A SURVEY PAPER ON BLOCKCHAIN TECHNOLOGY AND IT'S REAL-TIME APPLICATIONS

R. Vamshidhar Reddy,
UG Scholar, CSE,
Guru Nanak Institutions Technical Campus,
Hyderabad, India.
vamshi777reddy@gmail.com

V. Jaya prakash Reddy,
UG Scholar, CSE,
Guru Nanak Institutions Technical Campus,
Hyderabad, India.
v.jayaprakash999@gmail.com

ABSTRACT: Blockchain characteristics and components made itself so powerful such that the word "Blockchain" became so popular from the last decade and had the most impact after the invention of the famous cryptocurrency "Bitcoin" by an unknown person or group named Satoshi Nakamoto. The main components of blockchain are Nonce, Mining, Hashing, Digital signature and consensus are explained in this paper. Types of blockchain are public Blockchain, private and consortium which is the combination of both public and private blockchain. The real-time scenarios where blockchain technology can be implemented or already implemented are mentioned in this paper and further work to be done on blockchain technology also explained at the end of this paper.

Keywords**:** Blockchain, Cryptography, CipherText, Confidentiality, Authentication, Integrity, Non-Repudiation, Decentralization, Smart-contract, Consensus, Nonce, Mining, Digital signature.

Introduction

Blockchain is one of the biggest buzz words from the last decade. The hype surrounding the blockchain is due to bitcoin. Most people think that Blockchain has evolved from Bitcoin. But, Bitcoin is just a cryptography like Ethereum (ETH), Ripple(XRP), Libra(LIBRA), Litecoin(LTC) which are developed from Blockchain technology [1].

Right now everything we know of (WhatsApp, Google, Facebook, Banks, Real Estate) runs in a centralized manner to get what we want. The centralized manner like a person, company, government, authority can be controlled by themselves and they can change their terms of service, rules and laws whenever they need/want. As of now, it is working well and we least bother about the centralized system. But changing the rules, Terms of service, laws etc. is a limitation for users. Another worrying thing is storing our data in a centralised server such that those who have authority can view and sell our data [2,3]. And these limitations can be overcome by using blockchain. In Blockchain, we need not interact with the company, authority, person, place directly to get what we want/need. The rules, terms of services, laws can establish accordingly while the firm establishes such that it can't be altered in future.

Blockchain is an Immutable Decentralized (no central server) or centralized peer-to-peer network based technology [4][5]. Blockchain made itself powerful due to concepts Digital signature, Merkle tree, Mining, Consensus Algorithms, Hashing, Node, Nonce [4].

This paper will give a brief information about blockchain technology, components involved in blockchain, types of blockchain, Real-time applications of blockchain technology and future work.

Blockchain

The formal definition of blockchain is "It is an open, distributed ledger that can record transactions between two parts efficiently and in a verifiable and permanent way". Blockchain is a decentralized computation and information sharing platform which enables multiple authorization domains who do not trust each other, to cooperate, coordinate and collaborate in a rational decision-making process [5]. In simple words, It is a technology that provides a platform to different(unknown) people to connect and work (get what they need) together. The blockchain contains a growing list of records which are known as blocks as shown in Fig.2 connected using cryptography and each block contains block header and block body. Such that Block header stores the previous block hash, timestamp, Nonce, Merkle root, current block hash.

Whereas Block Body contains entire transactions and hashes [5].

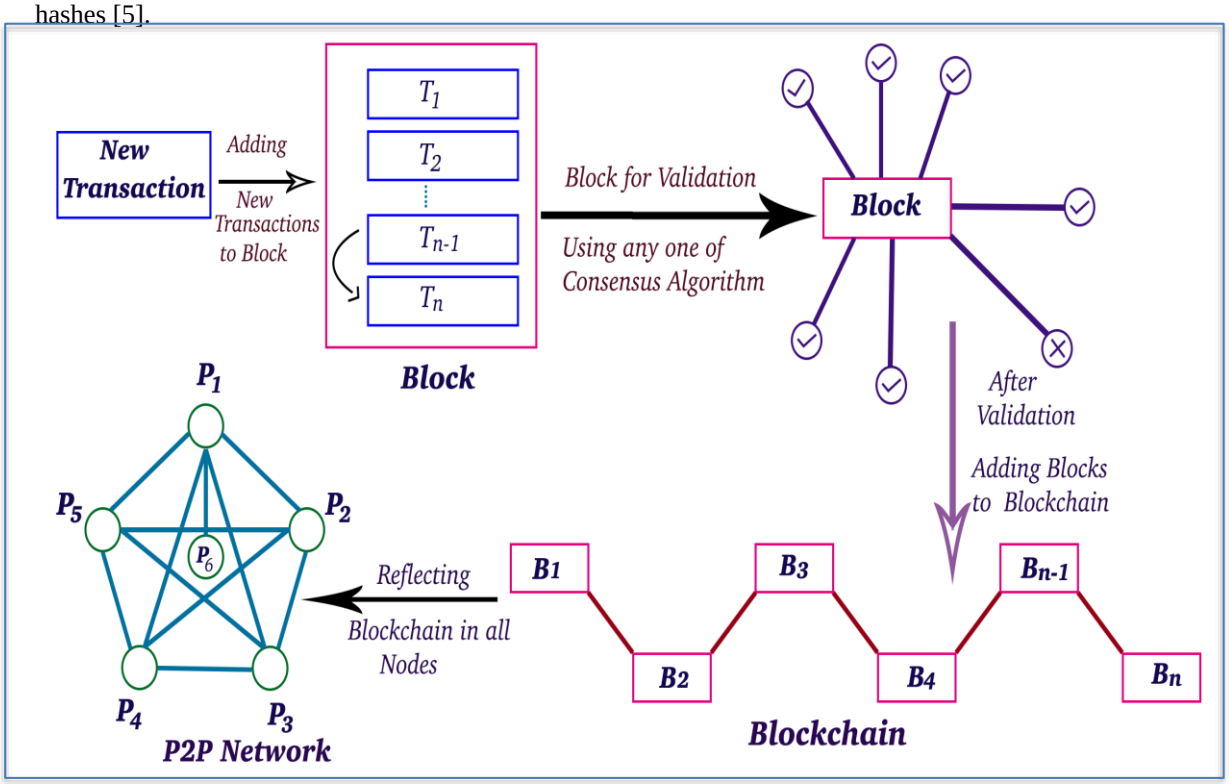

Fig.1. Architecture of Blockchain

Each block contains on average 500 transactions and size may vary from 1MB to 8MB. Mining statistics should be used to construct the block. The starting(First) block in Blockchain is known as the genesis block.

A new transaction can be added to the block and after reaching certain transactions in the block, miners requests for consensus algorithm and if it is accepted by >51% of nodes, then it can be added to the blockchain at the end by including previous hash in the new block as shown in Fig.2.

01. Components of Blockchain:

A. Hash function: In the blockchain, the cryptography hash function is used to hash the transactions as input and gives an output at a fixed size (32-bit or 64-bit or 128-bit or 256-bit) called as the hash. And it is a one-way hash function(OWHF) such that reversing of hash (fixed size output will not generate the input (Transactions) [6].

H(X)=X%n

- Where X is Message
  - H(X) is message Digest
  - n is the Nonce
- And H(X1) ≠ H(X2), if (X1 ≠ X2) and also accepts Avalanche Effect such that small change in the message leads to a huge change in output.

- Bitcoin mining uses SHA256 Algorithm.
  SHA 256 applied for "**Welcome to Blockchain"** text(Input) gives "**862d955a76a6b985f5d4b7cee5094e44fc0a1150bfef2f952743d2878819a9ea**" as hash (Output).

B. Nonce: Nonce is a random number (4 Byte field) which varies the Hash(Output) such that more Nonce is hard to break(Decrypt) [5,7].

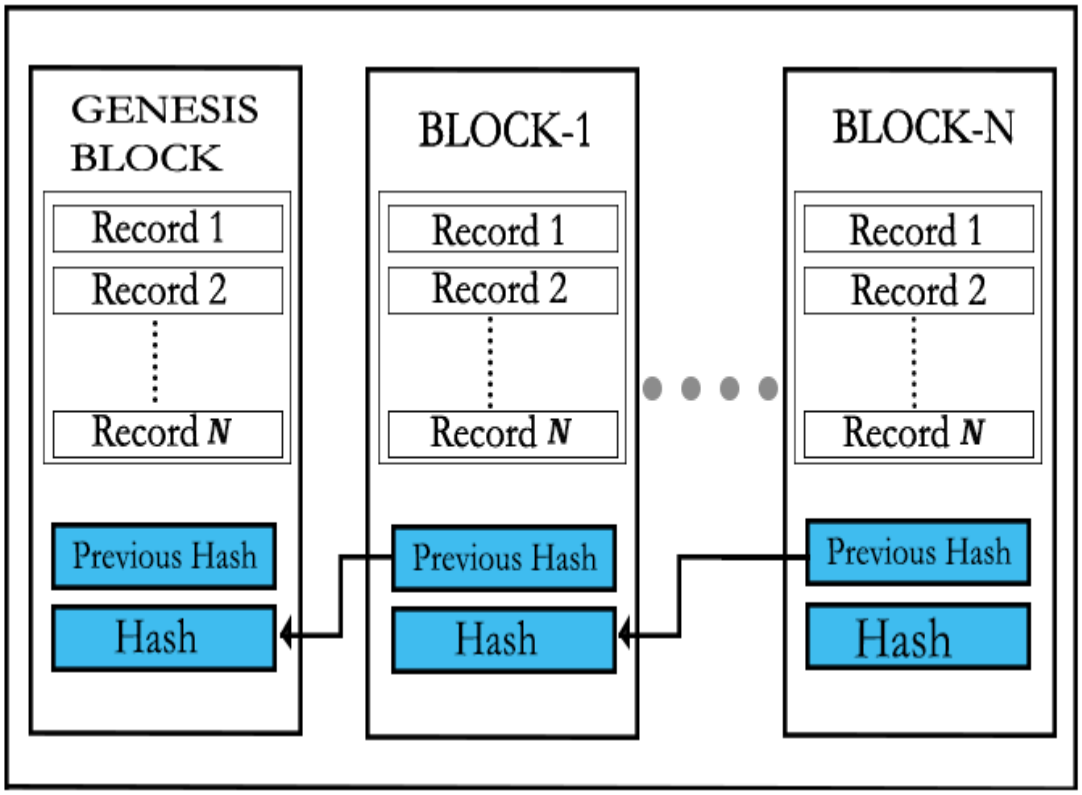

Fig.2. Blocks in Blockchain

C. **Mining:** Mining is the process of adding the blocks to the chain in blockchain by Miners. Miners construct the blocks and try to add it to the existing blockchain [5].

In Bitcoin: Bitcoins are generated during the mining-each time users discover a new block and these bitcoins generated per block are set to decrease geometrically, with a 50% reduction for every 210,000 blocks (Approx 4 years) such that miners will get fewer rewards as time progresses.

The theoretical limit for total bitcoins is slightly less than 21 million.

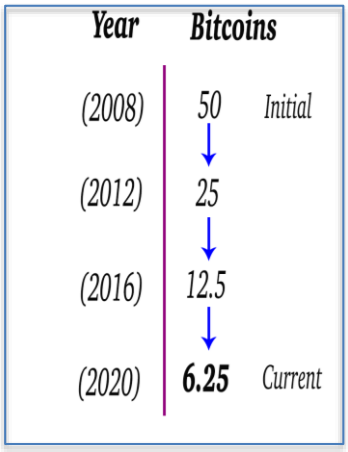

Fig.3. ***Bitcoins*** *Awarded to* ***Miners*** *for Mining*

D. **Consensus:** It is a procedure to reach a common agreement decentralized to take a decision to add the block to the chain. And ensures that the correct block is added to the chain and provides high security and fault tolerance [8].

Some of the Consensus Algorithm are mentioned below [9]:

a. **PoW:** Proof of Work consensus algorithm selects miners in a random process like trial and error method to generate blocks using a nonce. [9]
b. **PoS**: In Proof of Stack Consensus Algorithm the miner selection is based on the majority, Stack or wealth, age. [5]
c. **DPoS:** Delegated Proof of Stack Consensus Algorithm selects miner based on voting and election process.
d. **pBFT:** practical Byzantine Fault Tolerance consensus algorithm selects miner such that if a certain number of nodes approves. [5]

E. **Digital Signature:** By using cryptography we get confidentiality but Authentication is missing, which plays a major role in Peer-to-Peer (P2P) Network which can be achieved by Digital Signature. Digital signatures provide Authentication, Integrity along with Confidentiality.

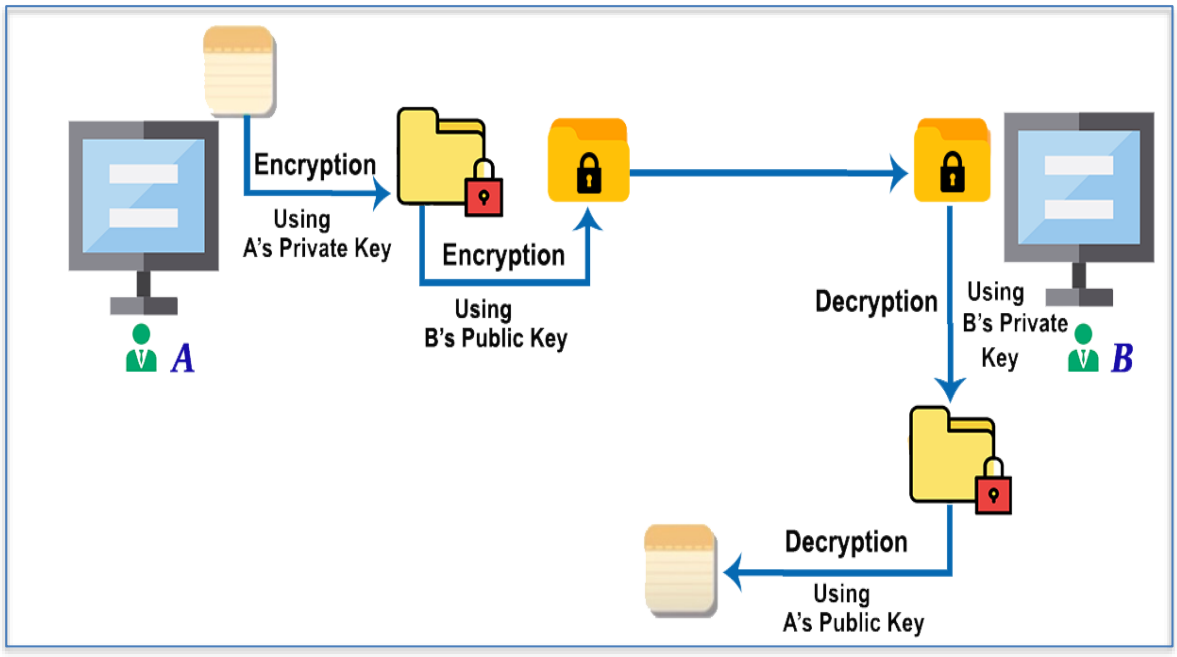

Fig.4. Digital Signature

Ex: If A(Sender) sends a file to B by encrypting it with B's public key.Receiver(B) decrypts with B's private key. But how B should be sure that this message(file) comes from A.It can be overcome by using Digital Signatures.

If there are 3 users(nodes) namely A,B,C.If A wants to send a file to only B: First it should be encrypted with A's private key followed by B's public key. So that B can decrypt it by using B's private key followed by A's public key. And C cannot decrypt the file as it should decrypt it with only B's private key which will have only with B.In this order only B can decrypt the file but C cannot. And B is sure that the file(message) comes from A, as it should be decrypted with A's public key first.

In this way Authentication along with Confidentiality is obtained by using Digital Signatures.

F. **Merkle Root:** It is a structure that allows for efficient and secure verification of content in a large body of data. [9]

G. **Smart Contracts:** Smart contracts in Blockchain provides a faster, cheaper and more secure decentralized platform and avoids the intermediate. [5]

02. Types of Blockchain

Basically, there are two models of the blockchain network based on permission criteria. They are Permissionless Blockchain Network and Permissioned Blockchain Network. But further, it can be classified into three types:

1. **Public Blockchain:** It is a permissionless blockchain network such that anyone(public) can look over the ledger and open to everyone to participate in the network. In this type of blockchain, the whole network will be decentralized and should use a permissionless consensus algorithm and no one can tamper the data [5].
EX: Famous cryptocurrency **BITCOIN**.

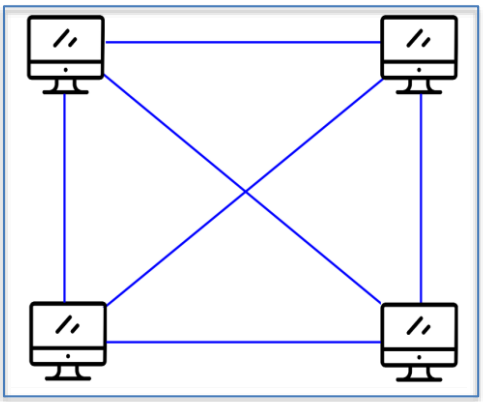

Fig.5. Public Blockchain

2. **Private Blockchain:** In this type of blockchain, predefined members get access to the network while consensus is building and those specific users can verify and add the blocks. It provides a higher level of verification and validation to transactions as it is centralized. [8]
EX: Ripple(XRP)

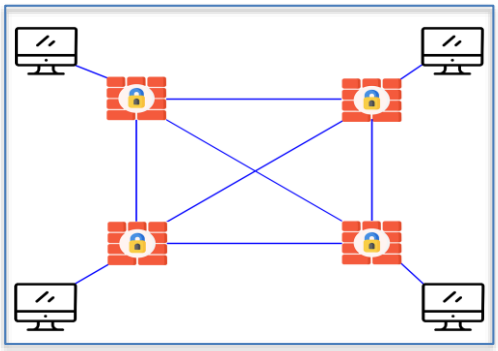

Fig.6. Private Blockchain

3. **Consortium Blockchain:** Consortium blockchain sometimes called a Federated Blockchain acts as an intermediate to both public and private blockchain such that blocks can be added into the chain once validation is done by few predefined users. It is partly decentralized. [8]
EX Quorum, Corda.

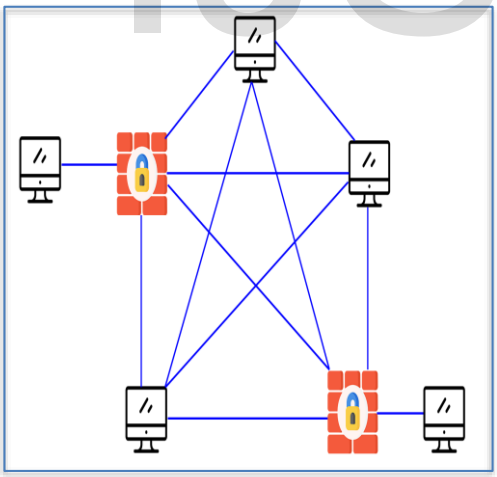

Fig.7. Consortium(Federated) Blockchain

Blockchain Applications

Blockchain technology can be applied in almost every place and can eradicate the centralised based systems.Pinyaphat et al. [3] mentioned that Blockchain technology can be implemented in the electronic health care system for Paying bills using bitcoins. Wubing et al. [9] highlighted the usage of smart contracts using blockchain technology to overcome the credit problems, risks while lending money such that the borrower's document can be revealed only once the loan is paid.

Some of the places where blockchain can apply are: Cryptocurrencies, Digital records, Energy, voting, Supply chain management, Education, Real estate, Finance areas like Insurances and Banking, Advertising.

a) Voting

As voting plays a major role in forming a government in most of the republic/Democratic countries. Normal EVM voting system may lead to tamper of votes which results in forming a different government, we can implement a decentralised voting system using blockchain technology such that people can elect the government genuinely[10]

b) Land Records

Almost all physical assets registrations and mortgage records can alter and modify which cause huge damage to both government and victims during registrations in the present system. Having a decentralized system to store the entire records with a timestamp can overcome the problem which can be accomplished by using blockchain technology. Such that, records entered by authorized persons can't alter and can provide security and trust to people. [9]

c) Healthcare

- As storing health records of each and every user in a centralized system is unsafe because storing the whole data(Records) under a single organization/person may lead to data misuse.
  As health records of particular users/citizens should store securely, we need a decentralized permission blockchain system such that only authorized persons after the particular user's permission can access the data (Health Records) and can save the life of patients in an emergency by checking the existing records of particular patient and even can update the records. [11]
- Wubing et al. [12] made clear that blockchain and artificial intelligence can solve the solutions for healthcare problems as the healthcare records have an issue with policy and privacy and need to provide an opportunity to track their own records.
- Wubing et al. [12] explored the usage of blockchain technology in healthcare from [13],[14].

d) Cryptocurrency

Starting from famous cryptocurrency BITCOIN to latest cryptocurrencies Zcash, Libra, Tether, Nano, stellar, Ethereum, Ripple, Litecoin, Peercoin, Omni, Emercoin runs through blockchain technology and can eradicate the physical currency and can save the time, cost for each transaction and can access the digital currency from anywhere throughout the world. And it is almost impossible to attack these applications and provide high security and trust. [10,12].

Nakamoto et al. [1] Explained how to use the blockchain technology in Cryptocurrency (Electronic payment system) and made a revolution over electronic cash and prevented double-spending problem using a peer-to-peer network by developing BITCOIN one of the most popular Cryptocurrency. Bitcoin is a completely decentralised, peer to peer, permissions cryptocurrency. Such that anyone can join and participate in it. Bitcoin maintains the longest proof-of-work chain with tamper-proof and every node/user can maintain a copy of whole records. Nakamoto[1] achieved it by including Digital signature, Merkle tree, Consensus Algorithms, Hashing, Node, Nonce

e) SolarCoin(Energy)

SolarCoin is the first digital currency-related to nature and it protects the natural capital. SolarCoin is the decentralized and non-government solar energy incentive program using blockchain technology. Based on the solar energy generation, Solarcoins can be granted and can use a digital currency. [2,12]

f) Supply chain management

In Supply chain management, the quality of the final product plays a major role. But the firms may not guess where the quality of goods changed due to multiple stages in between initial (Raw material) to the final stage (final product). So blockchain-based technology can solve these problems by providing the transparency such that organized persons can validate the transactions and can figure out the particular stages where good's quality gets changed because the blockchain-based system provides an interface such that records once entered can't alter(change). [15]

g) Education

The main problem in the current education system is fake certificates which results in unemployment for deserved people. So having a semi-decentralized permission blockchain system which contains all records can solve the above problem in such a way that once records entered by organized persons can't change and can store all the certificates can use it for authentication purpose. [16]

Zibin at al. [10] explained that blockchain technology can be applied to education in such a way that lessons(classes) are arranged in blocks such that students can earn coins once they complete reading the blocks.

h) Advertising

Due to a lot of advertisements on Televisions, Online, Offline(paper) people are unable to get whether the particular item is fake or real. And this problem can be solved by using Private blockchain system such that group of firms collectively forms at initial stage and declare a consensus such that new advertisements should follow(fulfil) the algorithm requirements and even can use any one of the consensus algorithms. [12]

i) Banking

Wubing et al. [12] highlighted that blockchain is being used in the Bank of England Santander along with payment protocol to transfer the payments in a real-time scenario using web/mobile application. And highlighted that Australian Securities Exchange replaced the current clearing system with blockchain technology to reduce the transaction costs and make every transaction safer and faster.

j) Insurance

Wubing et al. [12] explained the usage of blockchain in insurance by overcoming the traditional insurance policies and showed how to eradicate the brokers and can make it risk-free.

Conclusion

Blockchain technology can be applied in almost every place and can eradicate the centralised based system. As blockchain contains peer-to-peer nature and decentralised infrastructure. And can apply blockchain technology in the places wherever data is involved, such that stored data will not be tampered and we can own our data as **"Information is Wealth".** In this paper, we give an introduction to blockchain and make clear about bitcoin and blockchain technology and components involved in blockchain followed by types of blockchain and list some real-time applications and mention the work done on blockchain technology. We plan to do furthermore research on applying blockchain efficiently in healthcare and education.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.[Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] D.B.S.Suresh Kumar, D.Bala Krishna Kamesh, Dr. Syed Umar: "A Study on Big Data and its Importance" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 9, Number 20 (2014) pp. 7469-7479

[3] "Importance of Data"
Available:
https://www.import.io/post/what-is-data-and-why-is-it-important/

[4] Pinyaphat Tasatanattakool, Chian Techapanupreeda, "Blockchain: Challenges and Applications" DOI: 10.1109/ICOIN.2018.8343163 Conference: 2018 International Conference on Information Networking (ICOIN)

[5] Deepa Mahajan, Sarika Kadam "A Survey Paper on Blockchain Technology" International Journal for Research in Applied Science & Engineering Technology (IJRASET)ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue V, May 2019

[6] Rajeev Sobti, G.Geetha: "Cryptographic Hash Functions: A Review" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012
ISSN (Online): 1694-0814

[7] Ahmed Afif Monrat, Olov Schel´en and Karl: "A Survey of Blockchain from the Perspectives of applications, Challenges and Opportunities"
https://www.diva-portal.org/smash/get/diva2:1343319/FULLTEXT01.pdf

[8] Sandeep Kumar, Abhay Kumar, Vanita Verma "A Survey Paper on Blockchain Technology, Challenges and Opportunities" International Journal of Computer Trends and Technology (IJCTT)-Volume 67 Issue 4–April 2019

[9] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang,
" An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends"
Int. J. Web and Grid Services, Vol. 14, No. 4, 2018

[10] Blockchain: Opportunities for Health Care
Available:
https://www.healthit.gov/sites/default/files/4-37-hs_blockchain_challenge_deloitte_consulting_llp.pdf

[11] Wubing Chen, Zhiying Xu, Shuyu Shi, Yang Zhao, Jun Zhao. "A Survey of Blockchain Applications in Different Domains"
Available:
https://arxiv.org/ftp/arxiv/papers/1911/1911.02013.pdf

[12] Blockchain for Healthcare
Available:https://www.ehidc.org/sites/default/files/resources/files/blockchain-for-healthcare-341.pdf

[13] Will Blockchain Transform Healthcare?
Available:https://www.forbes.com/sites/ciocentral/2018/08/05/will-blockchain-transform-healthcare/#2e63a56c553d

[14] Blockchain Ready Manufacturing Supply Chain Using Distributed LedgerArticle · September 2016
Available:https://www.researchgate.net/profile/Radmehr_Monfared/publication/308163874_Blockchain_Ready_Manufacturing_Supply_Chain_Using_Distributed_Ledger/links/57fe2dde08ae7275640133b0/Blockchain-Ready-Manufacturing-Supply-Chain-Using-Distributed-Ledger.pdf

[15] Rakibul Hasan Sayed :"POTENTIAL OF BLOCKCHAIN TECHNOLOGY TO SOLVE FAKE DIPLOMA PROBLEM"
Available:https://jyx.jyu.fi/bitstream/handle/123456789/64817/1/URN:NBN:fi:jyu-201906253406.pdf