An Overview of Blockchain Architecture

Sweety Bakyarani. E

Assistant Professor
Department of Computer Science,
SRM Institute of Science and Technology, Kattankulathur, Chengalpattu District, India.

Abstract : Blockchain became a sensation overnight with the introduction of Bitcoin in 2008. Satoshi Takemoto the father of blockchain described Bitcoin as a "purely peer-to-peer version of electronic cash". Since then there has been no turning back for Blockchain. It has become the go to technology for decentralized and transactional data sharing across a large network of untrusted participants. It has introduced a different forms of distributed software architectures, where agreement on shared states can be established without trusting a central integration point. It helps in creating a decentralized environment, where transactions can happen without the interference of third-party organization. Every transaction is recorded permanently in a public ledger that is verifiable, transparent and secure. This is precisely one of the reasons for the Blockchains popularity. It has the potential for achieving groundbreaking changes in varied sectors ranging from finance, manufacturing sector, education and health care. This paper presents an overview of blockchain technology covering its history, architecture, also highlighting the challenges currently faced by the technology. A brief discussion on the algorithms used in blockchain-based systems and future directions of the blockchain technology is also presented.

***IndexTerms* - BlockChain, Decentralize, Consensus Algorithms.**

I. INTRODUCTION

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The PartTime Parliament [2] to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed [3]. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System [4], which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network. Nakamoto's paper contained the blueprint that most modern cryptocurrency schemes follow with variations and modifications. Bitcoin was just the first of many blockchain applications.

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion without a central repository and without a third party authority like a bank, company, or government. At basic level, they enable a community of users to record transactions in a shared ledger within that community. Under normal circumstance of operation in a blockchain network no transaction can be changed once published. In 2008, the idea of blockchain idea was combined with several technologies and concepts to create modern cryptocurrencies. Cryptocurrencies is nothing but electronic cash protected through cryptographic mechanisms instead of a central repository or authority like bank or government. The first such blockchain based cryptocurrency to be used was Bitcoin. Within the Bitcoin blockchain, information representing the electronic cash is attached to a digital address. Bitcoin users can digitally sign and transfer rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions. The Bitcoin blockchain is stored, maintained, and collaboratively managed by a distributed group of participants. This, along with powerful cryptographic mechanisms, makes the blockchain tamper proof and resilient to attempts to modifying blocks/ledgers or forging transactions.

Users utilize public and private keys to digitally sign and securely transact within the system. For cryptocurrency based blockchain networks, users may solve puzzles using cryptographic hash functions to get a rewarded which is a fixed amount of cryptocurrency. However, blockchain technology can be used for more than cryptocurrencies. Without trusted third parties, the trust within a blockchain network is enabled by four key characteristics of blockchain technology:

- **Ledger** – It maintains the full history of transaction and users can only append in the ledger. Transactions once recorded in a ledger cannot be deleted or overridden like in a traditional database.
- **Secure** – Entries in the ledger are cryptographically secured, so that tampering of the data can be prevented also the content in the ledger should be attestable.
- **Shared** – To provide transparency of all the transactions taking place the ledger is shared among the participants of the blockchain
- **Distributed** – Blockchains are inherently distributed to facilitate scaling. When the number of nodes is increased it reduces the chance that a bad actor can impact the consensus protocol.

II. BLOCKCHAIN CATEGORIZATION

Based on who determines and who can maintain the blocks Blockchain networks can be categorized into two permission model. If anyone can publish a new block, it is termed as *permissionless*. If only particular users can publish blocks, it is termed as *permissioned*. Permissioned blockchain networks is used for a group of organizations and individuals, typically referred to as a the consortium.

2.1 Permissionless

Permissionless blockchain networks are decentralized ledger platforms open to anyone publishing blocks, without needing permission from any authority. Permissionless blockchain platforms are often open source software, freely available to anyone who wishes to download them. As anyone has the right to publish blocks, anyone can also read the blockchain and issue transactions on the blockchain. Any blockchain network user within a permission less blockchain network can read and write to the ledger. This increases the risk of malicious partcipants attempting to publish blocks in a way that subverts the system. To prevent this, permissionless blockchain networks often utilize a multiparty agreement or 'consensus' system that requires users to expend or maintain resources when attempting to publish blocks. This prevents malicious users from easily subverting the system.

2.2 Permissioned

Permissioned blockchain networks are ones where users publishing blocks after being authorized by some centralized or decentralized authority . Since only authorized users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions. Permissioned blockchain networks may thus allow anyone to read the blockchain or they may restrict read access to authorized individuals. They also may allow anyone to submit transactions to be included in the blockchain or, again, they may restrict this access only to authorized individuals. Permissioned blockchain networks may be instantiated and maintained using open source or closed source software. They can have the same traceability of digital assets as they pass through the blockchain. They also use consensus models for publishing blocks, but these methods often do not require the expense or maintenance of resources as with permissionless blockchain networks. This is because the establishment of one's identity is required to participate as a member of the permissioned blockchain network; those maintaining the blockchain have a level of trust with each other, since they were all authorized to publish blocks and since their authorization can be revoked if they misbehave.

The following table summarizes the similarities and differences between the various blockchain architectures that can be adopted.

Table 2.1: Comparing Various Blockchain Architectures

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficiency (use of resources)	Low	High	High
Centralization	No	Partial	Yes
Consensus process	Permissionless	Needs permission	Needs permission

III. BLOCKCHAIN ARCHITECTURE

The structure of blockchain technology is represented as a list of blocks which describe various transactions and are arranged in a particular order. This lists can be stored as a flat file (txt. format) or in the form of a simple database. Two important data structures used in blockchain are:

- **Pointers** – Pointers are variables that keep address information of another variable.
- **Linked lists -** A sequence of blocks where each block has specific data and links to the following block with the help of a pointer.

The following are the main components of Blockchain architecture:

- Node – Refers to the user inside a blockchain, he has the copy of the ledger.
- Transaction – It is the smallest building block of a blockchain system.
- Block – It refers to the data structure used for keeping a set of transactions which is distributed to all nodes in the network
- Chain – This is a sequence of blocks in a specific order.
- Miners – These are specific nodes which perform the block verification process before adding anything to the blockchain structure.
- Consensus Protocol **-** a set of rules and arrangements that has to be followed to carry out blockchain operations.

The following is a blockchain architecture flow diagram that shows how all the above components work together in a digital wallet.

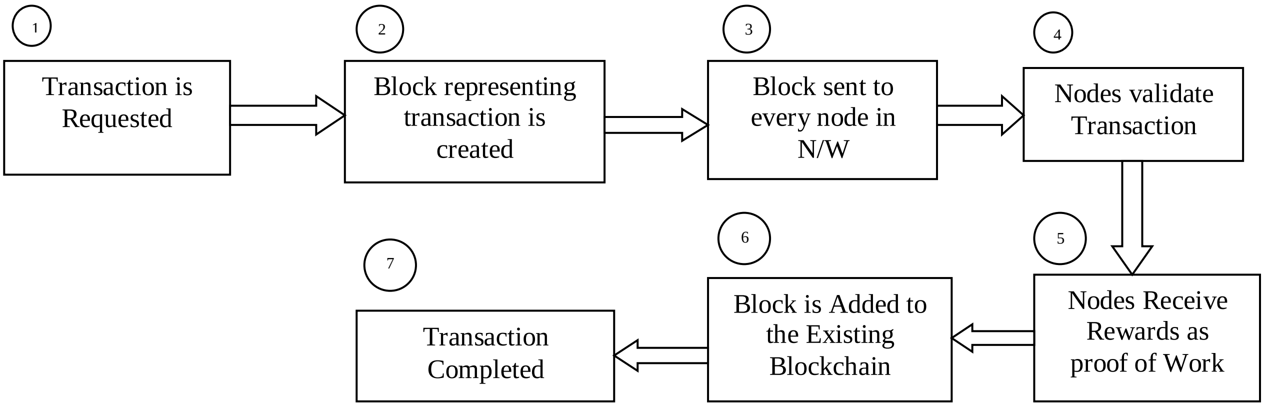
1
Transaction is Requested
2
Block representing transaction is created
3
Block sent to every node in N/W
4
Nodes validate Transaction
5
Nodes Receive Rewards as proof of Work
6
Block is Added to the Existing Blockchain
7
Transaction Completed

Fig 3.1: Working of Blockchain in a Digital Wallet

3.1. Structure of A Block:

A block is an aggregated set of data. Through mining process data is collected and processed and fitted to a block. Each block could be uniquely identified by digital fingerprint known as cryptographic hash . The first block is called as the Genesis Block. The new blocks formed will contain a hash of the previous block, so that blocks form a chain like structure. In this fashon, all the data represented as blocks can be connected through a linked list data structure (Eyal & Sirer, 2018).

The block header includes the following Information

- Block version: indicates which set of block validation rules are to be followed
- Parent block hash: a 256-bit hash value that indicates/points to the previous block in the chain.
- Merkle tree root hash: hash value of all the transactions in the block.
- Timestamp: current timestamp.
- nBits: current hashing target in a compact format.
- Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to authenticate transactions (Aitzhan & Svetinovic, 2018). In an untrustworthy environment asymmetrical digital signature is used. Illustrated below is the structure of a block body

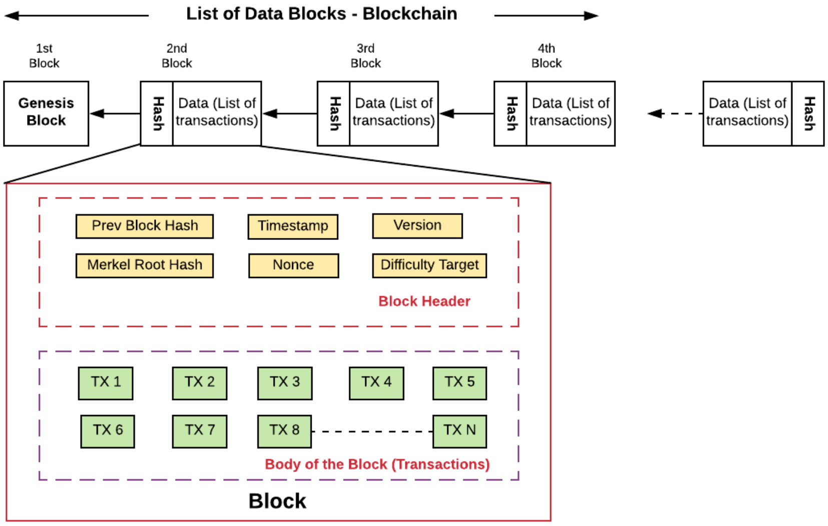

Fig 3.2: Structure of a Single Block in a Blockchain

IV. CONSENSUS MODEL

A key aspect of blockchain technology is to determine which user publishes the next block. This is solved through implementing a consensus models. In a permissionless blockchain networks there are generally many publishing nodes competing at the same time to publish the next block. How to resolve conflicts when multiple distrusting user nodes publish a block at approximately the same time and make them work together is the essence of consensus model.

The following properties are in place:

• The initial state of the system is agreed upon (e.g., the genesis block).

• Users agree to the consensus model by which blocks are added to the system.

- Every block in the chain has the hash digest of the previous block to maintain the chain structure

- Users can verify every block independently.

In permissioned blockchain networks there exists some level of trust between publishing nodes. In such cases there need not be a consensus model to determine which participant is going to add the block. As the level of trust increases, the need for resource usage as a measure of generating trust decreases.

In the following section we will discuss few commonly used consensus models

4.1. Proof of Work Consensus Model

In the proof of work (PoW) model, a user who sloves a computationally intensive puzzle is the one to publishes the next block. The solution found is the – proof that they have performed work. The puzzle is designed in such a way that solving the puzzle is difficult but checking the validity of the solution is simple . This makes it easy for all the other participating blocks to validate or invalidate the proposed new block.

A common puzzle method used for validation is to require that the hash digest of a block header be less than a target value. Publishing nodes make many small changes to their block header (e.g., by changing the nonce) trying to find a hash digest that meets the requirement. For each attempt, the publishing node must compute the hash for the entire block header. This is a computationally intensive process. The target value is usually modified over a period of time to adjust the difficulty and to influence how frequently blocks are being published.

4.2. Proof of Stake Consensus Model

The proof of stake (PoS) model is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed. Stake hear is often the amount of cryptocurrency that the blockchain network user has invested into the system. Once staked, the cryptocurrency cannot be spent. Proof of stake blockchain networks use the amount of stake a user invested as a factor for publishing new blocks. More a user invests more the possibility of him publishing a block. With this consensus model, there is no need to perform resource intensive computations as in proof of work. Since this consensus model utilizes fewer resources, some blockchain networks have decided to forego a block creation reward. In such systems, the reward for block publication is then usually the earning of user provided transaction fees.

4.3. Round Robin Consensus Model

Round Robin is a consensus model is used by some permissioned blockchain networks. In this model, nodes take turns in creating blocks. Round Robin Consensus has a long history starting with distributed system architecture. Time limits are set for each node within which it can publish new nodes, if a node is unable to publish within a given time frame the next node is given a chance. This model ensures no one node creates the majority of the blocks. Advantage of using this model is that it uses a straightforward approach, lacks cryptographic puzzles, and has low power requirements. Since there is a need for trust amongst nodes, round robin does not work well in the permissionless blockchain networks used by most cryptocurrencies.

4.4. Proof of Authority/Proof of Identity Consensus Model

The proof of authority also known as proof of identity consensus model relies on the partial trust of publishing nodes through their known links to real world identities. Publishing nodes must have their identities proven and verifiable within the blockchain network. The idea is that the publishing node is staking its identity/reputation to publish new blocks. Blockchain network users directly affect a publishing node’s reputation based on the publishing node’s behavior. The lower the reputation, the less likelihood of being able to publish a block. Therefore, it is in the interest of a publishing node to maintain a high reputation. This algorithm only applies to permissioned blockchain networks with high levels of trust.

4.5. Proof of Elapsed Time Consensus Model

Within the proof of elapsed time (PoET) consensus model, each publishing node requests a wait time from a secure hardware time source within their computer system. The secure hardware time source will generate a random wait time and return it to the publishing node software. Publishing nodes take the random time they are given and become idle for that duration. Once a publishing node wakes up from the idle state, it creates and publishes a block to the blockchain network, alerting the other nodes of the new block; any publishing node that is still idle will stop waiting, and the entire process starts over.

This model requires ensuring that a random time was used, since if the time to wait was not selected at random a malicious publishing node would just wait the minimum amount of time by default to dominate the system. This model also requires ensuring that the publishing node waited the actual time and did not start early. These requirements are being solved by executing software in a trusted execution environment found on some computer processors such as Intel’s Software Guard Extensions, or AMD’s Platform Security Processor, or ARM’s TrustZone. The following table summarizes all the consensus models discussed in the above section

Table 4.1: Consensus Models in Blockchain

Name	Goals	Advantages	Disadvantages	Domains	Implementations
Proof of work (PoW)	To provide a barrier to publishing blocks in the form of a computationally difficult puzzle to solve to enable transactions between untrusted participants.	Difficult to perform denial of service by flooding network with bad blocks. Open to anyone with hardware to solve the puzzle.	Computationally intensive, power consumption, hardware arms race. Potential for 51 % attack by obtaining enough computational power.	Permissionless cryptocurrencies	Bitcoin, Ethereum, many more
Proof of stake (PoS)	To enable a less computationally intensive barrier to publishing blocks, but still enable transactions between untrusted participants.	Less computationally intensive than PoW. Open to anyone who wishes to stake cryptocurrencies. Stakeholders control the system.	Stakeholders control the system. Nothing to prevent formation of a pool of stakeholders to create a centralized power. Potential for 51 % attack by obtaining enough financial power.	Permissionless cryptocurrencies	Ethereum Casper, Krypton
Delegated PoS	To enable a more efficient consensus model through a 'liquid democracy' where participants vote (using cryptographically signed messages) to elect and revoke the rights of delegates to validate and secure the blockchain.	Elected delegates are economically incentivized to remain honest More computationally efficient than PoW	Less node diversity than PoW or pure PoS consensus implementations Greater security risk for node compromise due to constrained set of operating nodes As all delegates are 'known' there may an incentive for block producers to collude and accept bribes, compromising the security of the system	Permissionless cryptocurrencies Permissioned Systems	Bitshares, Steem, Cardano, EOS
Round Robin	Provide a system for publishing blocks amongst approved/trusted publishing nodes	Low computational power. Straightforward to understand.	Requires large amount of trust amongst publishing nodes.	Permissioned Systems	MultiChain
Proof of Authority/Identity	To create a centralized consensus process to minimize block creation and confirmation rate	Fast confirmation time Allows for dynamic block production rates Can be used in sidechains to blockchain networks which utilize another consensus model	Relies on the assumption that the current validating node has not been compromised Leads to centralized points of failure The reputation of a given node is subject to potential for high tail-risk as it could be compromised at any time.	Permissioned Systems, Hybrid (sidechain) Systems	Ethereum Kovan testnet, POA Chain, various permissioned systems using Parity
Proof of Elapsed Time (PoET)	To enable a more economic consensus model for blockchain networks, at the expense of deeper security guarantees associated with PoW.	Less computationally expensive than PoW	Hardware requirement to obtain time. Assumes the hardware clock used to derive time is not compromised Given speed-of-late latency limits, true time synchronicity is essentially impossible in distributed systems	Permissioned Networks	Hyperledger Sawtooth

V. SMART CONTRACTS

The term smart contract dates to 1994, defined by Nick Szabo as "a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries." [17].

Smart contracts extend and leverage blockchain technology. A *smart contract* is a collection function- code and state-data. It is deployed using cryptographically signed transactions on the blockchain. The smart contract is executed by nodes within the blockchain networ. All the nodes that execute the smart contract must derive the same results from the execution, and the results of execution are recorded on the blockchain.

Blockchain network users can create transactions which send data to public functions offered by a smart contract. The smart contract executes the appropriate method with the user provided data to perform a service. The code, being on the blockchain, is also tamper evident and tamper resistant and therefore can be used as a trusted third party. A smart contract can perform calculations, store information, expose properties to reflect a publicly exposed state and, if appropriate, automatically send funds to other accounts. It does not necessarily even have to perform a financial function. It is important to note that not every blockchain can handle smart contracts. For many blockchain implementations, the publishing nodes execute the smart contract code simultaneously when publishing new blocks. For smart contract enabled permissionless blockchain networks like Ethereum the user issuing a transaction to a smart contract will have to pay for the cost of the code execution involved.

VI. BLOCKCHAIN LIMITATIONS AND MISCONCEPTIONS.

As with any new technology there is always a tendency to overhype and overuse of Blockchaining. The main reason for this being not understanding the technology complete and the technology being in its nascent stage. In the following section we will highlight some of the limitations and misconceptions that surround the Blockchain technology.

5.1. Immutability

Most publications on blockchain technology describe blockchain ledgers as being immutable. However, this is not strictly true. They are tamper evident and tamper resistant which is a reason they are trusted for financial transactions

5.2. Beyond the Digital

Blockchain networks work extremely well with the data within their own digital systems. However, when they need to interact with the real world, there are some issues (often called the Oracle Problem [22]). A blockchain network can be a place to record both human input data as well as sensor input data from the real world, but there may be no method to determine if the input data reflects real world events. A sensor could be malfunctioning and recording data that is inaccurate. Humans could record false information (intentionally or unintentionally). These issues are not specific to blockchain networks, but to digital systems overall. However, for blockchain networks that are pseudonymous, dealing with data misrepresentation outside of the digital network can be especially problematic.

5.3. Blockchain Death

Traditional centralized systems are created and taken down constantly, and blockchain networks will likely not be different. However, because they are decentralized, there is a chance that when a blockchain network "shuts down" it will never be fully shut down, and that there may always be some lingering blockchain nodes running. A defunct blockchain would not be suitable for a historical record, since without many publishing nodes, a malicious user could easily overpower the few publishing nodes left and redo and replace any number of blocks.

5.4. Cybersecurity

The use of blockchain technology does not remove inherent cybersecurity risks that require thoughtful and proactive risk management. Many of these inherent risks involve a human element. Therefore, a robust cybersecurity program remains vital to protecting the network and participating organizations from cyber threats, particularly as hackers develop more knowledge about blockchain networks and their vulnerabilities.

5.5. Malicious Users

While a blockchain network can enforce transaction rules and specifications, it cannot enforce a user code of conduct. This is problematic in permissionless blockchain networks, since users are pseudonymous and there is not a one-to-one mapping between blockchain network user identifiers and users of the system. malicious mining actions can include:

- Ignoring transactions from specific users, nodes, or even entire countries.
- Creating an altered, alternative chain in secret, then submitting it once the alternative chain is longer than the real chain. The honest nodes will switch to the chain that has the most "work" done (per the blockchain protocol). This could attack the principle of a blockchain network being tamper evident and tamper resistant.
- Refusing to transmit blocks to other nodes, essentially disrupting the distribution of information (this is not an issue if the blockchain network is sufficiently decentralized).

5.6. Resource Usage

Blockchain technology has enabled a worldwide network where every transaction is verified and the blockchain is kept in sync amongst a multitude of users. For blockchain networks utilizing proof of work, there are many publishing nodes expending large amounts of processing time and, more importantly, consuming a lot of electricity. A proof of work method is an effective solution for “hard to solve, easy to verify” proofs; however, it generally requires significant resource usage. Because of their different applications, and trust models, many permissioned blockchain technologies do not use a resource intensive proof, but rather they utilize different mechanisms to achieve consensus.

5.7. Public Key Infrastructure and Identity

When hearing that blockchain technology incorporates a public key infrastructure, some people immediately believe it intrinsically supports identity. This is not the case, as there may not be a one-to-one relationship of private key pairs to users (a user can have multiple private keys), nor is there a one-to-one relationship between blockchain addresses and public keys (multiple addresses can be derived from a single public key).

Digital signatures are often used to prove identity in the cybersecurity world, and this can lead to confusion about the potential application of a blockchain to identity management

VII. CONCLUSION

Blockchaining is a ground breaking technology that eliminates the usage of trusted third part in electronic transactions among users. With Bitcoin leveraging the use of BlockChain Technology there has been a rush to implement and this technology in a wide variety of applications. The use of blockchain technology is still in its early stages, but it is built on widely understood and sound cryptographic principles. As detailed throughout this publication, a blockchain relies on existing network, cryptographic, and recordkeeping technologies but uses them in a new manner. It will be important that organizations are able to look at the technologies and both the advantages and disadvantages of using them. Once a blockchain is implemented and widely adopted, it may become difficult to change it. Once data is recorded in a blockchain, that data is usually there forever, even when there is a mistake. For some organizations these are desirable features. For others, these may be deal breakers preventing the adoption of blockchain technology. Blockchain technology is still new and organizations should treat blockchain technology like they would any other technological solution at their disposal--use it only in appropriate situations.

REFERENCES

[1] Clarke, A.C., “Hazards of Prophecy: The Failure of Imagination,” from *Profiles of the Future: An Inquiry into the Limits of the Possible*, 1962.

[2] Lamport, Leslie. “The Part-Time Parliament.” *ACM Transactions on Computer Systems*, vol. 16, no. 2, Jan. 1998, pp. 133–169., https://dl.acm.org/citation.cfm?doid=279227.279229.

[3] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, 2016.

[4] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. https://bitcoin.org/bitcoin.pdf

[5] National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards (FIPS) Publication 180-4, August 2015. https://doi.org/10.6028/NIST.FIPS.180-4

[6] National Institute of Standards and Technology (NIST), Secure Hashing website, https://csrc.nist.gov/projects/hash-functions

[7] “Hash per Second.” *Bitcoin Wiki*, http://en.bitcoin.it/wiki/Hash_per_second.

[8] National Institute of Standards and Technology, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, Federal Information Processing Standards (FIPS) Publication 202, August 2015. https://doi.org/10.6028/NIST.FIPS.202

[9] National Institute of Standards and Technology (NIST), *Digital Signature Standard*, Federal Information Processing Standards (FIPS) Publication 186-4, July 2013. https://doi.org/10.6028/NIST.FIPS.186-4

[10] “LDAP.com.” *LDAP.com*, https://www.ldap.com.

[11] Taylor, D. (2018). An Analysis of Bitcoin and the Proof of Work Protocols Energy Consumption, Growth, Impact and Sustainability.

[12] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

[13] Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1545-1550). IEEE.

[14] Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 15(5), 840-852.

[15] Tahir, M., Li, M., Ayoub, N., Shehzaib, U., & Wagan, A. (2018). A Novel DDoS Floods Detection and Testing Approaches for Network Traffic based on Linux Techniques. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 9(2), 341-357.