different cryptographic concepts that are used in blockchain then it highlights the concept of quantum computing along with blockchain technology. In the end, it gives an insight of pre-quantum to post-quantum blockchain.

1. Introduction

Blockchain is a secured and distributed ledger which is managed by peer-to-peer network that lubricates the process of storing and verifying resources without using any centralized trusted authority. It is considered secure against attackers who compromises the centralized controllers. It was born with the cryptocurrency Bitcoin [1]. In the recent years, blockchain has gained significant attention from the industries and academia. Blockchain provides promising applications in various areas such as Internet-of-Things (IoT), cloud and healthcare [2]. It also provides network security services such as privacy, integrity, confidentiality and authentication [3]. Currently, trusted third parties provide these services. However, implementation of blockchain ensures security guarantee solving traditional security issues. Blockchain maintains a continuous record of data that is validated by all nodes participated in the network [4]. Implementation of blockchain is often usually for cryptocurrencies, distributed ledger system or smart contract, new platforms are also being announced constantly.

Cryptography was introduced to blockchain to make transactions and participants more secure. It ensures only intended user is able to obtain, read and write the transactions. Blockchain implements asymmetric key cryptographic algorithm and hash functions [5]. Generally, SHA-256 hashing algorithm is used in blockchain as the hash function [6]. Hash functions helps in maintaining the integrity of data inside the blocks of blockchain network by generating digital signatures and connecting the blocks in a blockchain [7]. Asymmetric key cryptographic algorithm, also known as Public-key cryptography makes use of key pairs that is public key and private key. Public key is considered as the address of the participant and it is visible to every participant in the network. Private key is kept confidential and is used to access the transactions [8]. Public-key encryption also plays part in digital signature which are used for verifying the authenticity of digital messages. Cryptocurrencies are one of the most significant applications of blockchain [9]. They also make use of public/private key pairs in order to maintain the user address in blockchain.

Technological developments have replaced classical computers with quantum ones. Quantum computing is an exponentially growing technology. It employs the laws of quantum mechanism and solves the problems that classical computer is unable to do [10]. However, Hash functions and public-key cryptosystem are both

threatened by the birth of quantum computers [11]. Quantum computers are able use Shor's algorithm in order to break some popular public-key algorithms in polynomial time [12]. Furthermore, Grover's algorithm can also be used by the quantum computers to accelerate the generation of hashes which can cause the entire blockchain to recreate blocks [13]. Therefore, blockchain is considered vulnerable to attackers that are able to make use of quantum computers. Certain quantum resistant cryptographic tools have also been developed to withstand these threats [14].

In summary, the major contribution of our work is as follows.

- This work gives description on the blockchain technology related to its background, architecture and its types.
- This work describes the security issues that occurs in the blockchain technology.
- This work provides insight on various blockchain technologies and the quantum level vulnerabilities residing in them.
- This work presents an overview on the various cryptographic concepts that are implemented in blockchain.
- Finally, this work presents the effect of quantum computing on blockchain and the post-quantum cryptosystem for blockchain.

The remainder of the paper is organised as follows, Section 2 presents the blockchain background including the architecture and properties, it explains the creation process of the blocks and further it describes the privacy issues in blockchain. Section 3 describes various blockchains and how quantum-capable attackers can exploit their vulnerabilities. Section 4 provides an overview of already in-use cryptographic concepts in blockchain. Section 5 presents the effect of quantum computing on the blockchain technology. Section 6 covers the pre-quantum to post-quantum evaluation of blockchain. Section 7 describes the post-quantum cryptosystems for blockchain.

2. Blockchain Background

Blockchain is a composition of network nodes and database. A blockchain database maintains record in form of blocks. It is fault-tolerant, shared, append-only and distributed database [15]. Blockchain users have access to the blocks but they can't delete or alter them. This section covers the introduction to blockchain technology and its principles. Following that explanation of mining or block construction techniques is given. Characteristics of

blockchains are also presented in this section along with different open-source blockchain implementation difference.

2.1 Blockchain Architecture

The Blockchain blocks are connected with each other via chain. Each block contains its predecessor's hash value and various verified transactions. It also included the timestamp that indicates the formation time of that block and a random numerical for the purpose of cryptographic operations. Nodes in blockchain maintain its peer-to-peer and distributed form. Even in the absence of third-party, blockchain lets communication parties interact with each other. These interactions get recorded and stored in blockchain database and provide security requirements. When a user has to interact with another user it then transactions are broadcasted into the network. Validation of interaction are checked through various nodes among the network and various valid interactions are then combined resulting in the formation of a new block. If the formed new block is valid, it joins the rest blockchain database and we can't remove or change it later. Blocks and transactions can't be dropped or altered in future because they are signed. Three generations of blockchain are there which respectively supports money transactions, assets and smart contract. Satoshi Nakamoto published the first generation [16] and it was implemented as a part of Bitcoin cryptocurrency. It was the first blockchain using application. The second generation shared assts instead of just money. These can be used to share any kind of assets such as good, votes etc [17]. Smart contracts were provided in the third generation of blockchain. A smart contract is a piece of code which is examined by everyone in the network. Thus, both parties stick to the contract because of its obligations. Third generation helped in increasing the popularity of blockchain and its application in services globally [18]. Figure 1 illustrates a blockchain architecture consisting of database and network of nodes.

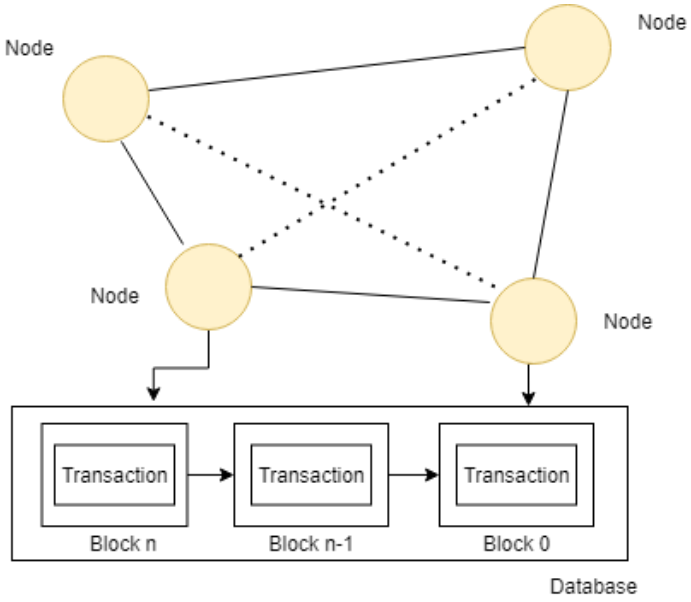

Figure 1: Blockchain architecture

2.2 Key Properties of Blockchains

Blockchain technology's key properties consists of cryptographic security, distributed nature, trustless system, non-repudiation guarantees and decentralized consensus. Below a brief description of these properties is given:

2.2.1 Cryptographic Security

The security algorithm should be fixed and guarantees that they can provide extreme security and are difficult to crack. Elliptic curve cryptography is being used by the blockchains which is difficult to crack. Additional it gets more difficult to crack because of decentralized consensus and trustless system [19]. As decentralization prohibits the simple changes in the characteristics of network. Every available information in the blockchain is hashed cryptographically. Private key is required to access the data and public key to carry out transactions.

2.2.2 Distributed Nature

Existing applications in blockchain are distributed in nature. It requires distributed control and security mechanisms. Centralized system is more popular among current security systems making inefficient for blockchain applications. Blockchain technology is distributed in nature. Therefore, blockchain security services can execute in distributive manner. Single person or authority doesn't control the framework in blockchain. We can store anything and because of the decentralized nature we posses' direct control over it through the private keys [20]. Relying on the third party isn't necessary for the asset's maintenance.

2.2.3 Trustless System

Third party can hinder in the security services and cause privacy risks if they are compromised. But the user in blockchain doesn't need to rely their trust on some third party. This system works mainly through the protocols, cryptography and code. While the blockchain technology is impenetrable which makes it difficult to compromise [21]. Attackers need to gain access of the entire system in order to compromise it. Therefore, it is trusted by the majority.

2.2.4 Non-repudiation Guarantee

It is a legal concept. This provides integrity and proof of origin of blockchain data. The problem that exists is that user can refuse their system interactions. But blockchain technology makes use of block and transaction signatures. Additionally, it also uses permanent database so that those transactions can't be contradicted later. Non-repudiation ensures that a party to communication must accept the authenticity of signature or message and the file has not been tampered with [22].

2.2.5 Decentralized Consensus

Consensus algorithm thrives the blockchain technology. Consensus helps the blockchain network to make decisions. In other words, it is the decision-making process for the active nodes in the network. In the centralized systems, failure of one controller point can end up failing the entire system. Blockchain technology is decentralised in nature Thus decisions are achieved by the agreement of various nodes and votes [23]. Each consensus algorithm has its own unique way to make decisions and improve previous mistakes.

2.3 Types of blockchains

Whenever the blockchain is applied the decision is made what kind of blockchain is best suited. Therefore, it is necessary to have clear understanding of the types of blockchain. Below section provides a brief description of the types available.

2.3.1 Public blockchain

Blockchain which is readable by anyone and transactions can be send and seen if they are valid by anyone are Public blockchains. They are considered inefficient. They are permissionless and anyone can take part in the network or in the consensus processes. Transactions can't be altered or censored on the network. The content in

blockchain is believed to be accurate. It requires more computing power to hold up trust. Therefore, in order to alter an entry in the blockchain system it requires for an attacker to at least gain 51% computing power of the total network [24].

2.3.2 Private blockchain

In these permission to access is slightly under control. The privilege to change or even read the state of blockchain is controlled for a few users. Therefore, it is not for anyone to join in only authenticate users can join the platform. In the network only few known nodes are permitted to take part. It is mostly used inside an organisation. The permission to write is usually centralized and limited to one organization. Private blockchains reduces the security breaches [25]. It denies the involvement of third-party control in the exchanging of data. Thus, counterparty risks are reduced.

2.3.3 Permissioned Blockchain

In this blockchain only particular IP addresses are allowed to perform specific actions. Network participants has the right to forbid users who take part in the consensus mechanism and who can make a smart contract and provide the authority to some users and hence prove the authentication of transaction blocks. The nodes use a control access layer for this purpose. A permission blockchain may have its own owner to validate the database, provide security services and control the privacy capacities [26]. But it is seen as violating the blockchain idea because only a few participate has control of the system which implies they can change on their own will.

Table 1 consists of summary of all blockchain types.

Type of Blockchain	Read	Write	Commit
Public	Anyone	Anyone	Anyone
Private	Authorized participants	Authorized participants	Network operators
Permissioned	Authorized participants	Authorized participants	All or subset of participants

Table 1: Types of Blockchain

2.4 Mining a Block

Creation of blocks in the blockchain is known as Mining. The blocks are further attached to the database. In some blockchains like bitcoin the creator of the first block is rewarded by the system in the form of money. Mining is considered as a critical process in blockchain technology. It permits the blockchain nodes for the creation of blocks which are also validates by others. If the formed block gets validation, then it gets involved in the database. Nodes helping in the creation of blocks are termed “mining nodes”. These blocks compete to each other and they try to form a fresh block as fast as they can in order to gain the prize.

Several methods are there which can determine that which block is going to be rewarded. Some methods are proof of stake (PoS), Proof of Importance (PoI) [27], Proof of work (PoW) [28], Proof of space (PoSpace) [29], minimum block hash, Measure of Trust (MoT) [30] and Practical Byzantine Fault Tolerance (PBFT) [31]. A brief description of these methods is given below:

2.4.2 Proof of Importance

The calculation of significance of an individual node is being done in this technique. The calculation is done based on the number of transactions and balance of that particular node. Priority to the most significant nodes is assigned on the basis of hash calculation. The high priority node is selected further to create the next block [27].

2.4.1 Proof of Work

It uses Bitcoin and many other blockchain technologies for the creation of new blocks by allocation of sufficient storage in order to perform mining. It requires more storage capacity instead of computational capability [28].

2.4.4 Minimum Block Hash

Paul et al. [30] came up with a mining idea where the miner is chosen randomly, not according to its resources. This approach chooses the miner on the basis of generated minimum hash value within the entire network.

2.4.3 Measure of Trust

This is another way of mining by selecting the node according to the trust level as the blockchain initiator [30]. Node’s behaviour determines the trustworthiness. To reward the nodes, they usually go for those nodes who follow the protocols. They are considered as good behaving nodes.

2.4.5 Practical Byzantine Fault Tolerance

It is a mining method which does not include any kind of resources but make use of blockchain consensus which are based on Byzantine fault tolerance method [31]. In this method, we select a head among the nodes and that leader determines the validation of transactions and issue a block for all nodes present in the network.

2.5 Privacy requirements and threats for blockchain

In the below section two analyses are given that covers the privacy requirements and threats which comes from the network, transactions and application.

2.5.1 Privacy requirements

To maintain the privacy, blockchain needs to full fill two requirements which are (1) The transaction links should remain invisible or undiscoverable, and (2) only the partaker has the idea of content in transactions. The privacy requirements should be dependent on the following factors:

Identity Privacy:

It implies that the user can only provide limited identity privacy. Some information about the blockchain user and their transactions can also be revealed by supervising the unencrypted network and going through the public blockchain, or some analysis strategies of behaviour such as know your customer (KYC) policy, ant-money laundering (AML) regulation [32]. It is meant for the intractability among the user identity, transactions between users and transaction data.

Transaction Privacy:

It means that the content of transaction is private and is permitted to only specific users. Otherwise, the data is kept hidden from the rest of the users in the public network of blockchain. Several blockchain applications are looking forward to use Transaction Privacy for the security purpose of users who are willing to get more privacy and don't intent to reveal their sensitive information [33]. Some examples of applications in which this is desired are big data's anonymous authorization or authentication or electrical heath record management.

2.5.2 Privacy threats

By tracing a transaction in a public blockchain network one can get the sensitive information of the user as the transaction consists of the participants, timestamp, trade values and signature of the sending party.In Bitcoin blockchain, the formation of pseudonyms takes place every time a user connects to the system. However, anyone can monitor the network activities or the blockchain information because of the public nature of

blockchain technology [34]. It can lead to de-anonymization of the user's real identities. Here some attacks are listed that may work for it.

- Network Analysis**:**

  Since blockchain technology is based on peer-to-peer network architecture, it implies that the IP address of a node can be leaked during the broadcasting of transactions. Koshy et al. [35] multi-relayer & non-rerelayed transaction, multi-relayer & non-rerelayed transactions and single-relayer transactions as three relay patterns for the purpose of network analysis.

- Transaction Fingerprinting:

  User related features of transactions are also a security threat. Androulaki et al. [36] characterized 6 features of any transaction behaviour. Those are Random time-interval (RTI), hour of day (HOD), time of hour (TOH), time of day (TOD), input/output balance and coin flow (CF). consideration of these factors increases the chances of de-anonymization of a user.

- DoS Attacks:

  A Denial-of-service (DoS) is a kind of cyber-attack in which the attacker makes a network or a machine unavailable. It is achieved by flooding the target with traffic or sending some information that might result in a crash. To hide IP addresses in Peer-to-peer network, anonymous network such as TOR is used. Yet, Biryukov et al [37] found out that DoS attack is able to disconnect TOR node from blockchain network.

- Sybil Attacks:

  It is a cyber-attack which is conducted on network service of a device. In sybil attack, an attacker brings down reputation system of a service by creating several pseudonymous identities. Sybil attack is able to break the decentralized anonymity protocols and increase the chances of finding out the identities of real users [38].

Transactions other than personally identifiable information goes into the public network. It can be used for the extraction of statistical distribution which can disclose new protocols in blockchain applications.

- Transaction graph analysis:

  It is based on the discovery of transaction features such as pattern, exchange rate or daily turnover. Ron et al [39] found out bitcoin's largest transactions in the transaction graph and identified four

transaction patterns in the network. These attributes may find out a financial history of a participant when implemented in conjunction along with de-anonymization schemes.

- AS-level deployment analysis:

  This scheme is aimed to drag the network of bitcoin by establishing connections with clients, requesting and collecting other peer's IP addresses in a recursive manner. Hence, one can gather tangible information about structure, size and distribution of the bitcoin network. These attributes can affect the resilience or vitality of the bitcoin ecosystem. Feld et al [40] studied the bitcoin system's distribution and size through autonomous systems (AS) and concluded that more than 30% of nodes in the network where of 0 AS while over 900 AS just contain a single node.

3. Quantum Computing and Blockchain technology

Quantum mechanism drastically increases computational capacity for some specific problem for example, factoring of large numerical into prime factors by Shor's algorithm and inversion of function from Grover's algorithm. Blockchain security is dependent upon the obscurity of certain cryptographic issues that are subverted by the ability of quantum computation

3.1 Threat of Quantum attacks:

Traditional computers follow the concept of classical mechanics and known as "classical computers". While "quantum computers" follows quantum mechanics which leads to a drastic gap in computational capacity. Quantum mechanics involves quantized (can't be divided further) physical quantities. For example, light is quantized, it consists of photons which can't be divided further. Many algorithms have been developed for classical computers which works for quantum computers significantly faster and provide greater information processing power, Deutsch's problem is an example of such [41]. In cryptographic systems those devices which are based on computation effort's asymmetry to compute a function and its inverse, a significant speedup may result in the breakdown of that system.

Initially, the creation of blockchain was for the context of Bitcoin to solve the issue of multiple spending [42]. Blockchain consists of blocks that are stored on public servers. Each block consists of data, hash of the preceding block, hash of the block, nonce that gives particular form to hash. Block uses hash of preceding block to strengthen the authentication for the preceding block. Blocks in the beginning of the chain can't be altered without altering the following blocks or inconsistency will occur in the hashes. Blockchain is relied on the computation of hashes in order to provide security from the modification of blocks. In quantum mechanics, two

aspects are studied which are able to invade the promises of blockchain. The first one is inversion of hashes which is supposed to be computationally tough. If a quantum computer can simplify it then there won't be any guarantee remains for upstream blockchain's authenticity and authenticity of blockchain entries can be compromised [43]. Grover's algorithm can be a threat to blockchain by attacking it in two ways. The first is by it can search for hash collisions and replace it by blocks without giving any harm to the integrity of the blockchain. The second is, it can speed up the generation of nonces, so that entire chains of record can be reformed with modified hashes crippling the integrity of the chain [44]. The secondary threat is, any blockchain implementation aspect that utilizes public or private key cryptography, whether it is for digital signature or information exchange among parties, a quantum computer can break the security of encryption. Grover's algorithm makes use of hashes to find the pre-image of a function. However, Shor's algorithm attacks blockchain that implements public/private key algorithm. This algorithm computes two prime factor of a composite number which is used as a public key in RSA algorithm [45]. Quantum computers are able to factor the integer which can't be done through classical computers, that makes it possible for attackers to forges digital messages or signatures.

3.2. Quantum Level vulnerabilities in blockchain platforms

Below we have discussed various technologies in blockchain, cryptographic scheme used by them, and how a quantum-capable attacker can exploit these dependencies.

3.2.1 Bitcoin

It was first described by Satoshi Nakamoto [46]. It is considered as the first true and most popular blockchain technology. A paper published in 2008 lead the way for distributed technologies development. It was implemented as a peer-to-peer payment method as resulted in getting rid of a central authority. Cryptographic schemes who permit peer in the network use it to for the transaction's validation and to store them in a secured cryptographic ledger. These cryptographic techniques can only be exploited by a powerful quantum computer otherwise it is safe from classical computers.

Bitcoin technology utilize Hashcash as it is PoW mechanism. Originally Hashcash was made for email systems to prevent denial of service. A prospective minor is required by Hashcash to determine a SHA-257 hash value for the header including some random numerical. Thus, that hash value is less than some predetermined numeric value. This number is a variable in the network [47]. Smaller number implies higher computational difficulty of issue. Hashcash PoW mechanism comes with two effects. First one is specialist hardware like ASIC miners

need to be used because of high difficulty parameters. Additionally, bad blocks may get added into the network because of PoW de-incentivizes.

3.2.2 Ethereum

It is considered as the second generation of blockchain. Ether and cryptocurrency are associated with it. It also proposed the usage distributed Applications (dApps) and smart contracts. An account-based system is used here in which each transaction will subtract or join Ether to some user's account. Smart contract permits blockchain users to make a contract which is computationally-binding. Which means that formation of transactions is dependable on some particular trackable objectives. Ethereum is currently going for the Proof-of-Stake (PoS) scheme. Previously it used EthHash which is a Proof-of-Work (PoW) mechanism. The PoW difficulty is created by a single round of SHA-3 (Keccak-265) hashing. A hash is created by the competition of mining nodes which provides the solution for the PoW problem. Casper is also a PoS scheme [48] which hasn't been implemented yet. PoW also prevents poor mining blocks because they will lose the ethers if the job is not done properly. The system security depends on the stake. As larger the value the more voting power the miner blocks will get. A user will be more honest if there are more coins on stake otherwise, they will end up losing more if discovered.

3.2.3 Litecoin

It is known as the source-code fork of the bitcoin blockchain technology. This implies that it has several similarities with Bitcoin blockchain. It also differs with bitcoin in many ways as this include the block time and PoW mechanism [49]. It possesses similar case with blockchain as an electronic payment method. However, it processes transactions in a faster manner in compare to Bitcoin because of short block time duration. It has a different PoW mechanism than Bitcoin which is called Scrypt. Scrypt is made for the consumption of less hashing power. This can be viewed through the comparison of power between Bitcoin and Litecoin as Bitcoin uses 46,000,000 TH/s [50] while Litecoin consumes only 298 TH/s [51]. Scrypt is designed by c. Percival [52] and it is considered as a less complex type of password derivation function. Originally it was designed for Tarsnap online backup system. Script is highly focused on usage of RAM on mining nodes. Therefore, it differs from other PoW mechanism as they focus on processing power. To sign transactions, Litecoin makes use of ECDSA method. It executes its signature with the secp-256k1 elliptic curve which is similar as Bitcoin.

3.2.4 Monero

It is based on the user privacy. By the usage of pseudonyms, various kind of blockchains advocate anonymity. We can find out transaction's sender or receiver by the use of chain analysis. We can even find out the number

of tokens that are exchanged, or the balance of any account. It keeps the identity of user and the amount transacted by the user hidden by the use of cryptographic techniques. It provides real anonymity to blockchain participants with the help of Pedersen Commitments [53] and Range Proofs [54]. It uses the ASIC-resistant CryptoNight v8 PoW method. This method is obtained from the Egalitarian Proof of Work from CryptoNote [55]. This method depends upon access to steady memory at some random time intervals. CryptoNight requires 2 Mb per second as it is memory intensive. EdDSA is being used in Monero as the signing algorithm. The twisted Edwards curve Ed25519 is used for the purpose of implementing EdDSA. This signature method is an alternative of ECDSA. It is still reliable on the difficulty of the discrete logarithm problems. A hashing function known as keccak-256 (SHA-3) is being used here.

3.2.5 Zcash

It is another blockchain technology which is based on privacy. However, it permits private accounts transactions into public ones and vice versa. It permits private and public both kind of transactions. Their transaction consists of zero-knowledge proofs which are in the form of Zk-snarks (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge); a trusted set up is being used.

Such set up makes use of some publicly-accessible element as a section for transaction proving mechanism. Centralized entity or association within the entire network in public ceremony form can generate such publicly-accessible elements. Zk-snarks is a kind of zero knowledge proof system which doesn't reveal the amount of transaction but permits the user to validate that transaction. Four kinds of transactions occur in Zk-snarks [56] which are: public, private, shielding and deshielding. The input and output among of transaction is hidden in private transactions. Public ones are known as "traditional transactions". They are similar to the other transactions in blockchain in which transaction amount can be publicly seen. Shielding transactions hide the previous transactions that are publicly visible while the work of deshielding transactions is quite the opposite. In order to gain consensus, Zcash uses the Euihas PoW. Equihash [57] is considered as a memory-hard PoW which is based on generalized birthday problem.

A summary of given vulnerabilities is presented in Table 2.

Blockchain	**Target**	**Risk level**	**Vulnerabilities**
Bitcoin	Transactions sent to network	High	Transactions which haven't turned into a

			block are vulnerable to quantum attacks. More significantly the signature scheme is risk vulnerable.
Ethereum	Re-use of public keys	High	It uses account-based system in which reuse of public keys is very common. Attackers can target previously declared transactions to the network.
Litecoin	Transactions sent to network	High	It is similar as bitcoin and equally vulnerable to quantum attacks.
Monero	Transactions sent to network and Unclear transactions	Medium	Monero uses EdDSA signature scheme which is vulnerable to quantum attacks since it is based on discrete logarithm problem.
Zcash	Zk-SNARK ceremony forms public parameter	Very high	It is highly vulnerable to quantum attacks which can take place against its signature scheme and consensus algorithm.

Table 2: Summary of Blockchain vulnerabilities.

4. Overview of used cryptographic concepts in blockchain

Various blockchain platforms already makes use of many cryptographic techniques. Since cryptography is a vast concept there are always possibilities to dig existing schemes and employ them in blockchain service. In the below section, some cryptographic concepts are presented which have already been implemented and analysed in blockchain.

4.1 Signature Scheme

Digital signatures are considered as a mathematical scheme which are based upon public-key cryptography. It focuses on the formation of short codes which are known as signatures of any digital message by using the private key and those signatures get the verification status by using corresponding public key. Digital signatures are used to prevent the forgeries and tampering in digital messages. Blockchain technology uses signature schemes for sign transactions [58]. It provides authentication to the sender along with integrity of transaction and non-repudiation of the sender. These schemes ensure anonymity and integrity in blockchain technology. It is considered one of the utmost significant cryptographic measures that makes blockchain technology publicly verifiable along with attainable consensus. Almost every blockchain makes use of signature scheme. Additionally, blockchain also provides some features like privacy, unlikability and anonymity by applying different signature schemes. Some of the signature schemes that have been applied in blockchain are given below:

Multi-Signature:

In this scheme, a bunch of participants signs a sole message. When a blockchain transaction is required a signature from the users it is beneficial to implement multi-signature scheme. OpenChain [59] and MultiChain [60] are two blockchain platforms that supports *M*-of-*N* multi-signature scheme, it minimizes the theft risk by having compromise tolerance up to *M*-1 cryptographic keys.

Ring Signature:

It uses a protocol in which a signature is formed on a message by one participant of a group protecting the individual identities of the signers. Anonymity of signers in the blockchain is achieved by using this scheme. CryptoNote [61] and A trustless tumbling platform [62] uses ring signature scheme for anonymity.

Blind Signature:

This scheme, employs the signatures in a privacy-related protocol where the message authors (or transactions) and signers are different parties. This scheme provides anonymity and unlikability of transactions. BlindCoin [63] makes use of blind signature scheme.

4.2 Zero-Knowledge Proofs

In this, a prover and a verifier i.e., two parties are involved. Initially, some statements are declared by the prover and then its validity is proved to the verifier, every information except statement remains undisclosed. Therefore, the statement is proved as 'transfer of an asset is valid' deprived of disclosing whatsoever related to the asset is being done by the zero-knowledge proof. These protocols are considered as extremely helpful cryptographic protocols to gain secrecy in the applications [64]. They can also be useful for the confidentially purpose of transaction data or asset while keeping them in the blockchain. Some public blockchain such as Zerocoin or Zerocash use zero-knowledge proofs for transactions that are untraceable or unlikable in nature. Zerocoin is considered as an extension of blockchain which provides unlikability and anonymity to the transactions with the help of zero-knowledge proofs. Zerocoin protocol does not require the involvement of third party and in this a user is able to produce Zerocoins equal the number of their Bitcoin. There are three ways by which a user can spend their Bitcoin i.e., by 1) generating secure commitment such as Zerocoin, 2) setting it down in the blockchain, and 3) broadcast of a transaction and zero-knowledge proof of the Zerocoin. Therefore, validation of Zerocoin and the verification of transaction can also be done by the other users. Thus, zero-knowledge proof protects the link between the user and the Zerocoin. But due to the large size of proof and high complexity, Zerocoin is considered as a costly protocol.

4.3 Access Control

Access control is about restricting resources and information selectively on that basis of some criteria or policies. The mechanism given in [65] can be used to control the access in the blockchain. The access can be to participate in the blockchain protocol or read/write access. Several mechanisms of access control are used in the blockchain. For example, attribute-based access control, role-based or organisational based. Access control can prevent the security breaches and data theft that are taking place in the recent years. Access control can also ensure data privacy in blockchain [66]. There exists different kind of mechanism of access control, some are described below:

Role-based Access Control (RBAC):

It is a method which restricts the system view to the system users conferring to their position in the system. Hence, it is implemented in blockchain where access depends on user role. It is being used in blockchain based healthcare solution [67]. Depending on the role every entity has its own access right in blockchain.

Attribute-based Access Control (ABAC):

In this approach, the access control protocols are dependent upon the structure of the attribute. These attributes can be user-specific, object-specific or environment-specific. For example, 'department' could be an attribute for any industry in blockchain environment [68]. Through 'department' we can restrict the access to data inside a blockchain.

Organization-based Access Control (OrBAC):

It is one of the richest models of access control. It consists of three things which are object, subject and action. These entities define that some subject has authorization to understand some action upon some object. OrBac is used in dynamic access control model and in IoT for fair access blockchain model [69].

4.4 Encryption Scheme

It is the procedure of transforming the data or information into a code by which only authorized parties have the access to it. Confidentiality of data inside the blockchain is achieved by it. Several types of encryption schemes are being used in blockchain. Symmetric-key Encryption, used for smart contract confidentiality [70] and Blockchain for smart home [71] in the Hyperledger fabric. Computation and searching over encrypted data are considered as a big challenge, however some techniques are there which are useful in this purpose. Searchable encryption is an example of such technique which is already used in permissioned blockchain. Searchable encryption is used for searching on encrypted data in the cloud. Functional encryption and fully homomorphic encryption are also used in blockchain for the computation of encrypted data. Authenticated encryption is also used in the blockchain which ensures simultaneously authenticity and confidentiality of data. In authenticated encryption, a connection is established by two peers, sharing of public key is done by both sides then it computes the shared data which works as symmetric key for the authenticated encryption algorithm. CAESAR [72] is a recently completed competition of cryptography which has identified six ciphers portfolio for authenticated encryption. Broadcast encryption provides anonymity of receiver nodes in the blockchain.

4.5 Secure Multi-Party Computation (SMPC)

Secure Multi-party computation allows parties to work in such a way that no single party has the access to all of the data, hence sensitive information won't get leaked. This scheme is based on the idea of jointly computing a function through parties by their input while keeping the input secret. for example, average salary of group of individuals can be calculated without revealing their actual salaries. Strong privacy can be achieved by using SMPC. Engima, which is a blockchain platform use SMPC to do so. In Engima, blockchain network and SMPC network are combined together, where blockchain network consists of hashes and SMPC contains data equivalent to those hashes. These hashes are divided among different nodes. Each node contains different piece of information hence, the view over SMPC network is different for each node. Hawk [73] is a blockchain model used for preserving the privacy of smart contracts. Hawk also states the useage of SMPC for the minimization of common reference string trust in SNARK proof that is used in the model. Decentralized systems like Keep [74] can also use SMPC for private storage of data. Wanchain [75] Cross-Chain network is also an application of SMPC. Wanchain consists of the concept of Storeman nodes. These nodes work together to generate public key pair of accounts and conduct the locking and unlocking of account.

4.6 Secret Sharing

This notion splits a secret into various parts among the participants, and is reformed by taking minimum number of parts. These parts are termed as shares and for each participant, they are unique. This technique is used for securing sensitive information. It is beneficial in SMPC for the share distribution between parties. Shamir's secret sharing [76] is used for the transaction data distribution, without any crucial data integrity loss in the blockchain. Decentralized Autonomous Organization (DAO) can also get benefit from the secret sharing by the distribution of information shares among the nodes of system rather than placing entire information in the nodes. Secret sharing can also be useful for safeguarding the crypto holder's private keys in various on-chain or off-chain bitcoin wallets. For example, let a firm has to place a single master private key bitcoin, for such purpose same key is stored among multiple persons with the help of secret sharing. Figure 2 presents distribution of a bitcoin wallet key between three participants by sharing the key shares. These shares don't hold any information of the actual key. However, any two out of three participants can construct the keys again by using their shares. Secret sharing can also store information in a decentralized manner which is advantageous to the blockchain by, it doesn't let unauthorized parties to have access over it.

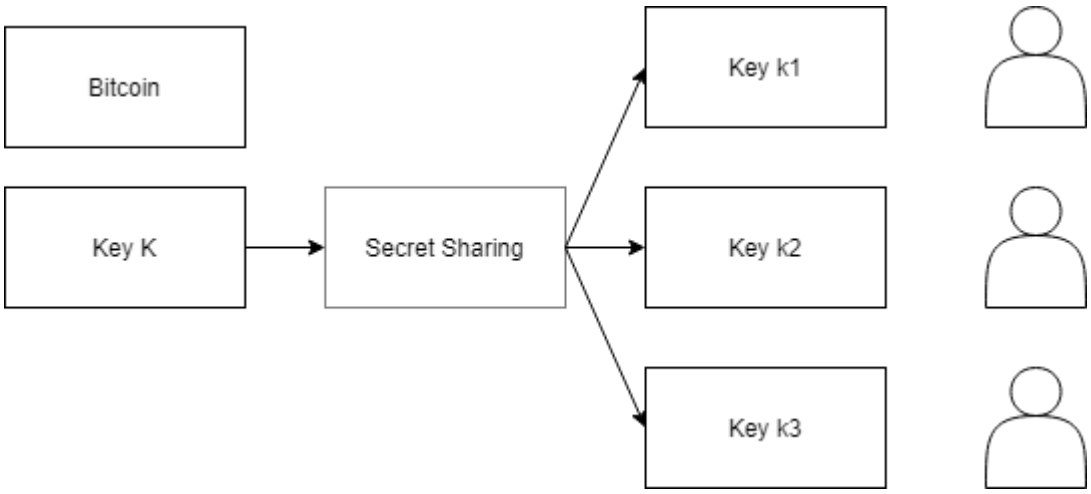

Figure 2: Secret sharing scheme for cryptographic wallet private key.

4.7 Accumulator

An accumulator is considered as a one-way function that provides a membership proof without disclosing identities of the individuals in an underlying set. This is used in blockchain for the formation of other cryptographic primitives for example, zero-knowledge proofs, commitment and ring signatures. Various cryptocurrencies use Merkle tree which is suitable for more comprehensive cryptographic accumulators that are data structure efficient in time and space used for testing set membership. Figure 3 presents the representation of blockchain transaction in a Merkle tree, block of the blockchain stores the root of Merkle tree. Non-Merkle accumulators are known as elliptic curve accumulators and RSA accumulators. Zerocoin [77] computes the accumulator A by overall coin commitments of network (Let $c_1,c_2,\ldots,c_n$) with membership witnesses for every item that the set contain. Accumulation coin calculates witness w with one exception. Knowledge of one coin is provided by the user using witness. Accumulator A and witness w remains publicly verifiable without need of any third party. Accumulator A is defined as:

$A=u^{c1\ c2\ c3\ldots c\ldots cn} \bmod N$,

Here u, n and A are integers and are known to everyone. c is a Pedersen commitment of coin with serial number s and random number z. witness w of coin c is defined as accumulation of all coins with exception of c:

$w=u^{c1\ c2\ c3\ldots c\ldots cn} \bmod N$.

Accumulators are utilized to design stateless blockchain where only a definite amount of storage is required by the nodes to participate in consensus.

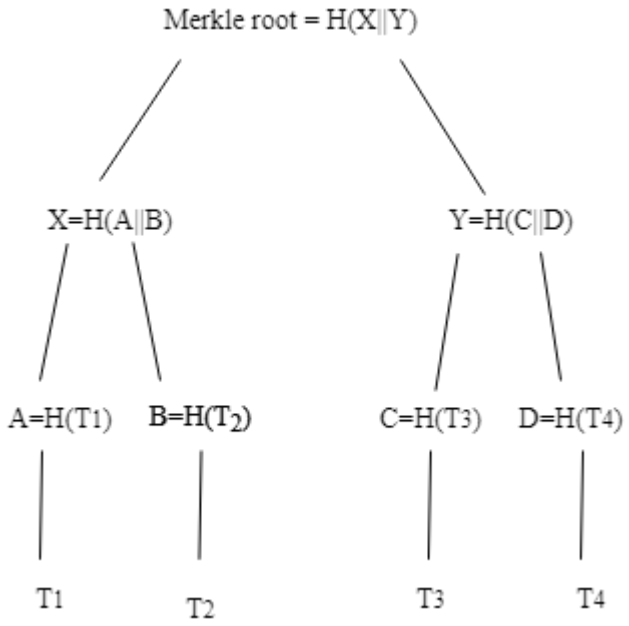

Figure 3: Merkle tree of Blockchain transactions

4.8 Lightweight cryptography

SHA256 and RSA are conventional cryptographic methods which work efficiently on systems with reasonable processing power and memory but not on devices with constrained battery, physical size or and memory. The implementation of conventional cryptographic methods in resource-constrained systems due to speed, energy consumption, large key size and implementation size is considered a challenge. Lightweight cryptography is the solution of this problem. It targets the embedded systems, sensor networks and other kinds of resource-constrained devices like RFID tags and end nodes of IoT. In comparison to conventional cryptography, Lightweight cryptography is considered faster and simpler but it comes with a flaw of being less secure as it is vulnerable to many attacks. Embedded devices with sensors in IoT are connected with each other through private or public network. Since these devices are resource-constrained, their issue of memory, communication and power consumption is solved by lightweight cryptography but security still lacks behind. To provide the solution of security issue, conjunction with sensor network can make use of blockchain. [78] provides a point to use blockchain and lightweight cryptography to improve the integrity and confidentiality of data in IoT devices. [79] also presents lightweight scalable blockchain (LSB) to improve the privacy and security of IoT devices. LSB makes use of hash function and consensus algorithm to achieve security.

5. Pre-Quantum to Post-Quantum Blockchain

Progress of quantum computing has made attacks related to Grover's and Shor's algorithm possible. Post-quantum blockchain is designed to withstand quantum computing attacks. In the below section presents an insight of pre-quantum evolution to post-quantum blockchain technique.

5.1 Blockchain Public-key Security

The strength of public-key cryptosystems has always been computed against the classical security attacks by bits-of-security level. This level is also defined as the efforts required to execute a brute-force attack by the use of a classical computer. Such as, an asymmetric cryptosystem possesses 1024-bit security and the effort needed to conduct a brute force attack by a classical computer on it is equal to the one required to execute a compromise a 1024-bit cryptographic key. [80] The cost can be up to hundreds of millions of dollars to break the current cryptosystems which has 80-bit security with the help of classical computers. 112-bit cryptosystems are studied to be safe against classical computing security threats for upcoming 3-4 decades. However, researches have shown that 1000-quibit quantum computer can break 160-bit elliptic curves while 1024-bit RSA would require about 2,000 qubits [81]. Such threats don't only affect cryptosystems that depends on integer factorization such as RSA or some elliptic curves (e.g., ECDH) but also based on other problems such as discrete logarithm problem. Shor's algorithm would be a faster solution for such kind of problems. There is not much of a progress on large powerful quantum computers as of now. The most powerful known quantum computer only possesses 79 qubits. It is claimed by IonQ. Even advanced organisations like U.S. National Security Agency (NSA) haven't made any significant progress.

5.2 Hash Function Security

Traditional hash functions are considered to resist the attacks caused by quantum computing in contradiction to the public-key cryptosystems [82]. In the recent times, academics have introduced some new hash functions to withstand the quantum attacks. Increasing the hash function's output size has been usually recommended. This recommendation is based on the concept that quantum attacks are able to utilize quadratic factors to increase the rate of brute force attack by following Grover's algorithm [83]. There are two ways in which Grover's algorithm can attack a blockchain:

- First one is by looking for hash collisions and followed by replacing the blocks of blockchain. Several hash functions may not have validiation for the post-quantum period, while others such as SHA-2 or SHA-3 would need to grow the size of output.

- Next one is to accelerate the mining in blockchain such as Bitcoin by using Grover's algorithm. It will let the entire blockchain recreate in a fast manner. Therefore, sabotaging their integrity.

Attacks by using Shor's algorithm can even affect hash functions. i.e., if hash function of gets broken then someone can make the use of Shor's algorithm by enough powerful quantum computer to forge digital signatures or impersonate the users of blockchain and steal their digital assets.

5.3 Initiatives of post-quantum blockchain

Post-quantum cryptography is one of the trending subjects and is discussed by many research projects such as PQCrypto [84], PROMETHEUS [85], CryptoMathCREST [86] or SAFEcrypto [87] and resulted in interesting results and reports. Although these projects and ideas resulted in notable results but their focus wasn't completely on post-quantum blockchain. However, some specific initiatives in post-quantum are there which are associated to most popular blockchain technologies. For example, Bitcoin Post-Quantum makes use of post-quantum digital signature method. It is an experimental branch of main blockchain of Bitcoin [88]. Another example we can take is of Ethereum 3.0, whose plan is to involve components which can resist quantum attacks such as zk-STARKs (Zero-Knowledge Scalable Transparent ARguments of knowledge) [89]. Other platforms of blockchain such as Abelian suggest the use of lattice based post-quantum cryptosystems to shield against these attacks. However, other blockchain technologies like Corda having experiments with SPHINCS which is a post-quantum algorithm [90]. NIST has also started a process for post-quantum public key cryptosystem [91] which is likely to deliver the drafts between 2022 and 2044. It is currently in its second round [92]. Its intention is that standards of new public-key cryptography will be able to specify one or more unclassified, public-key encryption and public disclosed digital signature that are globally available.

5.4 Ideal Characteristics of Post-Quantum Schemes

To achieve efficiency, post-quantum cryptosystems should possess following main features:

- Small size of keys:

  The device that makes interaction with the blockchain needs to use small private and public keys so that the storage space required can be reduced. Additionally, small keys also require comparatively easier computational operations for their management. This has even more importance for those blockchain technologies that makes use of IoT end devices that holds lesser storage or computational power. Iot took an exponential growth in the recent years just like other emerging technologies such as

Deep learning [93]. But it still faces some significant challenges. Security is a huge challenge with IoT devices since it is adopted widely and used with blockchain technology.

- Small signature and hash length:

  Increasing size of signatures or hash length will also increase the size of blockchain since it stores data transactions which includes user signatures and data or hashes [94].

- Execution with high speed:

  These schemes should be fast as much as they can so that they can allow blockchain processes a huge number of transactions per second [95]. Additionally, fast execution also requires low computational complexity.

- Less computational complexity:

  It is connected with fast execution. However, it should be noted that fast execution with a hardware device that doesn't use the post-quantum cryptosystem is considered to be computationally simple [96]. Therefore, it is required to analyse the switch between hardware, execution time and computational complexity.

- Low energy consumption:

  Bitcoin like blockchain technologies is known for consuming a lot power since it executes consensus protocol. Other factors also affect power consumption like hardware usage, number of transactions done and the security system which can consume relevant amount of power depending on the operation complexity [97].

6. Post-quantum cryptosystems for blockchain

There are total 4 core types of post-quantum cryptosystems the fifth one being the mix up of both post and pre quantum cryptosystem. A detailed description of these cryptosystems in presented in the below section.

6.1 Code-Based

These are based on error-correction codes supporting theory. For example, McEliece's cryptosystem which is based on code-based cryptosystem [98]. Its security is dependent upon syndrome decoding problem. This

scheme gives fast encryption as well as fast decryption which can be helpful in executing rapid blockchain transactions. However, this scheme needs to perform and then store large matrices operations which act for private and public keys. Such matrices take about 100kb to several mb's. When there is involvement of resource-constrained devices this amount of storage can get restricted. To overcome this problem, study of matrix compression techniques along with use of different codes such as Quasi-Cyclic Low Rank Parity-Check (QC-LRPC) or Low-Density Parity-Check (LDPC) and coding techniques is needed by future researchers. An observation of comparison between main characteristics of public-key code-based post-quantum cryptosystem which qualified the NIST call's second round is given in the below Table 3. The parameters given in Table 3 can be attuned with the security services required and so the size of key or performance can differ according to it.

Cryptosystem	Public key size (Bits)	Subtype	Quantum security (Bits)	Classical security (Bits)
RQC-I	6,824	Rank Quasi-Cyclic codes	-	128
RQC-II	11,128	Rank Quasi-Cyclic codes	-	192
RQC-III	18,272	Rank Quasi-Cyclic codes	-	256
NTS-KEM 1	2,555,904	Mc-Eliece and Niedrreiter	64	128
NTS-KEM 2	7,438,080	Mc-Eliece and Niedrreiter	96	192
NTS-KEM 3	11,357,632	Mc-Eliece and Niedrreiter	128	256
HQC 1	49,360	BCH codes and Quasi-Cyclic	64	128
HQC 2	87,344	BCH codes and Quasi-Cyclic	96	192
HQC 3	127,184	BCH codes and	128	256

		Quasi-Cyclic		
LEDACrypt KEM Level 1	14,976	QC-LDPC Niederreiter	-	128
LEDACrypt KEM Level 3	25,728	QC-LDPC Niederreiter	-	192
LEDACrypt KEM Level 5	36,928	QC-LDPC Niederreiter	-	256
BIKE-1 Level 1	20,326	QC-MDPC McEliece	-	128
BIKE-1 Level 3	39,706	QC-MDPC McEliece	-	192
BIKE-1 Level 5	65,498	QC-MDPC McEliece	-	256
BIKE-2 Level 1	10,163	QC-MDPC Niederreiter	-	128
BIKE-2 Level 3	19,853	QC-MDPC Niederreiter	-	192
BIKE-2 Level 5	32,749	QC-MDPC Niederreiter	-	256
BIKE-3 Level 1	22,054	QC-MDPC Quroboros	-	128
BIKE-3 Level 3	43,366	QC-MDPC Niederreiter	-	192
BIKE-3 Level 5	72,262	QC-MDPC Niederreiter	-	256

Table 3: Public-key encryption schemes built on post-quantum code that passed to NIST call second round.

6.2 Multivariate-based

It depends upon the complexity of systems who solves the multivariate equations, these are demonstrated as NP-hard or NP-complete [99]. They have high resistance to quantum attacks but it is still required that future research try to improve their speed of decryption which is because of the involvement of "guess work" and minimize their big size of keys and cipher text overhead [100].

At the moment, the most encouraging schemes that are based on multi-variation are those which are relied upon the usage of square matrices along with random quadratic polynomials, the cryptosystems are derived from Matsumoto-Imai's algorithm and are relayed upon Hidden Field Equations (HFE) [101]. Public keys are formed in this scheme by a trapdoor function which acts like a private key. Some most famous multivariate-based schemes count on Matsumoto-Imai's algorithm, on HFE variants or on Isomorphism of Polynomial (IP). Some other multivariate-based schemes are also been proposed like the ones which are based on Rainbow-like signing schemes such as Rainbow, TRMS, TTS etc. or on pseudo-random multivariate quadratic equations. But improvement of key size is still required since they take huge number of bytes per key.

6.3 Lattice-based

Such cryptographic schemes are built upon lattices. Lattices are set of points situated inside a n-dimensional space along with intervallic structure. Such security systems are based upon speculated hardness of the lattice issues such as the Shortest Vector Problem full for SVP. SVP comes under the category of NP-hard problem, its aim is to determine the shortest non-zero vector inside a lattice. Some other problems such as Shortest Independent Vector Problem (SIVP) or Closest Vector Problem (CVP) are similar to this concept but these can't be solved properly by using quantum computers [102]. These schemes provide implementation that results in the increased speed of transactions by blockchain users because they are generally computationally modest, hence, their execution can have high speed and in an efficient manner. However, for some other schemes, these implementations need to use and store large size of keys, comprising huge ciphertext overheads. Methods like NewHope or NTRU requires the management of keys in the order of a few thousand bits. The utmost encouraging lattice-based cryptosystems are considered those which are based upon the polynomial algebra [103] and Learning With Errors (LWE) problems and its variations such as LP-LWE or Ring-LWE [104].

6.4 Supersingular elliptic curve isogeny

Such methods are relied upon isogeny protocol for ordinary elliptic curve given in [105] but improved to deal with the quantum attack described in [106]. Only one isogeny-based public-key encryption method was able to enter the second round of NIST call i.e., SIKE. It is focused on pseudo-random walks in supersingular isogeny

graphs. This scheme can also be used for the creation of post-quantum digital signature scheme, but they aren't much popular and provides poor performance. Description of many signature schemes is provided in [107], these are based on problems of isogeny and Unruh transform which uses small sized keys an efficient signing and verification algorithms. Another Unruh transform based signature scheme is given in [108], which uses public key of 336-bytes and private key of 48-bytes for a quantum security level of 128-bit and forms a signature of 122,880 bytes (even if compressing techniques are being used). Thus, while executing isogeny-based cryptosystems or Super-singular Isogeny Diffie-Hellmann (SIDH) it is required to take care of the key size issue, especially when the devices are resource-constrained.

6.5 Hash-based signature schemes

Security of underlying hash functions is responsible for the security of these schemes in place of the hardness of some mathematical problem. These schemes date back to 70s, when a one-way function-based signature scheme was proposed by Lamport [109]. These days eXtended Merkle Signature Scheme (XMSS) variants such as SPHINCS or XMSS-T are known to be significant hash-based signature scheme in the post-quantum era that is earned after the Merkle tree scheme presented in [110]. However, due to the performance of SPHINCS and XMSS they are viewed as impractical for the purpose of applications in blockchain. Therefore, their substitutes have been proposed. One of the examples is XMSS, it is being used in blockchain by using single authentication path instead of a tree. Some other researchers suggested to substitute XMSS with XNYSS (eXtended Naor-Yung Signature Scheme). XYNSS combines Naor-Yung chains together with hash-based one-time signature scheme, it allows creation of chains with related signature.

7. Conclusion

In the recent years, blockchain has received notable attention because of its decentralized nature since it diminishes the need of trusted third party thus making it more secure. Blockchain is utilized to store, verify and update data and is expected to play a vital role for upcoming Internet interactive systems such as supply chain or IoT. However, blockchain is prone to attacks carried out by quantum computers such as Grover's algorithm and Shor's algorithm. This paper describes the architecture, properties and privacy threats related to blockchain. Further, it describes the vulnerabilities that a quantum-able attacker can targets inside different blockchains. Then this paper discusses the concept of quantum computing with blockchain and evaluation of blockchain from pre-quantum to post-quantum state. In the end, the post-quantum cryptosystems are being described.

References:

[1] Sathya, A. R., & Rao, K. V. (2020). Exploring the bitcoin network. *Bitcoin and Blockchain*, 23–35. https://doi.org/10.1201/9781003032588-2

[2] Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2020). Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. *Wireless Networks*. doi:10.1007/s11276-020-02445-6

[3] Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., & Debnath, N. C. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*, *61*, 102360. DOI: 10.1016/j.scs.2020.102360

[4] Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to Secure Iot: Background, integration trends and a way forward. *Journal of Network and Computer Applications*, 103050. doi:10.1016/j.jnca.2021.103050

[5] Mohamed, K. S. (2020). Cryptography concepts: Confidentiality. *New Frontiers in Cryptography*, 13–39. https://doi.org/10.1007/978-3-030-58996-7_2

[6] Hash function, message authentication code, and data expansion function. (n.d.). *Mobile Communication Systems and Security*, 387–415. https://doi.org/10.1002/9780470823392.ch10

[7] Digital currency, Bitcoin and cryptocurrency. (2018). *Inclusive FinTech*, 33–82. https://doi.org/10.1142/9789813238640_0002

[8] Stubbs, R. (n.d.). *Quantum computing and its impact on cryptography*. Cryptomathic. Retrieved November 6, 2021, from https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography.

[9] Bhushan, B., Sinha, P., Sagayam, K. M., & J, A. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, *90*, 106897. https://doi.org/10.1016/j.compeleceng.2020.106897

[10] Quantum Computer Programming. (n.d.). *Automatic Quantum Computer Programming*, 23–35. https://doi.org/10.1007/978-0-387-36791-0_3

[11] Cao, Z., Liu, L., & Christoforides, A. (2020). A note on one realization of a scalable Shor algorithm. https://doi.org/10.37686/qrl.v1i2.81

[12] *Shor's algorithm*. IBM Quantum. (n.d.). Retrieved November 20, 2021, from https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm.

[13] Bradben. (n.d.). *Theory of grover's search algorithm - azure Quantum*. Azure Quantum | Microsoft Docs. Retrieved November 8, 2021, from https://docs.microsoft.com/en-us/azure/quantum/concepts-grovers.

[14] Why Blockchain? (2018). *The Blockchain and the New Architecture of Trust*. https://doi.org/10.7551/mitpress/11449.003.0008

[15] Bhushan, B., & Sharma, N. (2020). Transaction Privacy Preservations for Blockchain Technology. *Advances in Intelligent Systems and Computing International Conference on Innovative Computing and Communications*, 377-393. DOI: 10.1007/978-981-15-5148-2_34

[16] Tempesta, S. (2019). Blockchain Architecture Reference. *Introduction to Blockchain for Azure Developers*. https://doi.org/10.1007/978-1-4842-5311-3_5

[17] Goyal, S., Sharma, N., Kaushik, I., & Bhushan, B. (2021). Blockchain as a solution for security attacks in named data networking of things. *Security and Privacy Issues in IoT Devices and Sensor Networks*, 211-243. doi:10.1016/b978-0-12-821255-4.00010-9

[18] Malik, A., Gautam, S., Abidin, S., & Bhushan, B. (2019). Blockchain Technology-Future Of IoT: Including Structure, Limitations And Various Possible Attacks. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. DOI: 10.1109/icicict46008.2019.8993144

[19] National Institute of Standards and Technology. (2002, December 3). *Security requirements for cryptographic modules*. CSRC. Retrieved November 20, 2021, from https://csrc.nist.gov/publications/detail/fips/140/2/final.

[20] Bolfing, A. (2020). Distributed Systems. *Cryptographic Primitives in Blockchain Technology*, 143–198. https://doi.org/10.1093/oso/9780198862840.003.0005

[21] Dong, Y., & Boutaba, R. (2020). Melmint: Trustless stable cryptocurrency. *Cryptoeconomic Systems*. https://doi.org/10.21428/58320208.b704a743

[22] Blockchain 2020 organizing committee. (2020). *2020 IEEE International Conference on Blockchain (Blockchain)*. https://doi.org/10.1109/blockchain50366.2020.00008

[23] Soni, S., & Bhushan, B. (2019). A Comprehensive survey on Blockchain: Working, security analysis, privacy threats and potential applications. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. DOI: 10.1109/icicict46008.2019.8993210

[24] Public policy in a blockchain era. (2019). *Understanding the Blockchain Economy*, 138–151. https://doi.org/10.4337/9781788975001.00013

[25] Larmuseau, A., & Shila, D. M. (2019). Private blockchain configurations for improved IOT security. *Blockchain for Distributed Systems Security*, 253–274. https://doi.org/10.1002/9781119519621.ch12

[26] Mitani, T., & Otsuka, A. (2019). Traceability in permissioned blockchain. *2019 IEEE International Conference on Blockchain (Blockchain)*. https://doi.org/10.1109/blockchain.2019.00045

[27] *Proof of importance definition: What is proof of importance?* Cryptomaniaks. (n.d.). Retrieved November 8, 2021, from https://cryptomaniaks.com/cryptocurrency-glossary/p/proof-of-importance.

[28] Todorović, V., & Tomić, N. (2019). Unsustainability of cryptocurrency concept based on the proof-of-work algorithm. *Bankarstvo*, *48*(1), 46–63. https://doi.org/10.5937/bankarstvo1901046t

[29] *Proofs of space - cryptology ePrint Archive*. (n.d.). Retrieved November 8, 2021, from https://eprint.iacr.org/2013/796.pdf.

[30] *Measuring trust* Edward L.GLAESER David I.LAIBSON j ...* (n.d.). Retrieved November 8, 2021, from https://scholar.harvard.edu/files/laibson/files/measuring_trust.pdf.

[31] Byzantine fault tolerance. (2021). *From Traditional Fault Tolerance to Blockchain*, 245–293. https://doi.org/10.1002/9781119682127.ch7

[32] Strauß, S. (2019). The interplay between identity, identification and privacy. *Privacy and Identity in a Networked Society*, 30–80. https://doi.org/10.4324/9780429451355-3

[33] Dwivedi, A., Mishra, A., & Singh, D. (2021). Cybersecurity and privacy issues of Blockchain technology. *Blockchain for Information Security and Privacy*, 69–94. https://doi.org/10.1201/9781003129486-4

[34] Plessing, P., & Omolola, O. (2020). Revisiting privacy-aware Blockchain Public Key Infrastructure. *Proceedings of the 6th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0008947104150423

[35] Koshy, P., Koshy, D., & McDaniel, P. (2014). An analysis of anonymity in bitcoin using P2P network traffic. In R. Safavi-Naini, & N. Christin (Eds.), *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Revised Selected Papers* (pp. 469-485). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 8437). Springer Verlag. https://doi.org/10.1007/978-3-662-45472-5_30

[36] Androulaki E., Karame G.O., Roeschlin M., Scherer T., Capkun S. (2013) Evaluating User Privacy in Bitcoin. In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39884-1_4

[37] Biryukov, Alex & Pustogarov, Ivan. (2015). Bitcoin over Tor isn't a Good Idea. 122-134. 10.1109/SP.2015.15.

[38] The threshold of cyber warfare: From use of Cyber Force to Cyber Armed Attack. (2020). *Cyber Operations and International Law*, 273–342. https://doi.org/10.1017/9781108780605.009

[39] Ron D., Shamir A. (2013) Quantitative Analysis of the Full Bitcoin Transaction Graph. In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39884-1_2

[40] Feld, Sebastian & Schönfeld, Mirco & Werner, Martin. (2014). Analyzing the Deployment of Bitcoin's P2P Network under an AS-level Perspective. Procedia Computer Science. 32. 10.1016/j.procs.2014.05.542.

[41] Chowdhury, N. (2019). Bitcoin: World's first cryptocurrency. *Inside Blockchain, Bitcoin, and Cryptocurrencies*, 61–89. https://doi.org/10.1201/9780429325533-4

[42] Chouhan, K., Rathore, P. S., & Dixit, P. (2020). Blockchain and Bitcoin Security: Threats in bitcoin. *Blockchain Technology and the Internet of Things*, 223–243. https://doi.org/10.1201/9781003022688-10

[43] Palladino, S. (2019). Blockchains. *Ethereum for Web Developers*, 1–16. https://doi.org/10.1007/978-1-4842-5278-9_1

[44] Callens, E. (2020). Financial instruments entail liabilities: Ether, Bitcoin, and Litecoin do not. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3630895

[45] Tu, Z., & Xue, C. (2019). Effect of bifurcation on the interaction between Bitcoin and litecoin. *Finance Research Letters*, *31*. https://doi.org/10.1016/j.frl.2018.12.010

[46] Raymer, M. G. (2017). Application: Quantum computing. *Quantum Physics*. https://doi.org/10.1093/wentk/9780190250720.003.0010

[47] Zubairy, M. S. (2020). Quantum Computing II. *Quantum Mechanics for Beginners*, 245–262. https://doi.org/10.1093/oso/9780198854227.003.0016

[48] Impact of quantum computing. (2019). *Quantum Computing for Everyone*. https://doi.org/10.7551/mitpress/11860.003.0011

[49] Djordjevic, I. B. (2021). Fault-tolerant quantum error correction and fault-tolerant quantum computing. *Quantum Information Processing, Quantum Computing, and Quantum Error Correction*, 469–530. https://doi.org/10.1016/b978-0-12-821982-9.00017-4

[50] Djordjevic, I. B. (2021). Cluster State-based quantum computing. *Quantum Information Processing, Quantum Computing, and Quantum Error Correction*, 531–561. https://doi.org/10.1016/b978-0-12-821982-9.00004-6

[51] Miglietti, C., Kubosova, Z., & Skulanova, N. (2019). Bitcoin, Litecoin, and the euro: An annualized volatility analysis. *Studies in Economics and Finance*, *37*(2), 229–242. https://doi.org/10.1108/sef-02-2019-0050

[52] Percival, C., & Josefsson, S. (2016). The scrypt password-based key derivation function. https://doi.org/10.17487/rfc7914

[53] Otavio Chervinski, J., Kreutz, D., & Yu, J. (2021). Analysis of transaction flooding attacks against Monero. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. https://doi.org/10.1109/icbc51069.2021.9461084

[54] Kim, M., & Lee, H. T. (2019). Experimenting with non-interactive range proofs based on the strong RSA assumption. *IEEE Access*, *7*, 117505–117516. https://doi.org/10.1109/access.2019.2936210

[55] Yu, J., Au, M. H., & Esteves-Verissimo, P. (2019). Re-thinking untraceability in the cryptonote-style blockchain. *2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*. https://doi.org/10.1109/csf.2019.00014

[56] Banerjee, A., Clear, M., & Tewari, H. (2020). Demystifying the role of ZK-SNARKs in Zcash. *2020 IEEE Conference on Application, Information and Network Security (AINS)*. https://doi.org/10.1109/ains50155.2020.9315064

[57] Bai, X., Gao, J., Hu, C., & Zhang, L. (2019). Constructing an adversary solver for equihash. *Proceedings 2019 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2019.23337

[58] Martin, K. M. (2017). Digital Signature Schemes. *Oxford Scholarship Online*. https://doi.org/10.1093/oso/9780198788003.003.0007

[59] Information technology openchain specification. (n.d.). https://doi.org/10.3403/30419807u

[60] G. Greenspan. (2015). MultiChain Private Blockchain. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper. pdf

[61] N. van Saberhagen. (2013). Cryptonote. [Online]. Available: https:// cryptonote.org/whitepaper.pdf

[62] *M obius: Trustless tumbling for Transaction Privacy*. (n.d.). Retrieved November 8, 2021, from https://eprint.iacr.org/2017/881.pdf.

[63] L. Valenta and B. Rowan, ‘‘Blindcoin: Blinded, accountable mixes for bitcoin,’’ in Financial Cryptography and Data Security, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds. Berlin, Germany: Springer, 2015, pp. 112–126

[64] Zero-knowledge proof systems. (2001). *Foundations of Cryptography*, 184–330. https://doi.org/10.1017/cbo9780511546891.005

[65] Discretionary-access control and the access-matrix model. (n.d.). *Access Control Systems*, 147–167. https://doi.org/10.1007/0-387-27716-1_5

[66] Foundations of security and access control in computing. (n.d.). *Access Control Systems*, 1–39. https://doi.org/10.1007/0-387-27716-1_1

[67] Role-based access control. (n.d.). *Access Control Systems*, 190–251. https://doi.org/10.1007/0-387-27716-1_8

[68] Biswas, P., Sandhu, R., & Krishnan, R. (2017). Attribute transformation for attribute-based access control. *Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control - ABAC '17*. https://doi.org/10.1145/3041048.3041052

[69] Mandatory-access-control model. (n.d.). *Access Control Systems*, 129–146. https://doi.org/10.1007/0-387-27716-1_4

[70] Data Encryption Standard (DES) and Advanced Encryption Standard (AES). (n.d.). *SpringerReference*. https://doi.org/10.1007/springerreference_73130

[71] Deguchi, A. (2020). From Smart City to society 5.0. *Society 5.0*, 43–65. https://doi.org/10.1007/978-981-15-2989-4_3

[72] D. J. Bernstein. (2014). CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. [Online]. Available: https://competitions.cr.yp.to/caesar.html

[73] Hawk. (n.d.). *Gravel and Hawk*, 25–25. https://doi.org/10.1353/chapter.471742

[74] Autonomous Decentralized Safety Critical System. (2018). *Autonomous Decentralized Systems and Their Applications in Transport and Infrastructure*, 33–57. https://doi.org/10.1049/pbtr009e_ch2

[75] *Decentralized finance interoperability*. Wanchain. (n.d.). Retrieved November 8, 2021, from https://www.wanchain.org/.

[76] Catrina, O. (2019). Efficient secure floating-point arithmetic using Shamir Secret Sharing. *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*. https://doi.org/10.5220/0007834100490060

[77] Takabatake, Y., & Okabe, Y. (2021). An anonymous distributed electronic voting system using zerocoin. *2021 International Conference on Information Networking (ICOIN)*. https://doi.org/10.1109/icoin50884.2021.9333937

[78] Information Technology. security techniques. lightweight cryptography. (n.d.). https://doi.org/10.3403/30204851

[79] Computer Security Division, I. T. L. (n.d.). *Lightweight cryptography: CSRC*. CSRC. Retrieved November 8, 2021, from https://csrc.nist.gov/Projects/Lightweight-Cryptography.

[80] Cryptographic key. (n.d.). *SpringerReference*. https://doi.org/10.1007/springerreference_11418

[81] Katz, J., & Lindell, Y. (2020). *post-quantum cryptography. *Introduction to Modern Cryptography*, 499–524. https://doi.org/10.1201/9781351133036-17

[82] Raymer, M. G. (2017). Application: Quantum computing. *Quantum Physics*. https://doi.org/10.1093/wentk/9780190250720.003.0010

[83] Diao, Z. (2010). Exactness of the original Grover Search algorithm. *Physical Review A*, *82*(4). https://doi.org/10.1103/physreva.82.044301

[84] PQCRYPTO Project. Accessed: Nov. 2, 2019. [Online]. Available: https: pqcrypto.eu.org

[85] Ruffell, I. (2018). Prometheus. *Classics*. https://doi.org/10.1093/obo/9780195389661-0304

[86] CryptoMathCREST Project. Accessed: Nov. 2, 2019. [Online]. Available: https://cryptomath-crest.jp/english

[87] O'Neill, M., O'Sullivan, E., McWilliams, G., Saarinen, M.-J., Moore, C., Khalid, A., Howe, J., del Pino, R., Abdalla, M., Regazzoni, F., Valencia, F., Güneysu, T., Oder, T., Waller, A., Jones, G., Barnett, A., Griffin, R., Byrne, A., Ammar, B., & Lund, D. (2016). Secure architectures of future emerging cryptography SAFEcrypto. *Proceedings of the ACM International Conference on Computing Frontiers*. https://doi.org/10.1145/2903150.2907756

[88] Bitcoin mechanisms. (2018). *Bits to Bitcoin*. https://doi.org/10.7551/mitpress/10710.003.0032

[89] Iyer, K., & Dannen, C. (2018). First steps with ethereum. *Building Games with Ethereum Smart Contracts*, 37–56. https://doi.org/10.1007/978-1-4842-3492-1_3

[90] Satheesh, V., & Shanmugam, D. (2020). Implementation vulnerability analysis: A case study on Chacha of SPHINCS. *2020 IEEE International Symposium on Smart Electronic Systems (ISES) (Formerly INiS)*. https://doi.org/10.1109/ises50453.2020.00032

[91] Bernstein, D. J. (n.d.). Introduction to post-quantum cryptography. *Post-Quantum Cryptography*, 1–14. https://doi.org/10.1007/978-3-540-88702-7_1

[92] Ciesla, R. (2020). Post-quantum cryptography. *Encryption for Organizations and Individuals*, 257–275. https://doi.org/10.1007/978-1-4842-6056-2_14

[93] The future of Deep Learning. (2019). *Deep Learning*. https://doi.org/10.7551/mitpress/11171.003.0010

[94] Information Technology. security techniques. hash-functions. (n.d.). https://doi.org/10.3403/01569240

[95] Badhwar, R. (2021). The need for Post-Quantum. *The CISO's Next Frontier*, 15–30. https://doi.org/10.1007/978-3-030-75354-2_2

[96] Vlahek, D. (2010). The problem of quantum computers in cryptography and post-quantum cryptography. *StuCoSReC. Proceedings of the 2018 5th Student Computer Science Research Conference.* https://doi.org/10.26493/978-961-7055-26-9.61-64

[97] Overbeck, R., & Sendrier, N. (n.d.). Code-based cryptography. *Post-Quantum Cryptography*, 95–145. https://doi.org/10.1007/978-3-540-88702-7_4

[98] R. J. McEliece, ‘‘A public-key cryptosystem based on algebraic coding theory,’’ Deep Space Netw. Prog. Rep., Tech. Rep. DSN PR 42-44, Jan./Feb. 1978, pp. 114–116.

[99] Bernstein, D. J. (n.d.). Introduction to post-quantum cryptography. *Post-Quantum Cryptography*, 1–14. https://doi.org/10.1007/978-3-540-88702-7_1

[100] Cipher text. (n.d.). *SpringerReference*. https://doi.org/10.1007/springerreference_10008

[101] L, V., & V, B. (2019). Encryption and decryption technique using matrix theory. *Journal of Computational Mathematica*, *3*(2), 1–7. https://doi.org/10.26524/cm49

[102] Asif, R. (2021). Post-Quantum cryptosystems for Internet-of-Things: A survey ON LATTICE-BASED ALGORITHMS. *IoT, 2*(1), 71-91. doi:10.3390/IoT2010005

[103] Khalid, A., McCarthy, S., O'Neill, M., & Liu, W. (2019). Lattice-based cryptography for IoT in a Quantum World: Are We Ready? *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*. doi:10.1109/iwasi.2019.8791343

[104] R. Lindner and C. Peikert, ‘‘Better key sizes (and attacks) for LWE-based encryption,’’ in Proc. Cryptographers’ Track RSA Conf., San Francisco, CA, USA, Feb. 2011, pp. 319–339

[105] A. Rostovtsev and A. Stolbunov, ‘‘Public-key cryptosystem based on isogenies,’’ Cryptol. ePrint Arch., Tech. Rep. 2006/145, 2006.

[106] A. Childs, D. Jao, and V. Soukharev, ‘‘Constructing elliptic curve isogenies in quantum subexponential time,’’ J. Math. Cryptol., vol. 8, no. 1, pp. 1–29, Jan. 2014.

[107] S. D. Galbraith, C. Petit, and J. Silva, ‘‘Identification protocols and signature schemes based on supersingular isogeny problems,’’ in Proc. ASIACRYPT, Hong Kong, Dec. 2017, pp. 3–33

[108] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, and V. Soukharev, ‘‘A postquantum digital signature scheme based on supersingular isogenies,’’ in Proc. Int. Conf. Financial Cryptogr. Data Secur., Sliema, Malta, Apr. 2017, pp. 163–181.

[109] Hash-based cryptography. (2021, March 06). Retrieved April 14, 2021, from https://en.wikipedia.org/wiki/Hash-based_cryptography#:~:text=Hash%2Dbased%20cryptography%20is%20the,type%20of%20post%2Dquantum

[110] R. C. Merkle, ‘‘A certified digital signature,’’ in Proc. EUROCRYPT, 1989, pp. 218–238