*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

# Navigating the Promises and Hurdles of Blockchain Technology: A Journey through Opportunities and Challenges

**R. Anandhi**
Assistant Professor,
Department of MCA, DDGD Vaishnav College, Arumbakkam, Chennai, India,
sekadhi@gmail.com

**G. Sekar**
Assistant Professor,
PG and Research Department of Computer Science,
Dr. Ambedkar Govt. Arts College, Vyasarpadi, Chennai, India, sekarg@daga.co.in

**Abstract**— Everyone has come across the buzz word of the industry "Blockchain". Today, Blockchain and the crypto-currencies have become parallel platforms where people have started performing their monetary/non-monetary transactions. It is a very popular technology that rules almost every sector in foreign country, but not approved fully by Indian government. Blockchain is the collection of blocks connected in a linear list fashion [1]. Each block encloses its own data, also holds the hash of the previous block which ties a new block to the previous one unlike linked list. If one of the blocks is removed from the blockchain, the entire chain will collapse because of loss of connectivity. Cryptography in hands with computer science ensures that nobody can change the data in blockchain network. Once information is added to the blockchain, it is impossible to remove or edit. The immutable nature makes the blockchain to serve as a trustworthy database of information. Once validated by the network's consensus algorithm(s), these blocks are added to an existing sequential chain of cryptographic hash-linked blocks, to ensure the integrity of the data in blockchain [2]. Hence this paper brings about the structure of blockchain, the creation of blocks, the data structure-Merkle tree to store the transactions, the distributed consensus algorithms to achieve agreement among the nodes, the popular use-cases and applications of blockchain.

**Keywords**- Blockchain, Merkle tree, Transaction, Genesis block, Block hash, PoW, PoS, PBFT.

## I.INTRODUCTION

Blockchain is a combination of business principles, economics, game theory, cryptography and computer science. A blockchain can be defined as a chain of blocks containing information as in the below diagram Fig.1. This technology aims to time-stamp digital documents so that they cannot be dated or tampered with. The purpose of blockchain is to solve the problem of duplicate records without the need for a central server. Blockchain doesn't work without the internet. Blockchain can be used to securely transfer money, property, contracts, etc. without the need for third-party intermediaries such as banks or governments. A blockchain is a peer-to-peer distributed ledger with algorithms cryptographically computed using immutable consensus (such as PoW). Blockchain technology not only helps users conduct cryptocurrency transactions, but also ensures the safety and anonymity of the users involved [3]. Blockchain can be called as the backbone of the entire cryptocurrency system. This is a data structure where each block is linked to another block with a timestamp. This is a connection-only transactional database, not a replacement for traditional databases. Each node/member of the blockchain network keeps a cryptographically protected copy of all past transactions. All information stored in the ledger is auditable and auditable, but cannot be edited. It is fault tolerant as it is decentralized and has no single point of failure.

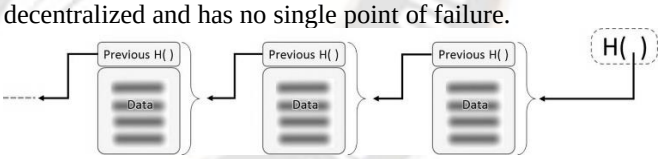


**Fig.1. Blockchain arrangement**

## II.EVOLUTION OF BLOCKCHAIN

Blockchain technology was explained by Stuart Haber and W. Scott Stornetta in 1991. They sought to introduce a computationally practical solution for timestamping digital documents so that they cannot be tampered with or retroactive [4]. They have tried a system to store time-stamped documents using cryptographically secured concepts. In 1992, Merkle incorporated his tree into the design, allowing him to combine multiple documents into a single block, making blockchains more efficient. Satoshi Nakamoto came up with the theory of decentralized blockchains in 2008. He improved the design, adding blocks to the original chain without requiring a signature by a trusted party, and his peer-to-peer network for timestamping and verifying each transaction without the need for a central authority. established. Blockchain development is

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

stable and promising [5]. In original work of Satoshi Nakamoto, the words block and chain were used separately, but eventually came to be known as his one word, blockchain, and by 2016 he had grown from 20GB to his has grown to 100GB.

## III.LAYERS OF BLOCKCHAIN

TCP/IP, like blockchain, is the communication protocol used by all internet applications. In fact, the TCP/IP layered approach is the standard for achieving open systems. There are still no agreed global standards that clearly separates blockchain components into different layers [6]. There are five layers in a blockchain networks as shown in Fig.2.

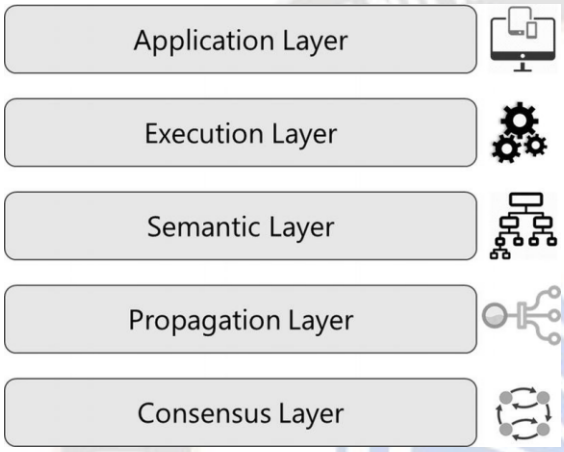


**Fig.2. Blockchain Layers**

- **Application layer** is the layer where the coding of the desired functionality and create an application for the end user is done. Client-side programming constructs, scripts, APIs, development frameworks, etc. For applications that use blockchain as a backend, the application may be hosted on a web server and may require web application development, server-side programming and APIs, etc.
- **Execution layer** is the layer that executes the sequenced instructions by the application layer across all nodes in the blockchain. A program must be running to successfully execute a transaction. Every node in a blockchain network should run a program/script independently, but given the same inputs and conditions, all nodes will always produce the same output to avoid conflicts.
- **Semantic layer** is the logical layer since it orders the transactions and blocks. A transaction (valid/invalid), has a set of instructions that pass through the execution layer have to be validated by the semantic layer. System rules can be defined here using data models, storage mode, in-memory/disk based processing and other supporting structures. The Merkle tree data structure is defined in this layer with a Merkle root in the block header to maintain the relationship between the block header and the set of transactions within the block (usually key-value storage on disk). This layer defines how blocks are linked among each other. Each block in the blockchain holds hash of previous block up to the genesis block. The final state of the blockchain is achieved through the contributions of all layers, but the interconnection of blocks must be defined by this layer.
- **Propagation layer** is a peer-to-peer communication layer that allows nodes to discover, talk to each other and synchronize about the current state of the network.
- **Consensus layer** is the base layer responsible for collecting the agreement from the blockchain nodes to have consistent state of the ledger. There are various algorithms for achieving consensus depending on the application by ensuring the safety and security like Proof of Work (PoW), Proof of Stake (PoS), deligated PoS (dPoS), Practical Byzantine Fault Tolerance (PBFT), etc.

## IV.THE STRUCTURE OF BLOCKCHAIN

Now we are clear about the fact that the blockchain is a data structure with a series of blocks linked together. A block can have a single transaction or multiple transactions. Unlike a linked list pointing to the next block, the previous block's hash is stored in the current block's header, and the hash of the current block and its block header is stored in the next block's header [7] and so on in blockchain setup as depicted in Fig.3. H() is a cryptographic hash function that maps any kind of arbitrary data of arbitrary length to a fixed size output. Basic properties of hash functions: determinism, computational efficiency, collision resistance, preimage resistance, and irreversibility. The first block created in a blockchain is called a “genesis block”. Each new block added to the chain becomes the parent block of the next block added [8].

Any attempt to change the header or block the content will break the whole chain. Suppose we change the data in block number 234. If we do this, the hashes stored in Block number 235's block headers will no longer match. What if we also change the hash stored in the block header of block 235 so that it exactly matches the changed data of 234? Hash data block 234 after the change and replace this new hash with the hash stored in the block header of block 235. Then the hash of block 235 is changed (because block 235 means data and header together) and does not match what is stored in the block header of block 236. We have to do this until the genesis block hash. Since everyone on the network has a copy of the blockchain with the latest updates, it is not possible to hack into most systems and change all hashes at once [9]. This guarantees for a tamper-proof blockchain data structure.

Each block can be identified uniquely by its hash. If we use SHA-256 (Secure Hash Algorithm-256 bits) to hash the blocks, it would produce a 256-bit hash output such as:

**000000000000000a73b6a2af7doog0ec3fc2ad38afd76ef15f3d1b71a6233664**

There are only 64 characters in it. Since the hash is represented by hexadecimal, every hexa digit can be represented using 4 bits, hence the output is 64 × 4 = 256 bits [10].

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

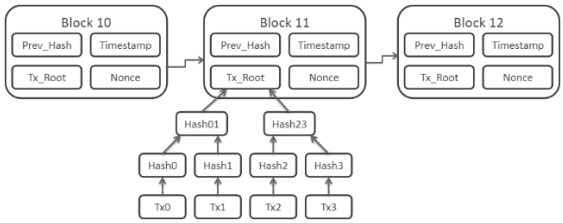


**Fig.3. Structure of a Block in the Blockchain**

**Merkle Trees**

A Merkle tree is a binary tree of cryptographic hash pointers named after its inventor, Ralph Merkle. A Merkle tree as shown in Fig.4 stores every transaction in a block by creating a digital fingerprint of the entire transaction set. This allows users to check if a transaction can be included in a block and later check if a transaction exists in a particular block. It also enables efficient and secure content consistency checking [11]. A leaf is a single-block transaction in the blockchain. Each leaf node is a hash of transaction data, and non-leaf nodes are hashes that combine previous hashes. Like other trees, it is built from the bottom up (that is, hashing transaction IDs at the leaf level and rehashing the hashed output up to the root node. Merkle trees iteratively compute hash pairs of nodes This hash is called the Merkle root or root hash. The Merkle root is a simple mathematical way of proving facts about a Merkle tree [12]. They are used in cryptocurrencies to ensure that blocks of data sent over P2P networks are secure.

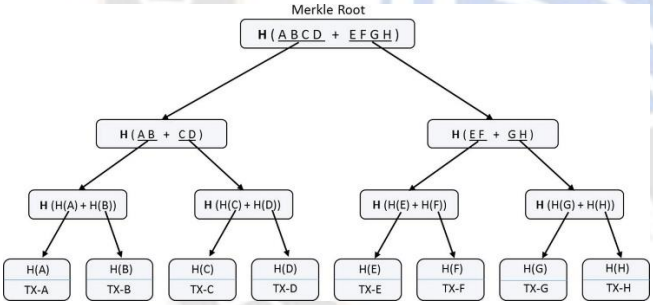


**Fig.4. Merkle Tree**

Merkle Trees are also tamper-proof. Operations at any level in the tree will not match the hash stored up to the higher levels of the hierarchy and up to the root node. It would be very difficult for a traitor to change all hashes of the entire tree. It also guarantees transaction order integrity. Changing only the transaction order will also change the hash in the tree until the Merkle root changes [13]. A Merkle tree is a full binary tree, so it must have an even number of leaf nodes. For odd transactions, the last hash is replicated once to create an even leaf node. Let's say we have 5 data nodes. Data1+Data2 can be hashed together to form a Merkle branch. The same is true for Data3+Data4. But data 5 doesn't have a pair to hash to the new branch. The only option is to keep traversing until we reach the exact block that matches the hash of the transaction. This is one case where Merkle trees are very useful. Merkle trees provide a very efficient way to verify that a particular transaction belongs to a particular block. If there are "n" transactions in the Merkle tree (leaf elements), this check will only take log(n) time.

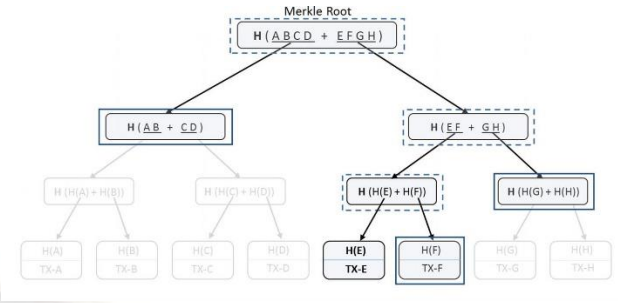


**Fig.5. Search Operation in Merkle Tree**

To check whether a transaction is in a Merkle tree, it is not needed to scan all the members of Merkle tree as depicted in Fig. 5. Instead, a subset of it is needed as shown in the above diagram. One can just start with the transaction to verify along with its sibling (it is a binary tree so there would be one sibling leaf item), calculate the hash of those two, and check whether it matches the hash of their parent [14]. Repeat the process with the obtained parent hash and its sibling at the given level and hash them together to have their parent hash. Continuing this process up to the top root hash is the fastest and available way for verifying the presence of transaction. The solid rectangles represent that those inputs are required and the dotted rectangles can be computed from the required input provided the solid rectangle data. In addition to the blocks in the blockchain are tamper resistant and do not provide even the slightest scope to change anything in a block, the Merkle tree also ensures that the order of transactions is preserved [15]. We already know that the hash functions are one-way and so no way can a traitor forge transaction that would match a given hash value. Further, it is even difficult to do so from transaction level till the Merkle root.

## V.PROPERTIES OF BLOCKCHAIN

- Preserving the atomicity of blockchain transactions is the most desirable property. Once a transaction is updated in the chain, it cannot be edited. When a transaction is sent to the network, most people have a copy of the transaction. Cryptographically protected, it is virtually impossible to change too many blocks of data consecutively. Therefore, all logged transactions remain in the system forever [16].
- Decentralized solutions with exposed transactions are vulnerable to many types of attacks. Attempts at counterfeiting are most evident, especially when we are trading something of value. Cryptographic hashes and digital signatures can be used to ensure that systems are tamper-proof. It is computationally impossible to forge someone's digital signature. Once we create a transaction and sign its hash, we cannot change the transaction later. Also, we can't later claim that we haven't made a transaction since we signed it.
- A decentralized peer-to-peer system should be democratic in nature. No entity in the system should be more powerful than another entity. All participants should have equal rights in all circumstances and decisions are taken when a majority reaches consensus [17].
- Double-spend attacks are common in both financial and non-monetary transactions. In a cryptocurrency

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

environment, double spending attempts occur when one person attempts to spend the same amount on multiple people. In a centralized system, preventing double spending is fairly easy as the central authority keeps track of all transactions. Also, the blockchain solution should be immune to such double-spending attacks. While encryption ensures the authenticity of transactions, it does not prevent double spending. Because technically both regular and double spend transactions are real. So, the only way to avoid double spending is to know every transaction. If we know all past transactions, we can tell if the transaction is an attempt to double spend. Therefore, a node validating a transaction must be able to reliably access all blockchain data since the genesis block.

## VI.DISTRIBUTED CONSENSUS MECHANISMS

***"The motive of the Consensus mechanism in a blockchain is to permit a set of separate nodes to distribute the proper to replace the community or gadget. However, the replace will appear in accordance to 3 mounted guidelines many of the set of members in a steady manner".***

A consensus set of rules is a method via which all of the friends of the Blockchain community attain a not unusual place settlement approximately the existing nation of the disbursed ledger via way of means of figuring out which blockchain transactions are legitimate and which might be not. Consensus mechanisms shape the spine of all cryptocurrency blockchains, and are what lead them to steady. Consensus algorithms acquire reliability withinside the Blockchain community and set up consider amongst unknown friends in a disbursed computing environment. Essentially, the consensus protocol makes positive that each new block this is brought to the Blockchain is the only and handiest model of the reality this is agreed upon via way of means of all of the nodes withinside the Blockchain. It makes the manner to acquire a choice nation with which all community members agree wherein the nodes don`t consider every other. Blockchain makes use of a consensus mechanism to set up governance amongst all of the community members. There are many one-of-a-kind kinds of consensus mechanisms, relying at the blockchain and its application. While they range of their electricity usage, security, and scalability, all of them proportion one motive: to make sure that statistics are authentic and honest. rewards, there is only transaction fees for the miners (more accurately validators). Some of the popular consensus algorithms in existence are:

**Proof of Work (PoW)**
A Proof-of-Work is a computational problem that takes a certain to effort to solve while the effort and the time taken to verify the results of the computational problem given are very less compared to the effort it takes to solve the computational problem itself [18].

**Proof of Stake (PoS)**
The Proof-of-Stake algorithm isn't about mining, but is about validating blocks of transactions. There are no mining rewards. A **stake** represents the money or the value we bet on a certain outcome. In PoS systems, the validators have to bond their stake (mortgage the amount of cryptocurrency) to be able to participate in validating the transactions. The probability of a validator producing a block is proportional to their stake; the more the amount at stake, the greater is their chance to validate a new block of transactions [19]. A miner needs to prove that they have a percentage of coins in the given time for the given currency. There isn't any relevant authority gift to validate and confirm the blockchain transactions, but each transaction withinside the Blockchain is taken into consideration to be absolutely secured and verified. This is feasible handiest due to the presence of the consensus protocol that is a center a part of any Blockchain community. In order to assure that each one member in a blockchain community agree on a unmarried model of history, blockchain networks put into effect consensus mechanisms/consensus protocols/consensus algorithms, which make the gadget fault-tolerant.

**Practical Byzantine Fault Tolerance Algorithm (PBFT)**
PBFT is an acronym for. PBFT is designed to work efficiently in asynchronous systems (there is no upper bound on when responses to requests are received). Optimized for less overhead time. PBFT is efficient compared to other consensus algorithms based on the effort required. It is one of the most widely used algorithms for consensus even in non-blockchain environments. PBFT is also a PoS-like algorithm that is not used to generate mining rewards. PBFT requests are sent to all participating nodes that have their own copy or internal state. When a node receives a request, it performs computations based on its internal state [20]. The result of the computation is shared with all other nodes in the system. So each node knows what the other nodes are computing. Consider the results of our own calculations and the results received from the nodes to make decisions and determine final values. The final value is shared by all nodes. At that point, each node knows the final decision of all other nodes. Everyone then makes the final decisions and final consensus is reached based on majority votes.

## VII.BLOCKCHAIN APPLICATIONS

We will look at some of the initiatives already taking place in industries such as finance, insurance, banking, healthcare, government, supply chain, Internet of Things (IoT), media and entertainment, to name a few [21].

- We can register any type of property or asset, whether physical or digital, including laptops, mobile phones, diamonds, cars, real estate, electronic registrations, digital files, notary services, proof of existence, bespoke insurance schemes, and more. A blockchain that trades these assets from one person to another, keeps transaction logs, and verifies validity or ownership.
- Many financial use cases are being developed on blockchain, such as: B. Cross-border payments, stock trading, loyalty and reward systems, bank-to-bank Know Your Customer (KYC), etc. Initial Coin Offerings (ICOs) are one of the hottest cases of their kind. ICOs are the best way to crowdsource today by using cryptocurrencies as digital assets. ICO coins can be thought of as digital shares in companies that are very easy to buy and trade.

- Using blockchain, the "wisdom of the crowd" can take leadership and harness collective wisdom to shape businesses, economies, and a variety of other national phenomena. Wisdom-of-the-crowd financial and economic forecasting, decentralized prediction markets, decentralized voting, and stock trading are all possible on the blockchain.
- The process of determining music royalties has always been complicated. Internet-enabled music streaming services have increased market penetration but have made royalty decisions more complex. Blockchain can largely address this problem by maintaining a public ledger of information about ownership of music rights and permitted distribution of media content.
- This is the age of IoT, with billions of IoT devices everywhere and more IoT devices joining the pool. With so many different brands, models, and communication protocols, it's difficult to have a centralized system for controlling devices and providing a common data exchange platform. This is also an area where blockchain can be used to build decentralized peer-to-peer systems that allow IoT devices to communicate with each other.  Blockchain is also gaining momentum in the government sector. There are use cases that require technical decentralization but political regulation by governments. Land registration, vehicle registration and management, electronic voting, etc. are some of the active use cases. Supply Chain is another area with some great use cases

## VIII.BLOCKCHAIN USE-CASES

- In 2016, smart Dubai office introduced Blockchain strategy for connecting entrepreneurs and developers with investors and leading companies to favor the development of various kinds of industries in Dubai and to make Dubai as `the happiest city in the world [22].
- CRaaS (Consumer Retention as a Service) is a loyalty program which is based on generating tokens for businesses affiliated with its related network and it can be stored in digital portfolios of user`s phones or accessing through the browser.
- In January 2017, the United Nations world food program started a project called humanitarian aid for the rural areas of the Sindh region of Pakistan. By using the Blockchain technology, beneficiaries received money, food and all type of transactions are registered on a blockchain to ensure security and transparency of this process.
- A cryptocurrency [23] is one medium of exchange like traditional currencies such as rupees, but it is designed to exchange the digital information through a process made possible by certain principles of cryptography. Cryptocurrency is a bearer instrument based on digital cryptography. In this type of cryptocurrency, the owner of the currency has ownership. No further records are kept of the owner's identity. Cryptocurrency is a peer-to-peer technology that is not regulated by any central authority or bank. Bitcoin issuance and transaction management are now integrated on the network. Popular cryptocurrencies include Bitcoin, Ethereum, Ripple, and Litecoin.

## IX.CONCLUSION

Blockchain has showed its strength in changing traditional and standard procedures by its salient features like tamperproof, non-editable, decentralization, auditable and secured. This paper gives a detailed description about the features of blockchain, its arrangement of blocks, applications, use-cases and the importance of consensus mechanism to achieve agreement among the nodes of blockchain network. Blockchain is only acting as the backbone for all cryptocurrency technology, also used in the fields like IoT, financial services, voting, health care etc. Hence blockchain acts as an immutable ledger to record the transactions taking place among the geographically apart nodes within no time and without a third party.

## REFERENCES

[1] [1] Sourabh Yadav, Monika Mangla, Nonita Sharma, Asmita Mahajan, "Blockchain framework for smart contract and distributive ledger for entity marketplace", International Journal of Blockchains and Cryptocurrencies (IJBC), Vol. 3, No. 2, 2022

[2] [2] Rishav Chatterjee, Rajdeep Chatterjee, "An overview of the emerging technology: Blockchain", 3rd International Conference on Computational Intelligence and Networks (CINE), October 2017.

[3] [3] Subodh Kesharwani, Madhulika P. Sarkar, Shailza, Jyoti, "Blockchain and Digital Payments-The New Paradigm", Cybernomics- An International Periodical, May 2019.

[4] [4] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of11th European Conference on Technology Enhanced Learning (EC-TEL2015), Lyon, France, 2015, pp. 490–496.

[5] [5] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals problem," ACM Transactions on Programming Languages and Systems(TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[6] [6] V. Buterin, "On public and private blockchains,"2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[7] [7] NRI, "Survey on blockchain technologies and related services," Tech.Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf

[8] [8] Sebastian Schuetz, Viswanath Venkatesh, "Blockchain, adoption, and financial inclusion in India: Research opportunities", International Journal of Information Management, May 2019.

[9] [9] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy(SP), San Jose, CA, USA, 2016, pp. 839–858.

[10] [10] Y. Zhang and J. Wen, "An iot electric business model based on theprotocol of bitcoin," in Proceedings of 18th International Conference onIntelligence in Next Generation Networks (ICIN), Paris, France, 2015,pp. 184–191.

[11] [11] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014.

[12] [12] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security, NewYork, NY, USA, 2014, pp. 15–29.

[13] [13] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technicalsurvey on decentralized digital currencies," IEEE Communications Sur-veys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[14] [14] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," Self-Published Paper, August, vol. 19, 2012.

[15] [15] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed.Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170[

[16] [16] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[17] [17] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.

[18] [18] J. Kwon, "Tendermint: Consensus without mining," URLhttp://tendermint. com/docs/tendermint { } v04. pdf, 2014.

[19] [19] V. Zamfir, "Introducing casper the friendly ghost," Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casper-friendly-ghost, 2015.

[20] [20] Sachchidanand Singh, Nirmala Singh, "Blockchain: Future of financial and cyber security", 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), December 2016.

[21] [21] Bhargava, Richa, "Blockchain Technology and Its Application: A Review", IUP Journal of Information Technology; Hyderabad Vol. 15, Iss. 1, March 2019.

[22] [22] Harsha Gandhi, Rupali More, Nainisha Patil, "A Blockchain in Banking Application", Global Journal for Research Analysis, April 2019.

[23] [23] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain",2015.