A Comprehensive Study of Blockchain Services: Future of Cryptography

Sathya AR[1], Barnali Gupta Banik[2]
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation, Deemed to be University
Hyderabad, Telangana-500075

***Abstract*—Cryptography is the process of protecting information from intruders and letting only the intended users' access and understand it. It is a technique originated in 2000 BC where simple methods were used in earlier times to keep the information in a way that is not understandable by everyone. Only the intended receiver knows how to decode the information. Later, as technology advances, many sophisticated techniques were used to protect the message so that no intrusion can invade the information. Many mathematically complex algorithms like AES, RSA are used to encrypt and decrypt the data. Due to the advancements in the computer science field, recently, cryptography is used in the development of cryptographic currencies of cryptocurrencies. Blockchain technology, a distributed ledger technology identified to be the foundation of Bitcoin cryptocurrency, implements a high-level cryptographic technique like public-key cryptography, Hash Functions, Merkle Trees, Digital signatures like Elliptic curve digital signatures, etc. These advanced cryptographic techniques are used to provide security to blockchain data and for the secure transmission of information, thereby making Blockchain more popular and demandable. Blockchain applies cryptography in various phases, and some of the techniques used in Blockchain are advanced in cryptographic sciences. This paper intends to provide a brief introduction to cryptography and Blockchain Technology and discusses how both technologies can be integrated to provide the best of the security to the data. This paper reviews the various cryptographic attacks in Blockchain and the various security services offered in Blockchain. The challenges of blockchain security are also analyzed and presented briefly in this paper.**

Keywords*—Cryptography; cryptocurrencies; blockchain; bitcoin

I. Introduction

Blockchain is a distributed, P2P, decentralized network where data is secure and tamper-proof. The transaction over the networks are recorded transparently without any third party. Although Blockchain technology was developed to support cryptocurrencies, industries of various sectors show great interest in adapting them for their interest. Like financial transactions, supply chain, secure contracts, sharing sensitive information, governance, and many more. The critical issues of existing systems are information security and data storage. Blockchain technology resolves these issues by assuring transparency and maintaining the integrity of the stored data. Generally, it is believed that the data is authentic if there is a central server or a third party to maintain the data. It is very much essential to encrypt the data if there is no trusted central system. Therefore, cryptography plays a vital role in Blockchain. In Blockchain, cryptography is adapted to ensure the consistency of the data, guard user privacy, and transaction information [1].

The organization of the paper is as follows. Section II elaborates the cryptography background of Blockchain Technology. Section III discusses the convergence of cryptography and Blockchain. The various security attacks and security services are presented in detail in Sections IV and V, respectively. Section VI summarizes the applications of blockchain technology and the different challenges are described in Section VII.

II. Background

A. Related Knowledge on Blockchain Technology

Blockchain is a decentralized public ledger distributed over the network recording the transactions of the network [2]. The distributed ledger is open to the public, and every node in the network has a copy of the ledger. Transactions over the network are combined as blocks, and every block is connected to the previous block using hashing algorithms. The network nodes strictly protect the data into blocks and broadcast the information to the network. Hashing helps in ensuring the data integrity by linking each block with the other by the hash code. Thus, a chain of blocks linked via a hash is called Blockchain. The simple architecture of Blockchain has been demonstrated in Fig. 1. Blockchain is the underlying technology of the most popular cryptocurrency Bitcoin. Later many other cryptocurrencies, like altcoins, peercoins, litecoins added more popularity to this technology. At present, Blockchain is one of the fastest-growing technologies due to its unique features like immutability, integrity, security, and reliability. After bitcoin, Ethereum is the most successful Blockchain- based project. Ethereum is a platform used to develop decentralized applications (DApps) and Smart contracts. Over the last decade, there are several MNC's that backs up many start-up companies for Blockchain-based projects. At present, companies of various domains are researching to find the possible use-case to fit in Blockchain so that maximum benefits can be achieved. However, many Blockchain-based solutions are still in the pilot stage and need more research and regulations to standardize. FinTech, Supply-chain, Healthcare, IoT, Decentralized storage, smart contracts are some of the most researching areas of Blockchain.

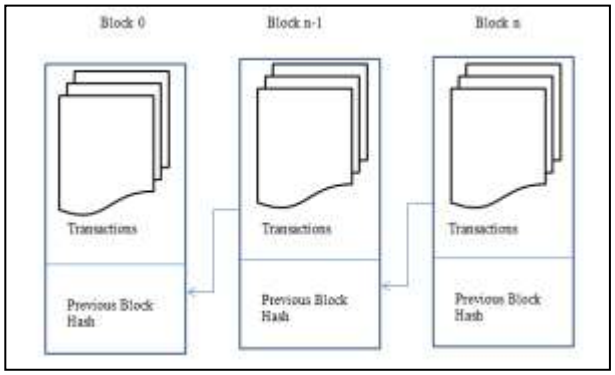


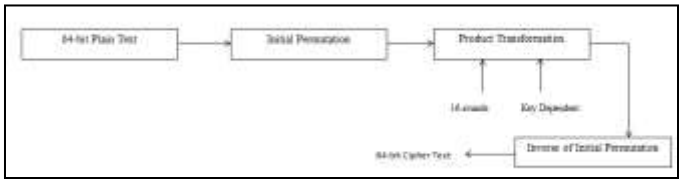
Fig. 1. A Simple Blockchain Architecture.

B. Related Knowledge on Cryptography

Cryptography came into existence even before the age of computing. In ancient times, a simple cryptography algorithm called Caesar cipher is used to transmit messages. In Caesar cipher, each alphabet will be replaced by a letter three places after that. For example, A becomes D, B becomes E, and so on. The message remains private as long as the system used in creating the ciphertext remains secret. Therefore, the process of keeping information safe and protecting them from attack is termed cryptography. So, cryptographic algorithms are introduced with encryption keys to decrypt the secret messages. These methods can be easily broken by identifying the frequency of letters. Later, Enigma Machine, a system using multiple rotors, is used to generate ciphertext, which cannot be broken quickly based on letter frequency. The need for protecting business secrets gave rise to the development of the Data Encryption Standard (DES) by IBM. As the computing power increases, Advanced Encryption Standards (AES) are developed due to inadequacies of DES. Encryption has become an integral part of everyday life, which is also the backbone of cryptocurrencies. Although many of the cryptography algorithms become obsolete, Blockchain uses hashing, public-key cryptography, and Merkle Tree cryptographic methods [3].

1) Symmetric encryption: Two popular methods used to encrypt the data are Symmetric and Asymmetric encryption. Symmetric key algorithms are traditional encryption algorithms. It uses a single private key is used to encrypt and decrypt a message. Symmetric algorithms needed both the sender and the receiver to agree upon the private key before information exchange. Symmetric methods are faster compared to asymmetric methods. Nevertheless, the algorithm's security depends on keeping the key secret. If the key is lost, the encryption algorithm can be cracked easily. Also, by using a complex mathematical formula on an encrypted plaintext, it is possible to find the key used to decrypt the plain text. The symmetric key algorithms are of two types Sequence and packet encryption algorithm. In a sequence encryption algorithm at a time, a single bit of data is encrypted, whereas a set of bits is encrypted in packet encryption. DES algorithm, a popular symmetric encryption scheme, uses the conventional form of Encryption, block cipher. The general process of the DES encryption technique is shown in Fig. 2.a, whereas the detailed internal process is shown in Fig. 2.b.

The plaintext has to be transformed, and the block containing the information will be divided into two parts and then is transformed by a function f. It will be repeated 16 times. The two parts of the information are combined after product transformation. An inverse transformation will be applied to the combined information. As an example, the original first reverse transformation, the left shifted message is 48 bits, and then the existing 32-bit value is replaced by the final result instead of the substitution result. The substitution operation is done as per the steps above. The method mentioned above is the execution cycle of the function f, and the output is XOR worked with the left part, replacing the current output with the actual part. The DES encryption method was finished after 16 run cycles. The same algorithm is used for decryption as well. The key must be in reverse, while decrypting is the only difference. A circular key is generated for every circle by DES, and transfers for relocation to the right in turn [5]. One of the significant drawbacks of symmetric algorithms is weak keys. The weak key is the one that contains all 0's, all 1's or half 0's, and half 1's after symmetry drop operation. The weak key allows the attacker to decipher the DES encryption at a reduced time.



(a) A High-Level view of a Symmetric Encryption Method.

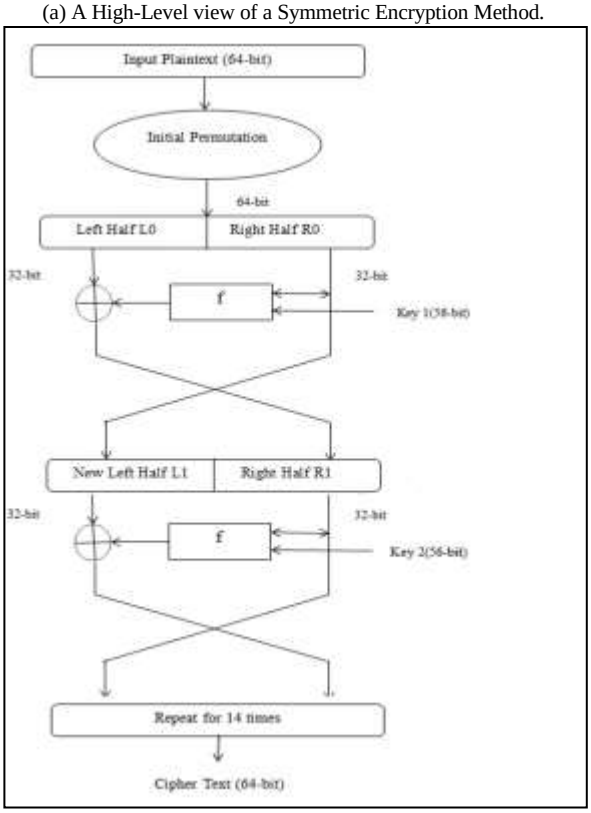


Fig. 2. (b). Internal Process of DES Encryption Algorithm [4].

2) Asymmetric encryption: The Asymmetric Encryption was developed to resolve the problems of symmetric key algorithms. It is otherwise called as public-key cryptography. In asymmetric Encryption, two different keys name public and private keys are used in encryption and decryption process. Both the keys are mathematically linked. The public key is used in the encryption process, and it can be decrypted using the private key. The security of the network is assured by two unrelated keys in public-key cryptography. The process of public key Encryption and decryption can be denoted by the equation below.

$$\text{EncryptKey1(Plaintext)} = \text{Cipher} \quad (1)$$

$$\text{DecryptKey2(Cipher)} = \text{Plaintext} \quad (2)$$

$$\text{DecryptKey2(EncryptKey1(Plaintext))} = \text{Plaintext} \quad (3)$$

3) Comparison between symmetric and asymmetric key encryption: Both symmetric and asymmetric key Encryption has its advantages and disadvantages. In a secure transmission, the symmetric key algorithm is highly efficient, whereas efficiency is relatively low in public key cryptography. Though the use of two different keys in the asymmetric method significantly improves the security process, there is a decline in the transaction speed when compared with symmetric methods [6]. Thus, the combination of the public key and symmetric key gave rise to digital envelopes for transmitting data safely. It allows the data to be encrypted as fast as symmetric key and as secure as the public key.

III. The Convergence of Cryptography and Blockchain Network

Blockchain Technology is a combination of a peer-to-peer network, cryptography, and Game Theory. Blockchain uses cryptography in various ways, especially security and privacy mechanisms [7]. Enabling digital signatures, wallets creation, secure and transparent transactions are some of the areas where Blockchain uses cryptography. Some of the essential cryptographic techniques used in Blockchain are Hashing, Digital signatures, and Merkle Trees [8].

Fig. 3 summarizes the different cryptographic components included in Blockchain.

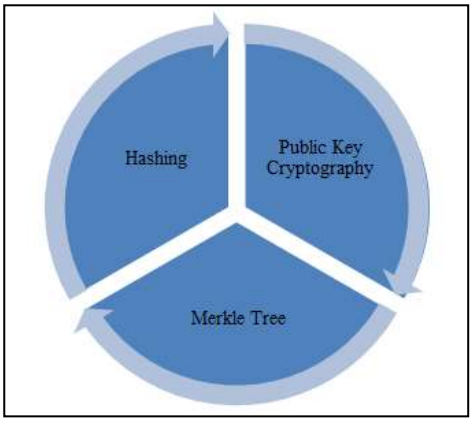


Fig. 3. Role of Cryptography in Blockchain.

A. Hashing Mechanism

Hashing is a cryptographic method in which any kind of data is converted to character strings. Hashing not only provides security, but it also provides efficient storage of data as the size of hashing output is fixed. Any hash algorithm, only if it confirms specific properties, it can be used for providing security services. These properties are not inherently provided by any general-purpose hash functions. This is the reason why algorithms like SHA-2 are considered as cryptographic hash functions. Some of the critical features of hashing are the one-way or pre-image resistance nature, which is why it always produces the same output for the same input. Also, by using hashing output, it is impossible to deduce the input. The second pre-image resistance property assures that no two different messages can have the same hash value. Any minor change in the input also creates an entirely different hashing output, and no two inputs can ever produce the same hash output. This is due to the collision resistance property of the hashing function [9]. The only concern of hashing is that generating hash values should be fast and should not use much computing power. The hashing algorithm used in bitcoin blockchain is SHA-256. SHA-256 is a part of the SHA-2 cluster and generates a 256 bits or 64 hexadecimal characters output. Refer Fig. 1 of blockchain architecture, which shows how the blocks are connected using the hash of the previous blocks.

SHA-256 algorithm follows a two-phased approach: pre-processing of the message and main loop. In the first phase, i.e., the message pre-processing phase, the process of filling the message length and binary bit on any message length is performed. Later, the messages are split into many 512 bit message blocks. In the second phase, a compression function processes the entire message blocks of phase-I. In other words, the input of a new compression function is the output of the previous compression function, and the output of the final compression function is the hash of the final message.

In Blockchain, each transaction is hashed and bundled together in blocks, and each block is connected to the predecessor block using a hash pointer, i.e., the hash of all information of every previous block is stored in the Header of every block. Hashing is responsible for Blockchain's distinct feature of immutability and is used for verifying any transaction's integrity. This can be achieved by comparing the calculated hash with the stored hash value in the block header. Once the public keys are generated using ECDSA, a set of hash functions are applied to the key to generating a unique hash address. The public-private key pairs can also be generated using a hash function [10].

The block view is given in Fig. 4. A block contains a block header and a block body. The Header includes many data like the hash value of the previous block, nonce- a random number, timestamp, target value, and Merkle root. The block body includes the set of all transactions in the block. Prev Hash: It is the hash value of all the information of the previous block. This also assures the integrity of the previous block data. Nonce: A random number whose initial value is 0. The bitcoin node always conducts an SHA-256 procedure on the block's total data. If the SHA-256 value determined by the current random number does not satisfy the criteria; instead,

one unit reduces the random number and the SHA-256 operation proceeds. A new data block is created and approved by the P2P network if the value of SHA-256 is smaller than the current block's SHA-256 value. This process of block generation is called Proof-of-Work (PoW). Timestamp: This is the time at which the data is written in the block. The data blocks are arranged in chronological order based on the timestamp on the header block. Target: A target hash is a value that a hashed block header needs to be below or equivalent to in order to create a new block. The SHA-256 value in the block determines the target value. Merkle Root: Merkle tree is a hash tree to verify the integrity of a large amount of data. Transaction List: All information about the transactions like Payer, Receiver, Timestamp, the amount transferred, transaction id, etc.

The usage of the hashing mechanism in Blockchain is categorized into the following. Address generation, Proof-of-Work(PoW), Block generation, Random number generator, Message Digest (MD) signatures, and bridge components [11].

Due to the advancements in the mining techniques, the possibility of having 51% attacks [12] is increasing, thereby giving rise to new hashing mechanisms. It is well known that SHA-256 is the hashing algorithm used in Blockchain. Some of the other popular hashing algorithms are SCrypt, a memory hard hash function used in Litecoin, Fairbrix and Tenebrix [13], X11, which is used in Darkcoin is a combination of 11 hash functions taken from SHA-3[14], Equihash, another hard memory function proposed by [15] and Ethash an ASIC-resistant hash function widely adapted in Ethereum based cryptocurrencies [16].

B. Digital Signatures

Digital Signature is an Asymmetric Cryptographic method, specifically public key Encryption. Unlike symmetric cryptography, where the same key is used by both the sender and receiver asymmetric method uses a pair of the key is connected by cryptography. If user A wants to prove certain information is authentic and wants to maintain data integrity, then he/she can digitally sign the information and can transmit over the network. In bitcoin, digital signatures are used to make cryptocurrency transactions. To create a digital signature, the information to be sent will be processed by a hashing algorithm to generate unique strings. Later, these strings can be digitally signed using user A's private key. In more straightforward ways, the digital signature is a combination of hash code and the private key of the user. Moreover, to verify, the user's public key can be used to check the authenticity of the user as well as the data. Fig. 5 shows the sending and verification of digital signatures. Elliptic Curve Digital Signature Algorithm (ECDSA) and RSA are some of the algorithms used in generating the public and private key pairs. DSA's elliptic curve version, ECDSA, is widely used in blockchain implementation as it provides many benefits, such as decreased key size and quicker calculation compared to other discrete algorithms based on logarithms and factoring algorithms based on modules[17]. Relevant domain parameters specify elliptic curves are ideal for cryptographic operations [18]. A variety of such curves are available, and few are standardized by NIST, IEEE, ANSI, and others.

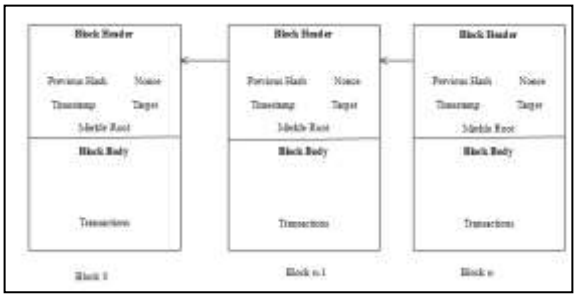


Fig. 4. Structure of a Block.

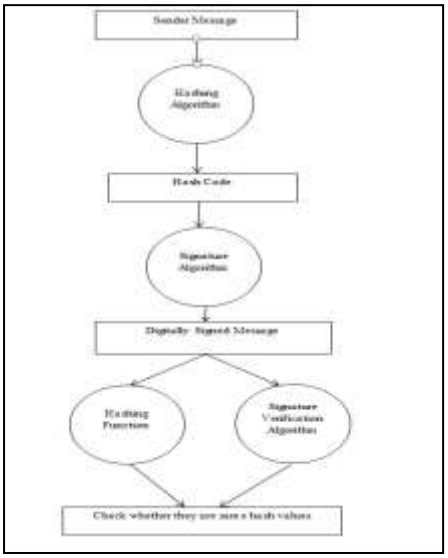


Fig. 5. Signing and Verification of Digital Signatures.

C. ECDSA

The digital signature scheme used in bitcoin blockchain for signing the transaction is the Elliptic Curve Digital Signature Algorithm, i.e., ECDSA [19]. The standard "secp256k1" elliptic curve algorithm is used in Blockchain. Secp256k1 is built on a finite field with an elliptic curve. Its engineered design will produce an advantage of 30 percent over other curves due to its unique structure. The sep256k1 constant will effectively eliminate loophole possibilities. ECDSA is immune to 'chosen-message attack,' where a genuine entity E intends to fabricate a valid signature on an unknown message m, once the attacker acquired the signature of the entity E by posting a set of queries to a collection of messages (other than m).

It is known that Blockchain uses public/private key pair. The public key encryption method is used to generate key pairs. A private key is a random number, whereas the public key is generated by encrypting private keys using the elliptic curve multiplication technique. A public key generates the bitcoin address of a user through a single entry encrypted hash function. The private key is created by selecting a random number between 1 and 2^{256}. The number should be selected in such a way that it should not repeat and predicted easily. In bitcoin to generate the 256-bit random number, the random number generator of the OS is used. This generated random number is the private key k. The private key k is multiplied with the defined generation point G of the curve to get another

point in the curve. That would be the corresponding public key K. The connection between K and K is static in a uni-directional way. In other words, it is possible to detect K from k but not the other way. Several algorithms are used in different cryptocurrency platforms to generate addresses. For instance, SHA-256 and RIPEMD160 are used in Bitcoin, whereas Keccak 256 is used in Ethereum [20].

D. Merkle Trees

Merkle tree is a method of hashing a considerable amount of data that is divided into small blocks, and each block is hashed and is combined and re-hashed again with another block to generate a combined hash. This is a repetitive process and will be continued until a single hash code is achieved from a group of blocks. Refer Fig. 6 below for a Merkle tree representation.

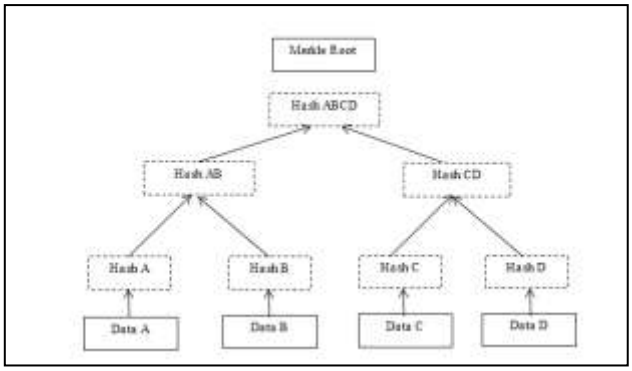


Fig. 6. Representation of a Merkle Tree.

Merkle tree uses a hashing mechanism and stores the hash output rather than storing the data itself. The Merkle root is the root node of a Merkle tree, which has the combined hashes of the left and right sub-trees. Since each block holds the hash value of the previous block, the data in Blockchain is unchangeable [21]. A double SHA-256 hash algorithm is used in the Bitcoin blockchain. In other words, the original data of any length is applied to two SHA256 hashing operations. For uniform identification and storage, a 256-binary digit is used. Various cryptographic algorithms are used by different Blockchain. SHA-256 is being used by Bitcoin blockchain. Ethereum uses Keccak256, whereas Litecoin and Dogecoin use a lighter and faster cryptographic algorithm Scrypt. Hashing helps in ensuring the integrity of the data in Blockchain.

IV. Possible Security Attacks on Blockchain

Despite its nature to secure data, Blockchain is susceptible to different security-related attacks [22][23]. Fig. 7 shows the various security attacks on a blockchain network, and possible solutions for those attacks are listed in Table I.

A. Key Attacks

1) Cryptographic algorithm attacks: The elliptical curves used in Blockchain cryptographic operations are derived using parameters that may be compromised and can allow an attacker to know the secret numbers to break the encrypted messages of 32-bit size [24].

2) Hashing attacks: Most of the blockchain implementations use the SHA-256 algorithm as it is considered to be secured. However, SHA algorithms can be attacked by length extension attacks. Through this attack, one can add intruder-controlled data to digitally signed information and can change the hash of the message without revealing the shared information. Hashing algorithms are also prone to birthday attacks in which the collision resistance property of the hashing can be broken [26].

B. Identity Attacks

1) Sybil attacks: In Blockchain, few specific nodes will be identified as the target node, and the intruder will not relay any transactions to and from the target node and deploys double-spending attacks using the target nodes.

2) Impersonation attacks: Imitating like honest nodes to gain access.

3) Replay attacks: Communication between two genuine users is imitated by the intruder to gain access and steal the hash key. Reusing the hash key makes the intruder an authentic user.

C. Manipulation Attacks

1) Eclipse attack: A particular node will be identified and will be isolated from the network and will not get any transactions or blocks from the rest of the network. The intruder will waste the resources of the target node or use it for malicious activities [31].

2) Transaction malleability: It is a bitcoin design issue where the transactions can be changed after creation but before getting added to a block. Information like sender and receivers address, money transferred will not be changed, but data like transaction id can be modified. As the transaction id gets changed, it is not possible to validate the transactions, and attackers can withdraw money transferred.

3) TimeJacking attacks: Timejacking is an attack that aims to bias the timestamp of a target node by linking several peers to a target and transmitting an incorrect time to the target. This lets the node to reject transactions due to wrong timestamps. It is thereby letting the malicious user to do fraudulent transactions.

Fig. 7. Various Blockchain Security Attacks.

TABLE I. SUMMARY OF SECURITY ATTACKS IN BLOCKCHAIN

Category	Attacks	Solution
Key Attacks	Cryptographic Algorithm Attacks	Use cryptographically secure random number generator
	Hashing Attacks	Use double SHA-256 [25]
Identity Attacks	Sybil Attacks	Create unchangeable chains where interactions between users are assessed periodically [27].
	Impersonation Attacks	Use Feature-based Signatures and distributed incentives approach [28][29].
	Replay Attacks	Use elliptic curve based Encryption or have one-time private-public key pairs [30]
Manipulation Attacks	Eclipse Attack	
	Transaction Malleability	
	TimeJacking Attacks	Several countermeasures suggested like time monitory, network encryption, checking the node connection diversity [32].
Reputation Attack		No proper approaches yet
Service Attacks	Race Attacks	Hold till at least a minimum number of confirmations are received.
	DDoS Attacks	No standard solutions yet.
	Double Spending Attacks	
	Finney Attacks	Wait for more confirmation.
	Vector 76 Attacks	
	Collusion Attacks	
Malware Attacks		
Application Attacks	Design Errors	It is fixed by dividing Ethereum Blockchain into Ethereum Classic and Ethereum. Better desi.gn
	Coding Errors	Better design and coding principles

D. Reputation Attack

Act of changing the reputation of a user from bad to good. This can be done by having a new account or by hiding the fraudulent transactions.

E. Service Attacks

1) Race attacks: Malicious users create two transactions one genuine and one false. Any node which takes zero confirmations (a transaction yet to be included in the block) is then targeted, and the false transaction is directly sent to the target, whereas the genuine transaction is sent to the pool. The target may approve the transaction that is not genuine and may provide the service.

2) DDoS attacks: The network may be seized, and a vast amount of service requests may be sent that the network may not be able to handle [33].

3) Double spending attacks: By bribing the significant number of nodes, a user may be able to spend the assets more than once.

4) Finney attacks: These are the continuation of double-spending attacks, where the attacker adds all his internal transactions to his block and releases only when he finishes double-spending them by zero-confirmation methods.

5) Vector 76 attacks: A mixture of Finney and Race Attacks.

Collusion Attacks: Popularly it is the 51% attack where more than 51% of the network resources are compromised or controlled by a single source. This enables any malicious activity to take place within the network.

F. Malware Attacks

It is a standard attack in pocketing cryptocurrencies. This can get into Blockchain by mining software or storing some arbitrary data along with immutable data. Leads to several other attacks like DNS, Man-in-the-Middle Attacks [34].

G. Application Attacks

1) Design errors: The design of the Decentralized Autonomous Organization (DAO) allows the users to take their money out or put them in a separate DAO. This system was later hacked and led this feature to repeatedly put the funds in child DAO but before the actual fund transmission.

2) Coding errors: A bug in coding led to the attacks of wallets.

V. SECURITY AND PRIVACY SERVICES OF BLOCKCHAIN

Every node in the blockchain network maintains a copy of the Blockchain, and a miner is the one who creates and validates the block. A Blockchain network is a peer-to-peer network that verifies itself and eliminates the third party for verification. It offers rewards to the network nodes that do the validation process honestly. This process of validating the transactional data is called mining. The Blockchain uses concepts like Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Space (PoSpace), Practical Byzantine Fault Tolerance (PBFT), etc. based on a hashing scheme to validate the data. A cryptographic puzzle has to be solved by a network and then broadcasts the results to the network for verification to include a timestamp to the network. This proof-of-work concept keeps the network authentic. The SHA-256 algorithm is used in PoW as it is comparatively complex to solve but can be verified easily. The variety of security and privacy services offered by Blockchain are listed below [35].

A. Services of Encryption and Authentication

1) Traditional systems: The vital security services that any network can offer are Authentication and Encryption. This can be achieved by using public-key cryptography (PKI) framework. Of all the security services offered by PKI, user authentication, and message confidentially are the most severe service in all network applications. User authentication can be done by having digital signatures and confidentiality by using simple encryption/decryption techniques [36]. It is well known that traditional PKI systems use a trusted third-party certificate

authority (CA) to manage the key distribution. Another approach is Web of Trust (WoT), which follows a decentralized approach by locally generating the key and verified by a trusted third-party. Some of the challenges of these traditional PKI systems are security, cost, and centralized system. Security of generating and distributing the key is at risk if the trusted third-party (CA) is negotiated. Since there is a central system involved the risk of a system failure leading to data loss and increased cost for maintenance by a single entity. On the other hand, in WoT systems to join a network, the users have to create trust with the existing users, who might be a difficult task for new users. Moreover, both the traditional systems lack in identity retention, i.e., it lets the users impersonate the identity of a user who already registered in the network.

2) Current Blockchain-based PKI

3) Authentication services through Encryption

The drawbacks of traditional PKI systems can be resolved by Blockchain-based PKI. Since Blockchain is distributed in nature, it does not need a centralized repository of data. Prior trusts among the users are not necessary as the trust is created based on the majority of votes by the nodes (miners) [37]. Blockchain has many open-source implementations leading to economical and efficient solutions. Several approaches are followed to attain Blockchain-based PKI solutions.

a) Instant Karma PKI: The traditional CA approach is extended in this approach, where the activity of CA is recorded in Blockchain. This helps to identify the compromised CA's, thus eliminating trust related issues of the traditional PKI system. However, including a CA still creates a dependency on the third party.

b) Distributed PKI: Distributed PKI uses a web-based domain registration system in which the user generates the private and public key pair, and as a transaction, the public key is registered in the Blockchain. This approach avoids the man in the middle attacks by connecting the identity of the user with the latest key of the user [38].

c) Gan's Approach: A key based verification system exclusively for IoT environments is proposed by Gan [39]. This aims to have a private blockchain to store the nodes' public keys and validating them. It includes a centralized CA which is connected to some validators who are responsible for generating the keys and maintaining the blockchain database. The IoT devices are connected to these validators. This is a cyclic process where a validator brings in the public key of an IoT node, gets it validated, and signed through the CCA and records the transaction on Blockchain. However, this approach as well suffers the central point of failure due to a centralized CA.

d) Blockstack: Namecoin [40], a division of bitcoin, is used here to develop a distributed PKI system. Namecoin enables data storage in blockchain transactions. This system uses a name-value pair to record the user names and will be stored in the Blockchain. Blockcstack modifies the Namecoin system by including the public key as another name-value pair. Similar to Namecoin, Certcoin [41], another decentralized network is used for identity retention services.

e) Blockchain-based IBC: Identity-based cryptography techniques need a centralized system to generate private keys. Hence, if this central system is compromised, the entire system can be compromised. This problem of centralization can be resolved by using a Blockchain-based approach as it adapts a decentralized approach. Since users can generate their keys in the blockchain network, there is no need for a central system to generate the key pairs.

B. Services of Confidentiality

A privacy service lets the user set the control and accessibility of the data by the network. It enables complete ownership of the data. Data privacy is more important in the case of networking systems as the network is shared by many users.

1) Traditional techniques: In general, data privacy can be achieved by defining Access Control List (ACL) where the user lists who can access what information and when. An encryption technique, like homomorphic Encryption [33], can be used to prevent unauthorized access. Another traditional approach is Data anonymization, where the user's identity can be hidden and hence not possible to link them with the data. Some of the techniques to achieve data anonymization are K-anonymity, T-closeness, and L-diversity. Although several approaches are available to assure data privacy, there are few drawbacks like scalability, efficiency, lack of ownership, and methodical lifecycle approach, which cannot be overlooked.

2) Blockchain-based privacy: The decentralized data privacy based on Blockchain can resolve the drawbacks of traditional systems. It guarantees complete ownership of data by the users and enables a dynamic ACL as and when needed. Blockchain-based systems are highly dependent on cryptographic techniques; hence they are still challenging to implement. The objective of data privacy based on Blockchain is to construct a layer named the blockchain layer above the data storage layer [42]. This allows the users to define their ACL and publish them through smart contracts. This enables the data to be stored as blockchain transactions which are encrypted. Therefore, no central entity can own the data as in traditional systems. Nevertheless, the data can be accessed if they are part of the blockchain network and only if the ACL allows them. Some of the privacy preserving techniques based on Blockchain are listed below:

a) Zyskind's Technique: This is a decentralized approach in which data and ACL are stored in blocks of the Blockchain, and the user (owner) is provided complete access to it. The user can send ACL and data as a transaction over the blockchain network and will be verified by the nodes of the network. Whenever some other user needs to access the data, a request can be sent to the network and can receive an encrypted response only if he has given access to ACL.

b) Fair Access and IoT: Fair access is a decentralized, pseudonymous privacy preserving mechanism that enables the user to access and control their data. Through Fair-Access, a

user can grant, receive, request, and revoke access through smart contracts.

C. Data Integrity Services

Integrity means that data is correct and valid. This property guarantees that data have not tampered when stored or during transmission. In Blockchain, the data can be the ones that are stored, produces, and accessed by the network. Integrity in Blockchain is assured by digital signatures and public-key encryption methods [43].

1) Traditional techniques: Currently, using data replication techniques and cryptographic tools, data integrity is maintained. Cryptographic tools can be public-key cryptography and digital signatures, which will not allow any unauthorized person to access the information. It is possible to identify whether the data has been modified by using any signature verifying technique. Keeping the keys secret is the main task in traditional methods, but if the key is identified once, it is not possible to foresee the attacks that can happen [44].

In traditional techniques, identifying an intruder in case of an attack is a severe problem. This is because intrusion could have happened anywhere, like transmission, processing, or storage. The need to identify the intruder can be various like to detect the kind of mischievous activities, to modify the access mechanism, or to punish the intruders. Dependency on a third party is another factor where trust can be an issue. Also, integrity is another added security that would need additional resources and adds complexity to the system.

2) Blockchain based integrity: Blockchain has built-in integrity checks where the sender signs the transactions, and a miner verifies it. It is known that data, once saved in Blockchain, is tamper-proof forever, thereby assuring integrity. For IoT devices, a specialized framework for data integrity has been proposed [45]. The objective of this framework is to store the encrypted hash values of user data on Blockchain. Later, the hash values can be used to verify integrity. Another approach is Storj, a P2P system used for storage. It stores the hash values of the blockchain database, which is immutable and ensures data integrity.

VI. Applications of Blockchain Technology

Decentralized nature, immutability and the security services feature of blockchain makes the technology to dive in various domains. Many industries currently focusing to identify an appropriate use case for Blockchain to fit in. Some of the major areas where Blockchain is applied other than Financial services are Education [46], Healthcare [47], Supplychain, IoT [48], Data Management and security services [49], Energy sector [50] and so on. The wide variety of applications where Blockchain can be adopted is shown in Fig. 8.

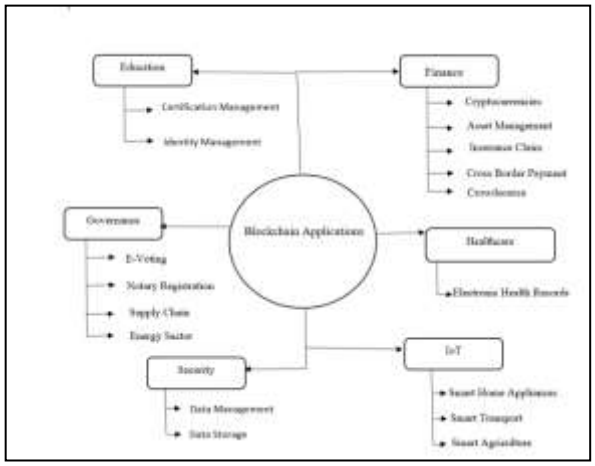


Fig. 8. Applications of Blockchain Technology.

VII. Challenges of Blockchain Security

A. Scalability

Many of the blockchain implementations have scalability issues due to the block size and the approximate time taken to publish the blocks. Few types of research suggest enhancing the scalability by increasing block size. More transactions can be accommodated if the block size is increased [51]. However, increasing block size delays the propagation speed. However, as per the discussion in [52], the current propagation techniques are not optimized and increase the risk of several attacks. So if the block size increment decreases the block propagation speed, it may increase the possibility of more attacks. Another countermeasure for this scalability problem is SegWit. SegWit, otherwise called Segregated Witness, creates a certain amount of space in a block by separating the data used for verifying the transactions. i.e., signature data and transaction data. However, this approach alone cannot suffice to handle Blockchain's scalability issue.

B. Privacy

As discussed before, bitcoin and several other cryptocurrencies, though considered to be anonymous they genuinely are not [53]. It may not be easy but not impossible to find the real identity of the user using their transaction history. Thus, they can be termed as pseudonymous. There is some software available to de-anonymize the cryptocurrencies. The possible approach to solve this privacy issue has CoinJoin services. CoinJoin combines several accounts and then transfers the coin in a pseudo-random manner and makes the transaction anonymous. Ethereum blockchain, where smart contracts and DApps are used, are highly susceptible to privacy issues. To keep the smart contracts, secure and anonymous many methods are suggested by V Buterin in [54].

C. Computations and Time Consumption

Majority of the applications that are currently used are simple and does not require high computational resources, whereas blockchain client needs very high computational abilities to handle the mining activity. Providing any security service needs quick processing capabilities, but in Blockchain, the consensus mechanism and mining process is time-

consuming [55]. However, this issue has been addressed in Ethereum and Hyperledger platforms but still needs many improvements to handle this issue.

VIII. Discussion

In this paper, a comprehensive study on the cryptographic techniques with a specific emphasis on blockchain technology and related security and privacy aspects of it. We have provided in the survey the cryptographic techniques that are included in blockchain and an in-depth study on various attacks on the blockchain network. We have also presented a detailed investigation of various security and privacy services of blockchain. The application areas and the challenges of the technology are also briefly discussed in this paper. The paper included referrals from peer-reviewed works aiming to provide a detailed insight of the blockchain technology from the security perspective.

IX. Conclusion

In the past decade, Blockchain Technology is the interesting inventions of cryptography and information & communications. This paper presents the evolution of cryptographic mechanisms and the different cryptographic methods used in Blockchain. The various security attacks aimed at Blockchain are also discussed. The different security services offered for authentication and privacy and the challenges of Blockchain are discussed in brief. This study highlights that blockchain implementations are majorly based on the cryptographic concepts and provides a roadmap for future developments in blockchain technology. Thus, it can be concluded that cryptography plays a major role in the internal functioning of blockchain technology. The foundation for blockchain transactions and wallets are based on public-key Encryption, and the use of cryptographic hashing mechanism along with Merkle tree concepts enables the immutable nature of Blockchain and providing a high-end security.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976. DOI: 10.1109/TIT.1976.1055638.

[2] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Accessed: February 13, 2018. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf.

[3] Xiaochun Yun • Weiping Wen Bo Lang • Hanbing Yan • Li Ding Jia Li Yu Zhou (Eds.), Cyber Security, 15th International Annual Conference, CNCERT 2018, Beijing, China, August 14–16, 2018 , doi.org/10.1007/978-981-13-6621-5.

[4] W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed. Prentice-Hall, 2005.

[5] J. Shivani and Ranjan Senapati. “Robust Image Embedded Watermarking Using DCT and Listless SPIHT.” Future Internet, vol. 9, no. 3, July 2017, p. 33. DOI.org (Crossref), doi:10.3390/fi9030033.

[6] Aparna, Puvvadi, and Polurie Venkata Vijay Kishore. “An Efficient Medical Image Watermarking Technique in E-Healthcare Application Using Hybridization of Compression and Cryptography Algorithm.” Journal of Intelligent Systems, vol. 27, no. 1, Jan. 2018, pp. 115–33. DOI.org (Crossref), doi:10.1515/jisys-2017-0266.

[7] Sheping Zhai, Yuanyuan Yang, Jing Li, Cheng Qiu, Jiangming Zhao. "Research on the Application of Cryptography on the Blockchain," Journal of Physics: Conference Series, 2019, DOI:10.1088/1742-6596/1168/3/032077.

[8] S. G. Aruna Sri, P., and D. Lalitha Bhaskari. “A Study on Blockchain Technology.” International Journal of Engineering & Technology, vol. 7, no. 2.7, Mar. 2018, p. 418. DOI.org (Crossref), doi:10.14419/ijet.v7i2.7.10757.

[9] R. Martino and A. Cilardo, "SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey," in IEEE Access, vol. 8, pp. 28415-28436, 2020. DOI: 10.1109/ACCESS.2020.2972265.

[10] Sahu, Aditya Kumar, et al. “Digital Image Steganography Using Bit Flipping.” Cybernetics and Information Technologies, vol. 18, no. 1, Mar. 2018, pp. 69–80. DOI.org (Crossref), doi:10.2478/cait-2018-0006.

[11] Wang, Licheng, Xiaoying Shen, Jing Li, Jun Shao, and Yixian Yang. "Cryptographic primitives in blockchains." J. Netw. Comput. Appl. 127, (2019): 43-58. https://doi.org/10.1016/j.jnca.2018.11.003.

[12] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, Mohammed Samaka. "SecurityServices Using Blockchains: A State of the Art Survey," IEEE Communications Surveys & Tutorials, 2019, DOI: 10.1109/COMST.2018.2863956.

[13] Krawczyk H. (2010) Cryptographic Extraction and Key Derivation: The HKDF Scheme. In: Rabin T. (eds) Advances in Cryptology – CRYPTO 2010. CRYPTO 2010. Lecture Notes in Computer Science, vol 6223. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-14623-7_34.

[14] E. Duffield and K. Hagan, "Darkcoin: Peer-to-peer crypto-currency with anonymous blockchain transactions and an improved proof-of-work system," Mar. 2014 [Online]. Available: http://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf.

[15] Biryukov, Alex, and Dmitry Khovratovich. "Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem." IACR Cryptology ePrint Archive 2015 (2015): 946. DOI: https://doi.org/10.5195/ledger.2017.48.

[16] Q. Zhou, "Irregular-Program-Based Hash Algorithms," 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 2019, pp. 125-128. DOI: 10.1109/DAPPCON.2019.00024.

[17] Li, Xiaoqi et al. "A Survey on the Security of Blockchain Systems." ArXiv abs/1802.06993 (2018): n. pag. https://doi.org/10.1016/j.future.2017.08.020.

[18] Certicom-Research, 2000. Sec2: Recommended Elliptic Curve Domain Parameters. http://www.secg.org/SEC2-Ver-1.0.pdf.

[19] Johnson, D., Menezes, A. & Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA). IJIS 1, 36–63 (2001). https://doi.org/10.1007/s102070100002.

[20] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564. DOI: **10**.1109/BigDataCongress.2017.85.

[21] R.C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," Advances in Cryptology — CRYPTO '87, Springer, 1987. DOI:10.5555/646752.704751.

[22] Dasgupta, D., Shrein, J.M. & Gupta, K.D. A survey of Blockchain from the security perspective. J BANK FINANC TECHNOL 3, 1–17 (2019). https://doi.org/10.1007/s42786-018-00002-6.

[23] A. Averin and O. Averina, "Review of Blockchain Technology Vulnerabilities and Blockchain-System Attacks," 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, Russia, 2019, pp. 1-6. DOI: 10.1109/FarEastCon.2019.8934243.

[24] Schneier on Security (2007) Retrieved November 1, 2018, from https ://www.schne ier.com/essay s/archi ves/2007/11/did_nsa_put_a_secre t.html.

[25] M. Raikwar, D. Gligoroski and K. Kralevska, "SoK of Used Cryptography in Blockchain," in IEEE Access, vol. 7, pp. 148550-148575, 2019. DOI: 10.1109/ACCESS.2019.2946983.

[26] N. Anita. and M. Vijayalakshmi., "Blockchain Security Attack: A Brief Survey," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-6. DOI: 10.1109/ICCCNT45670.2019.8944615.

[27] Keutmann (2018) Keutmann/Trustchain. Retrieved November 1, 2018, from https://githu b.com/keutm ann/Trust chain.

[28] Wang Q, Qin B, Hu J, Xiao F (2017) Preserving transaction privacy in bitcoin. Future Generation Comput Syst. https://doi.org/10.1016/j.future.2017.08.026.

[29] Choo R, He X, Lin C, He D, Vasilakos AV (2018) Bsein: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Netw Comput Appl 116:42–52. https://doi.org/10.1016/j.jnca.2018.05.005.

[30] Huang X, Xu C, Wang P, Liu H (2018) LNSC: a security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE Access 6:13565–13574. DOI: 10.1109/ACCESS.2018.2812176.

[31] L. Wan, D. Eyers and H. Zhang, "Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 194-201. DOI: 10.1109/Blockchain.2019.00033.

[32] Maria A, Zohar V (2017) Hijacking bitcoin: routing attacks on cryptocurrencies. In: IEEE symposium on security and privacy, pp 375–392. https://arxiv.org/abs/1605.07524.

[33] A. A. Andryukhin, "Phishing Attacks and Preventions in Blockchain-Based Projects," 2019 International Conference on Engineering Technologies and Computer Science (EnT), Moscow, Russia, 2019, pp. 15-19. DOI: 10.1109/EnT.2019.00008.

[34] Arunima Ghosh, Shashank Gupta, Amit Dua, Neeraj Kumar, Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects, Journal of Network and Computer Applications, Volume 163, 2020,102635, https://doi.org/10.1016/j.jnca.2020.102635.

[35] Leiyong Guo, Hui Xie, Yu Li, Data Encryption based Blockchain and Privacy-Preserving Mechanisms towards Big Data, Journal of Visual Communication and Image Representation, 2019, 102741, https://doi.org/10.1016/j.jvcir.2019.102741.

[36] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," Proceedings 42nd IEEE Symposium on Foundations of Computer Science, Newport Beach, CA, USA, 2001, pp. 136-145. DOI: 10.1109/SFCS.2001.959888.

[37] G. Karame and S. Capkun, "Blockchain Security and Privacy" in IEEE Security & Privacy, vol. 16, no. 04, pp. 11-12, 2018. DOI: 10.1109/MSP.2018.3111241.

[38] S. Singh and N. Singh, "Blockchain: Future of financial and cybersecurity," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, 2016, pp. 463-467. DOI: 10.1109/IC3I.2016.7918009.

[39] S. Gan, "An IoT simulator in NS3 and a key-based authentication architecture for IoT devices using blockchain," M.S. thesis, Indian Inst.Technol. At Kanpur, Kanpur, India, 2017. Accessed: February 13, 2018. [Online]. Available: https://security.cse.iitk.ac.in/node/240.

[40] T. Chang and D. Svetinovic, "Data Analysis of Digital Currency Networks: Namecoin Case Study," 2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS), Dubai, 2016, pp. 122-125. **DOI:** 10.1109/ICECCS.2016.023.

[41] C. Fromknecht, D. Velicanu, and S. Yakoubov, "A decentralized public key infrastructure with identity retention," IACR Cryptol. ePrint Archive, p. 803, 2014.

[42] M. C. Kus Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2543-2585, third quarter 2018. DOI: 10.1109/COMST.2018.2818623.

[43] X. Yi, R. Paulet, and E. Bertino, Homomorphic Encryption and Applications (Springer Briefs in Computer Science), vol. 2. Cham, Switzerland: Springer Int., 2014, pp. 27–46. https://doi.org/10.1007/978-3-319-12229-8.

[44] J. Lou, Q. Zhang, Z. Qi and K. Lei, "A Blockchain-based key Management Scheme for Named Data Networking," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, 2018, pp. 141-146. DOI: 10.1109/HOTICN.2018.8605993.

[45] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in Proc. IEEE Int. Conf. Web Services (ICWS), Honolulu, HI, USA, 2017, pp. 468–475. DOI:10.1109/ICWS.2017.54.

[46] Kumar, S.M.K.V., et al. “Incorporation of Blockchain in Student Management System.” International Journal of Innovative Technology and Exploring , vol. 8, no. 6, Apr. 2019, pp. 664–68.

[47] KusumaLatha, K., et al. “Warehousing Of Medical Data Using Blockchain.” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 7, May 2019, pp. 604–07.

[48] P, Tejaswi, et al. “An Efficient Blockchain Security for Distributed System.” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 6, Apr. 2019, pp. 1265–69.

[49] Poluri, M., et al. “IOT Ecosystem with Blockchain and Smart Contracts.” International Journal of Recent Technology and Engineering, vol. 7, no. 6, Mar. 2019, pp. 638–41.

[50] Uppalapti Krishna , Tapasvi, et al. “A Framework Using Blockchain Application to Monitor & Control Logs.” Journal of Advanced Research in Dynamical and Control Systems, no. Special Issue 2, 2018, pp. 459–65.

[51] Ammbika, V. M., and D. S. Rao. “Limitations of Blockchain Technology with Its Applications.” International Journal of Recent Technology and Engineering, vol. 8, no. 2S11, Nov. 2019, pp. 3646–52. DOI.org (Crossref), doi:10.35940/ijrte.B1459.0982S1119.

[52] Decker C, Wattenhofer R (2013) Information propagation in the Bitcoin network. IEEE P2P 2013 Proceedings, pp. 1–10. DOI: 10.1109/P2P.2013.6688704.

[53] Khalilov, Merve Can Kus and Albert Levi. "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems." IEEE Communications Surveys & Tutorials 20 (2018): 2543-2585.DOI: 10.1109/COMST.2018.2818623. DOI: 10.1109/Blockchain.2019.00033.

[54] Foundation E (ed.) (n.d.) Privacy on the Blockchain. Retrieved November 01, 2018, from https ://blog.ethereum.org/2016/01/15/privacy-on-the-block chain.

[55] Junfeng Xie, Helen Tang, Tao Huang, F. Richard Yu, Renchao Xie, Jiang Liu, Yunjie Liu. "A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," IEEE Communications Surveys & Tutorials,2019. DOI: 10.1109/COMST.2019.2899617.