International Journal of Knowledge Based Computer Systems
7 (1), June 2019, 25-32
http://www.publishingindia.com/ijkbcs/

Intramural Analysis of Blockchain

Prathyusha Kanakam[1*], Raghu Varma Edarapalli[2] and Shaik Mahaboob Hussain[3]
[1]Department of CSE, MVGR College of Engineering, Vizianagaram, Andhra Pradesh, India.
Email: prathyusha.kanakam@gmail.com
[2]Department of CSE, MVGR College of Engineering, Vizianagaram, Andhra Pradesh, India.
Email: raghuvarmaedarapalli@gmail.com
[3]Department of CSE, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India.
Email: mahaboobhussain.smh@gmail.com
*Corresponding Author

Abstract: Today blockchain technology is gaining a lot of mainstream attention and is already used in a variety of applications, not limited to cryptocurrencies. blockchain is a decentralized database system which is the collection of blocks of data. Databases exist before blockchain limited only with the data storage and not providing any security features. These databases are maintained under a trusted third party where it acts as a central server as well as a repository that stores entire data of that particular network. This centralized system has replaced by blockchain technology where every node of the connected network maintained a ledger of transactions. This article gives a clear schematic view of blockchain architecture and its contents in detail. It also extends the preliminaries associated with blockchain technology such as hashing, smart-contracts. Also, the authors proposed the influence of the Internet of Things along with blockchain technology in several domains where the blockchain can be indulged to associate the data with evading any tampering from outside sources like supply chain management, etc.

Keywords: Blockchain, Hash function, Hashing, Proof of Work (PoW), Smart-contracts.

I. Introduction

Blockchain works as the spine for the entire crypto-currency system. Blockchain technology helps the user transaction with security and anonymity. Blockchain is the growing list of blocks which contains records that are linked using cryptography. Each block composed of a cryptographic hash of the preceding block, a timestamp and transaction data which are indulged in it generally. By its design, a blockchain is resistant to manipulation of the information. The blockchain serves as an open and based on the distributed ledger technology (DLT) that can store transactions among two users in a verifiable and persistent way. This ledger is shared among distinct parties to maintain integrity.

F. Casino *et al.* has demonstrated well in his paper [1] affirming the contemporary applications of the blockchain technology and some of the arguments as per the current status. Authors considered multiple applications enabled with blockchain in various domains like healthcare, business and IoT etc. In terms of the persistence of this technology, one should understand the current issues. Most of this technology is signifying used in Business, Industry, health and security stand in the row. Most of the additional applications are also being use in governance, data management and education purpose. Recently, AI and big data analytics are evolving with a further number of exceptional applications. J. Bonneau *et al.* implemented an evaluation framework and investigated various issues of bitcoins for estimating and enhancing the privacy issues concerning bitcoin [2]. Apply the blockchain technology, bitcoin trades will execute as a block of reactions by hashing the precede blocks. Authors have demonstrated a serious influence on the bitcoins and their existence which may be implemented and secured with better applications using blockchain technology. Mahdi H. Miraz and M. Ali, stated the significance of this blockchain technology with various example distributed storage systems, proof-of-location, healthcare and case studies behind the emerging cryptocurrency [3]. Z. Zheng *et al.* have accomplished enormous work by distinguishing the several algorithms which are being apply in different applications of blockchain [4]. Essentially, authored considered some consensus algorithms like Proof of work which will be used in the network as well as proof of stake, which lessens the energy. However, the author additionally issued some challenges with these blockchain technology applications. Authors explored well concerning the transaction flows with the peer to peer along including the comprehensive scenario of the bitcoin cryptocurrency simultaneously with various applications in security point of view [5]. Authors have done their research for especially in the financial sector [6] and its influence by the emerging cryptocurrency and blockchain technology. Similarly, they demonstrate the working model of the blockchain with Transformation of Financial Services related to the financial system, other industries like education and health.

Blockchain technology helps the user transaction with security and anonymity. This ledger has shared among all users. Blockchain works as the spine for the entire crypto-currency system. The core part of crypto currencies is the blockchain where the cryptocurrencies are transmitted through this technology from one peer to another peer. As it is decentralized methodology, there is no need of trusting process of any single entity, unlike traditional approaches. So, every client or node in the network will be allowed to accord without having trust in each other. In 1991, Stuart Haber and W. Scott Stornetta brought out a state-of-art methodology of computing solution for time-stamping digital documents to avoid backtracking as well as tampering them further [7]. In the very next year, merkle tree is added benefit of storing several documents in a single block. After the introduction of bitcoin in 2004, the patent associated with merkle tree and blockchain has lapsed. Then later in 2013, Vitalik Buterin, a programmer and a co-founder of the Bitcoin Magazine announced about the scripting language behind bitcoin that can be apply to various decentralized domains. Failing to gain agreement in the community, Vitalik started the development of a new blockchain-based distributed computing platform called Ethereum, which featured a scripting functionality, called smart contracts [8]. Smart contracts are programs or scripts that are deployed and executed on the Ethereum blockchain; they can be used for example to make a transaction if certain conditions have met. Smart contracts are written in specific programming languages and compiled into bytecode, which a decentralized Turing-complete virtual machine, called the Ethereum virtual machine (EVM) can then read and execute.

II. Blockchain Architecture

Blockchain itself is a database or collection of data, and this set of data may be any type either text, audio, image or video and so on. Every block is associated with a header to differentiate the set of data related to one block to data from another block [4]. Here the block header acts as the delimiter between different blocks as illustrated in Fig. 1.

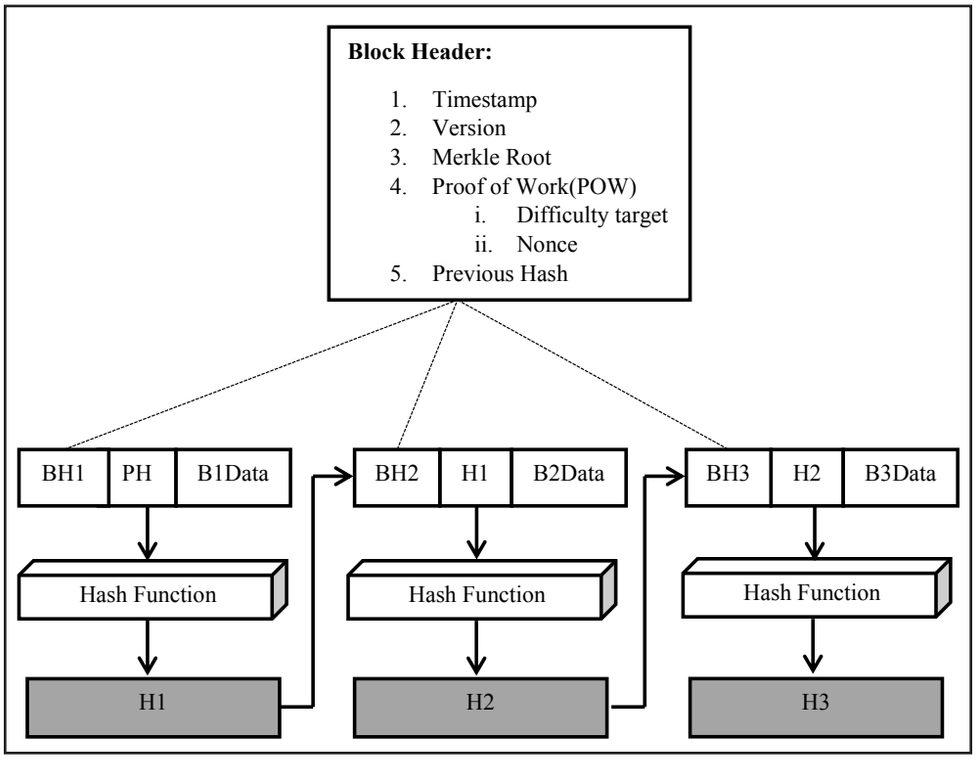

Fig. 1: Internal Schema of Blockchain

Every block header includes the fields.

- Timestamp: Gives the meta-information about data and time
- Version: Denotes the type of algorithm used for hashing and its version
- Merkle Root: Every merkle root is the root hash of the blocks that hold the transactional data.
- Difficulty Target and Nonce: It related to algorithm Proof of Work (PoW) which is used to identify the process of creating a root hash of a block.
- Previous Hash: Illustrates the link through which blocks have chained together.

For instance, let say B1, B2, B3 are the sub-blocks that holds data and H1 represents that hash of block 1, H2 represents the hash of block 2 and H3 represents hash block 3. As discussed earlier, every block's header holds the previous hash as its fields. Thus, block 2 header holds H1, block 3 header holds H2, and so on. Thus, the blocks are linked together in the chain process. The reason behind this chaining process is easy backtracking.

Blockchain exhibits the characteristic of immutability, i.e., once a block has created, it cannot be changed further, as single bit effects the hash produced or desired as the blockchain technology itself indicates the chaining concepts and network that uses this technology will also be interlinked with nodes to exhibit decentralized nature. Every node will have the copy of transactional data of every block that has transmitted between any 2 peers with specific to that network. Thus, every node can see the change effected while doing the transactions. So, bit change in block affects the hash and is detect by any of the nodes which are connected through the network.

Blockchain is a kind of database that holds the data of any type in terms of block and linked or chained to another block. Most predominant blockchain is public blockchain where the network of nodes in which each node will be aware of the data transmitted using this technology from one node to another node over the network.

As it is a decentralized approach, anyone can enter the blockchain and change the hash. Here two challenges will occur if any hash is changed; it automatically affects the next block hash. So, it is difficult to change all the blocks until the end. The second one is the algorithm maintained by blockchain technology. This technology depends on the algorithm called Proof of Work (PoW) used to validate the block, which is a key point of security in blockchain [9].

Proof of Work (PoW) indicates the process to make a block. It takes a long time to add or change in the blockchain. It is store on several machines not just on a central server. So, every node of the network will have a copy of blockchain. If any block is added or changed, it needs to be verified by every node in the network. Consensus algorithm will help in adding a new block into blockchain.

Another issue while dealing with blockchain technology is that each block header holds the previous block's hash value. Then there occurs to challenge that rise in the previous hash value of the first block. Every first block in the blockchain is known as genesis block, and the previous hash value of this block is zero by default.

III. Security Algorithms in Blockchain

Security in blockchain achieved through hashing on blockchain. Hash is a cryptographic mechanism that takes the arbitrary length input of any data like text (maybe string or single bit), audio, image, string, and so on [10]. From single bit to trillions of bits produces the fixed-length output where length depends on the type of algorithm used (SHA 256 / SHA 512). A hash function is a mathematical approach to un-reveal the block data, which are involved in the transactions and produces fixed-length output. It is difficult to get back the original data from the hash. Thus, it is a one-way hash function. Every produced output is of fixed length as shown in Fig. 2, and most of the output is smaller in size when compared to input.

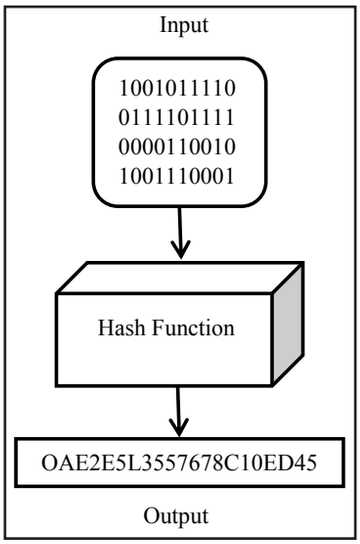

Fig. 2: General Procedure of Hash Function

Characteristics of the hash function:

- No change in the output given by hash function ever the input is repeated number of times.
- It is very faster in computation while deriving the hash of any input data.
- It is difficult to get the original data back even though it repeats the same has every time. If any of hash is reveal, it should crack through brute force method. If the input data is of smaller, then it is easy to break the hash back to original data, but it is not feasible for trivial input data which is of trillion sizes.
- No two-input data will have the same hashes; thus, hash function is resistant for the collision.
- Ever a single bit change in input data may affect the hash value.

Once the hash value has derived for given input data, it is difficult or impossible to get back the original data, unlike the traditional encryption and decryption standards. Thus, the hash function has annotated as a one-way function in which reverse is not possible with it. The advantage lies in the size of hash value derived irrespective of the input data given to it. For instance, if the input data is in trillion size say 1024, the hash value derived for that input data is only 256 bits (in case of SHA 256) or 512 bits (in case of SHA 512) depends on the algorithm used for hashing.

Table I: Security Algorithms Used for Hashing in Blockchain

Name	Type
MD (Message Digest)	MD1, MD2, …, MD6
SHA (Secure Hash Algorithm)	SHA0, SHA1, SHA2, SHA3

Table I lists various security algorithms used in blockchain for hashing, we generally use SHA2 that has 2 types of algorithms depends on the number of bits produced as output i.e., SHA-256 produces an output of length 256 bits, SHA-512 produces an output of length 512 bits irrespective of the input length.

IV. Role of Hashing in Blockchain

As the blockchain states linked together and each state is hashed with the hash function, it is difficult to derive the original input from the current state of the hash. This deriving process is known as mining. Mining the hashes to get back the original text can be done with the brute-force method; the miners will try every combination of hashes to get the original text. It is a trivial part in case of huge input data which is of trillion sizes and may take some years long to break the hash and CPU as well as memory.

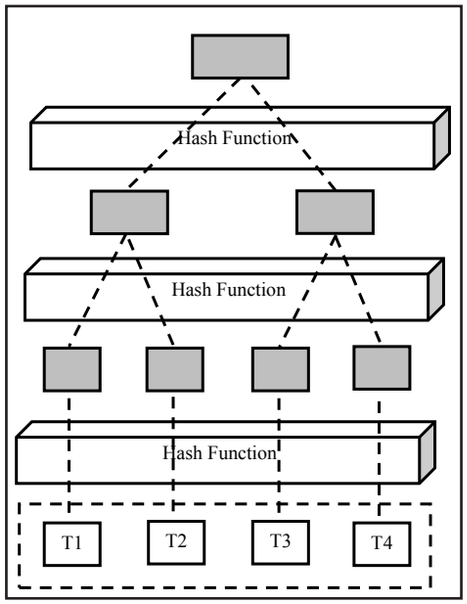

Fig. 3: Process of Obtaining Root Hash in the Form of Merkle Tree

To maintain integrity, which is one security reason every block is divided as transactional data and produces a separate hash for every transactional data. Here the block is hashed several times to get the root hash of that particular block. Each block, along with hashes, hashes of hashes, hash function at various levels derives the root hash of each block as shown in Fig. 3.

The specialized data structure to represent the Meta details of blockchain and acts as the core part of the blockchain. The Meta details hold the transactional data and produce their respective hashes by applying hash functions at different levels until a root hash is derive for every block. The intermediate hashes are also known as hashes of hashes. Merkle tree allows determining any changes in the Meta details or transactional data of any block by rehashing the original data and comparing these hashes with the previous hashes produced as well as with the root hash [11]. Although any suspicious activity will be determined by merkle tree. Thus, it provides security in every block.

V. Smart Contracts

It is the decentralized mechanism that agrees with the parties for transactional purposes. It is generally a code executing with blockchain technology that defines a set of rules to be followed by the peers involved in transferring process of this digital assets. Smart contracts give a sophisticated view of facilitating, verifying and enforce the negotiation and performance of the agreement between parties. These parties may be individual peers or institutions and the assets they own, which are formalized by smart contracts itself [12].

Smart contracts resemble the legal contracts as they back with only law and enforcement, but all of the legal standards are adopted [13]. It is a negotiation between parties at the time of executing the code. The procedure involves a decentralized approach that they do not involve any third-party consultants while performing the digital assets transactions. It follows a distributed mechanism where the assets deposited by one or more parties can being redistribute to other parties which are not known at the time of the contract initiation.

Smart contracts enforce code that defines standardized transaction rules at both the protocol and application level to reduce the transactional costs - the security they provide through tracking the performing of the transactions and exclusive transaction cost savings. A vending machine is a proved instance of smart contracts that it reacts to the situation to eject the product for the coins produced by the customer.

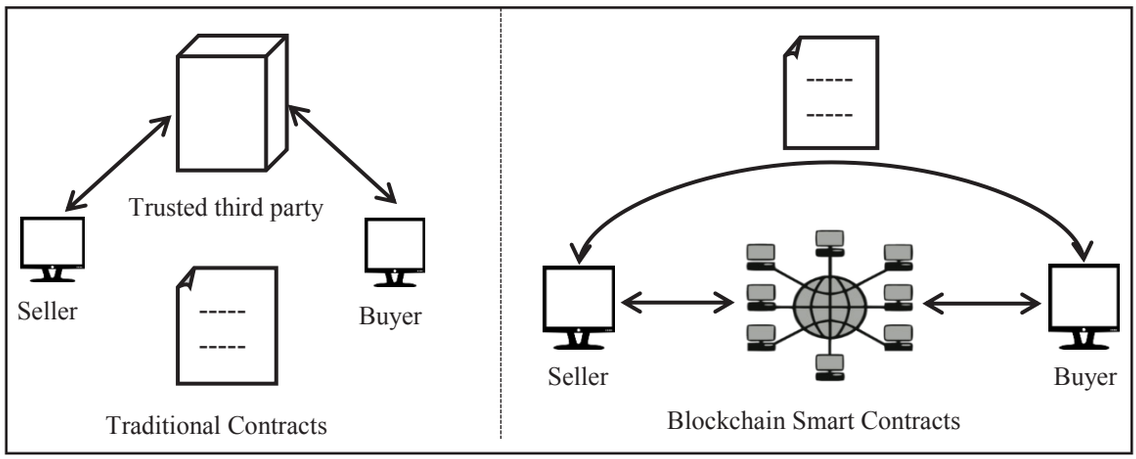

Fig. 4: Comparison of Both Traditional and Smart Contracts

Unlike the traditional contracts have as shown in Fig. 4, smart contracts verify the transactional data is blockchain. As the assets are chained directly through the network to both the parties so that integrity will be maintained throughout the transaction and the original details will be well known to both the parties which are at either end. Thus, smart contracts do not deserve any third party to be trusted as well as it provides high security. The characteristics of smart contracts include:

- Self-verifying
- Self-executing
- Tamper-resistant

The agreement itself indicates the transaction rule, so that has adopted between parties as well as the assets their own which are formalized in the digital form and follow legal obligations whenever the conditions met. All these legal obligations and rights that the parties should possess will be in the machine-understandable format for making the process automated. Thus, the network which shares the agreement code among the parties will guarantee a high degree of security as well as reduces the dependencies on the intermediates as well as provides lower transaction costs. This entire process is illustrated in the flow chart (Fig. 5).

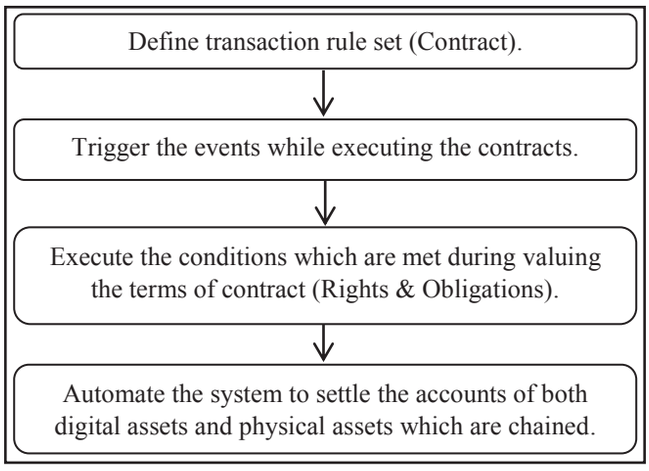

Fig. 5: Flow Process of Working on Smart Contracts

VI. Relation with Blockchain

Smart contract possesses valid set of transactions rules between the parties (maybe companies or people) who formalizes their relationship in terms of blockchain. Combination of blockchain with smart contract allows maintaining the integrity among different parties which area participated in digital transactions. Thus, the blockchain network allows verifying every node to identify the rightful owner of any product in case of buying and selling the product through smart contract.

```
/* contract attempts to get the coins*/
function transferFrom ( address_from,
address_to, unit 256_value) returns (bool
success){
/* checks if sender has enough */
if(balanceOf[_from]<[_value]  throw;
/* checks for overflow */
if (balanceOf[_to]+_value < balanceOf[_to])
throw ;
/* checks allowance*/
if (_value > allowance[_from][msg.sender]) throw
;
// substract from sender
balanceOf[_from]-= _value;
/* add the same to the recipient*/
balanceOf[_to]+=_value;
allowance[_from][msg.sender]-= -value;
Transfer(_from,_to,_value);
return true;
}
```

Fig. 6: Sample Program of Smart Contract

Sample contract to get coins is described below in Fig. 6. It is a module-based program, i.e., and every contract is program defined for a specific function. Here, while transfer the coins, one need to check the constraints like the balance of sender, the capacity of a receiver, sharing the transaction with other peers in the network and so on. As it uses SHA-256, the output obtained after hashing is to be 256 unit of length.

VII. Applications of Blockchain

As the blockchain resembles the database where it is the collection of any data, this state-of-art technology can be applied to various domains to make the respective data securely. The following are the fields associated with blockchain technology.

- Financial Sector: Blockchain technology reshaping the financial services to reduce the business transactions by allowing data incoherent, secured and crystal-clear manner. Predefined ineffectual business models are started to confront disruptions to begin highly systematized block chained based platforms [14].
- Money: Now a day's blockchain technology becomes the revolution in money purposes. They are decentralized and distributed that records in the public digital ledger which can be viewed across by the with an internet connection. It contains the cryptographical algorithms to ensure highly secure and reliable. It mainly avoids the third-party transaction fees during the transactions. In the technological view, it reduces the paper-based cash and third-party services (e.g. PayPal, skrill) and has global transactions. Examples of the crypto currency are bitcoin, Litecoin, Ethereum etc.
- Security: In all the sectors, identification plays a crucial role, but with the common comprehension it was facing significant obstacles like hacking databases and accounts [15]. By using the blockchain technology it overcomes those problems where identity can be in an irrefutable and immutable manner. By comparing both methods, the present system faces the password-based systems which can be hacked easily, while in the blockchain technology identity was done by digital signatures designed by public-key cryptography.
- Music: Main issues in the music industry were transparency and clarity of ownership. The user frequently checks the basic details of a song line composer, writer, and performer. This basic information is necessary to ensure that the creator gets paid for their work. By using blockchain technology, it creates the perfect database of music rights, to the transparent transmission of artist credits. Mainly it creates the decentralized system that introduces the system that fans could pay for the song only what they listened, and these smart contracts ensure this amount is split based on the predefined terms. Some examples of these decentralized system music system are Napster and lime wire [16].
- IoT: As per the cisco, 50 billion devices are coming to online 2020. IoT is a top-notching technology with centralized connected devices. With issues of IoT such as managing billions of devices, storing metadata, the

security it was combined with the blockchain technology which turns the IoT centralized system into a decentralized system. By combining these technologies many issues resolved like single node failure and for producing a more resilient system. To increase the supply chain management efficiently, blockchain and IoT technology together can improve the potential [18]. Manufacturing and transportation required the product monitoring system which can done with the combined technology. Some of the emerging areas where the combination of technology to be considered for more optimization and efficient. The complete picture has represented in Fig. 7.

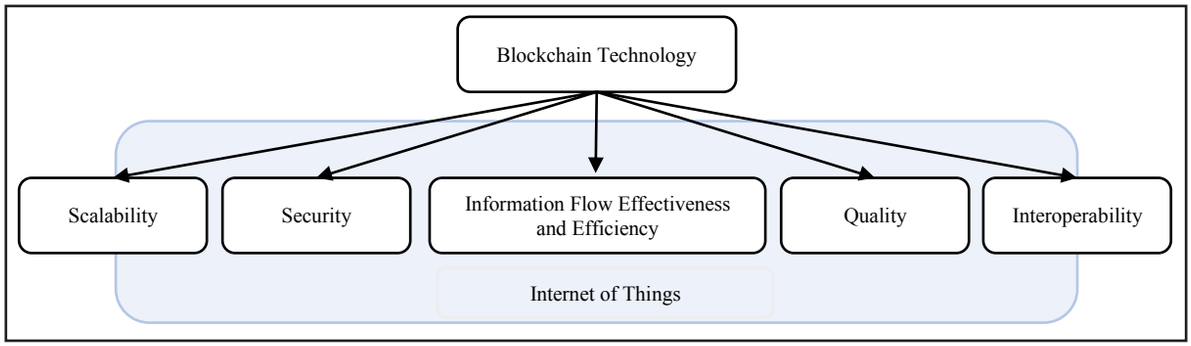

Fig. 7: Impact of Blockchain with IoT [17]

VIII. Challenges of Blockchain

Every technology includes pros and cons. Even the high secured blockchain also limited with some issues. Fig. 8 shows the challenges associated with blockchain technology.

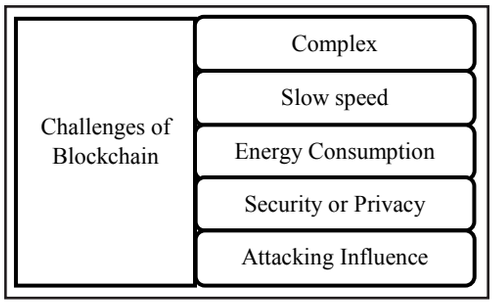

Fig. 8: Challenges of Blockchain

Limitations of Blockchain:

- Complex: The terms associated with blockchain technology is difficult to understand, such as consensus, chain, nodes, and miners and so on.
- Slow Speed: Time taken for the transaction is very long. As concerned with VISA, it will do 1000 transactions per sec whereas bitcoin does 7 to 10 transactions per sec.
- Energy Consumptions: For adding the block, the miners must solve the puzzle and spent lots of time while doing that. It will lead to huge consumption of resources.
- Security or Privacy: Every node will know the transactions while transmitting if the data is confidential, it will be watch by everyone.
- Attacking Influence: If the network possesses 51% of strength in networks as attackers, it will lead to an attack.

IX. Conclusion

Blockchain acts as a repository that can store any data and can applied to any field. In this paper, the intramural analysis of blockchain is projected. It includes the architecture, internal technique behind this state-of-art technology called hashing and smart contracts, which has applied along with blockchain can used over various sectors like banking, insurance energy, e-government, telecommunication, music & film industry, the art world, mobility, education and many more. Also, some of the applications have been discussed along with the challenges. This paper also proposed the impact of performances and the efficiency of the various applications with the combination of the Internet of Things through the blockchain technology. That can be applicable for scalability of the IoT applications as well as it impacts the auditing of the IoT solutions. Smart contracts are the code that uses solidity programming languages that resembles JavaScript and compiled on Ethereum virtual machine for creating contracts for voting, crowd-funding, blind auctions, multi-signature, wallets and many more. As the world follows the centralized mechanism where the entire network depends on the single server, blockchain answered to give the decentralized mechanism and security is maintained till the end block. It is difficult to crack any of the blocks even though it is openly available (public blockchain).

References

1. F. Casino, T. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55-81, 2019, doi: 10.1016/j.tele.2018.11.006.

2. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, and E. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *IEEE Symp. on Security and Privacy*, 2015, doi: 10.1109/sp.2015.14.
3. M. Miraz, and M. Ali, "Applications of blockchain technology beyond cryptocurrency," *Annals of Emerging Technologies in Computing*, vol. 2, no. 1, pp. 1-6, 2018, doi: 10.33166/aetic.2018.01.001.
4. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *IEEE Int. Congr. on Big Data (BigData Congr.),* 2017, doi: 10.1109/bigdatacongress.2017.85.
5. M. S. Hussain, P. Kanakam, and R. V. Edarapalli, "Exploring bitcoin cryptocurrency: An analysis, applications and it's market influence," *International Journal of Computer Applications*, vol. 181, no. 26, pp. 44-47, 2018, doi: 10.5120/ijca2018918112.
6. D. Knezevic, "Impact of blockchain technology platform in changing the financial sector and other industries," *Montenegrin Journal of Economics, Economic Laboratory for Transition Research (ELIT)*, vol. 14, no. 1, pp. 109-120, 2018.
7. D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," *Sequences II*, Springer, New York, NY, pp. 329-334, 1993.
8. J. Aron, "What's wrong with bitcoin?," *New Scientist*, vol. 221, no. 2955, pp. 19-20, 2014.
9. L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *IEEE 41st Int. Conv. on Information and Communication Technology, Electronics and Microelectronics (MIPRO),* 2018.
10. Z. Qi, R. Squires, M. Buer, and D. Chin, "Methods and apparatus for performing hash operations in a cryptography accelerator," U.S. Patent No. 7400722B2, 15 July 2008.
11. M. Szydlo, "Merkle tree traversal in log space and time," in *Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 541-554, 2004.
12. A. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *IEEE Symp. on Security and Privacy (SP),* 2016.
13. R. O'Shields, "Smart contracts: Legal agreements for the blockchain," 21 N. C. Banking Inst. 177, 2017. [Online]. Available: https://scholarship.law.unc.edu/ncbi/vol21/iss1/11
14. P. Treleaven, R. G. Brown, and D. Yang. "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14-17, 2017.
15. I. C. Lin, and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653-659, 2017.
16. J. Wishnia, "Blockchain technology: The blueprint for rebuilding the music industry," *Cardozo Arts & Entertainment Law Journal,* vol. 37, no. 1, pp. 229-262, 2019
17. A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the internet of things and blockchain technology in supply chain management," *Future Internet,* vol. 11, no. 7, 2019.