www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 9 Issue 05 May 2020, Page No. 25029-25038
ISSN: 2319-7242 DOI: 10.18535/ijecs/v9i05.4482

Blockchain in Depth

[1]Saransh Kotha*, [2]Pearl Patel

VIT Mumbai, INDIA

Abstract

Blockchain is defined as a group of unsegregated blocks over a P2P network. It is also considered as a decentralised ledger which holds the records of any online event. It offers a secure platform for knowledge and value transfer even in an untrustworthy network. In digital transactions on blockchain, each transaction is verified by all the nodes within the network using consensus protocol. Through this paper we will give a comprehensive overview of how Blockchain technology works, its current and future applications and how it can change the digital events in future.

Keywords: Cryptocurrency, Distributed Ledger, Blockchain, Smart Contracts, Bitcoin, Ethereum.

1. Introduction

A simple Blockchain is a linked list that uses hash pointers. This can easily act as a tamper evident log. This chain of data, when shared across a network creates a decentralized, trust less, secure and immutable Distributed Ledger.

In short, blockchain is a time-stamped collection of permanent data records stored within a block and operated by a network of computers that are not controlled by a single individual. Each of these data blocks is encrypted and bound to one another using the principles of cryptography. The data within the network is accessible to every peer within the network. Since it is a ledger of shared and immutable records, by its very nature all that is created on the blockchain is transparent, and the person responsible for a specific transaction is accountable for their actions.

These properties of blockchain were leveraged to create cryptocurrencies such as Bitcoin.

Bitcoin is the most popular real life application of blockchain. The first thing that comes into our minds when we talk of blockchain is Bitcoins. Bitcoins currently validate multibillion-dollar global market of anonymous digital transactions without any government interference. Cryptocurrency (i.e. bitcoins) is a modern form of digital asset, distributed on a network spread across a wide range of computers. The decentralised structure allows them to live free from the power of any central authority.

Our current digital transactions are governed by some central authorities where they are assumed to be trusted. We assume that the trusted third party is telling us the truth about our transactions and about our digital assets. Still the third party possess a threat what if its hacked, manipulated or jeopardized. Here is when Blockchain Technology comes in the picture. Its principle of decentralisation has remodelled the entire digital world by introducing distributed ledger, immutable blocks with digital assets of all the nodes within the networks and introduction of consensus protocol which is used to verify every transaction taking place in the network and eliminating chances of any cyber-attack. The blockchain is further classified into two types:

1. Permissioned Blockchain: It can be defined as the blockchain network in which there is no restriction to enter the network. It is like a public blockchain where anyone can participate.
2. Permissionless Blockchain: It can be defined as the blockchain network in which there are restrictions so that only the people who have permission granted by a particular individual or a group can join the network. It can be referred as a private blockchain where only selected people can participate.

Structure of the paper is as follows: Section 2 What is Blockchain Technology Section 3 Second Generation of Blockchain (i.e. Ethereum Blockchain) Section 4 Enterprise Blockchain (i.e. Hyperledger and R3 Corda) Section 5 Innovation and Hidden Dangers of Blockchain Technology. Section 6 Conclusion and References

2. Blockchain Technology

Blockchain is defined as a widely distributed database blocks of digital transactions that have executed and shared among the nodes within the entire network for verification the transaction. Blockchain records the transaction right from the beginning and all the blocks are immutable, hence one node can access any block to view the information which is public within the block but cannot modify it. All the participating nodes in the blockchain network are anonymous. The identity of any hidden transactions is represented and based on the public key. Since blockchain is referred as a linked list hence each block is connected to the previous block through its hash value and each new block is added to the chain in same fashion.

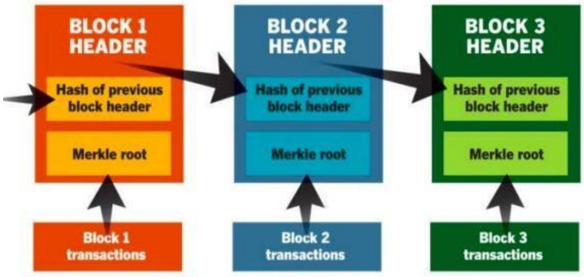


Fig. 1: Simplified Cryptocurrency Blockchain [Ref.: 16]

Elliptic Curve Cryptography (ECC) is a public key encryption technique which is used for authenticating each transaction. The elliptic curve general form over a finite field is:

y^2 = x^3 + ax + b

Elliptic curve point scalar multiplication is given as:

Q = P + P + P…

Repeated n times will give:

Q = nP

Some of the key parts of Blockchain Technology are as follows:

- **Block**: It can be defined as a ledger that holds all the digital transaction history which can refer to any form of transaction like money, agreements, land deed etc. The starting block of the chain is referred as the Genesis Block. These blocks are designed with certain rules and properties such as fixed size of the block, transactions holding capacity of the block etc. at the time of establishing the network. In bitcoin blockchain each block is created after every 10 minutes.

- **Chain**: Once a block is created it is added to the chain of blocks through a hash which is described below. Since blockchain is referred as a linked list therefore all the blocks are chained to each other through their hash. The hash value of the previous block is inserted in the new block as shown in the Fig.:1. This way a link is created between the old blocks and the new block. Since the hash value of any block is very volatile to changes, hence if any of the block is altered the hash value of the block will be changed and all the blocks after that block will be considered as faulty since the previous hash value will not match with the altered block's hash value. This way if there is any Cyber-attack over any block, we will be able to identify it. This makes each block within the blockchain immutable.

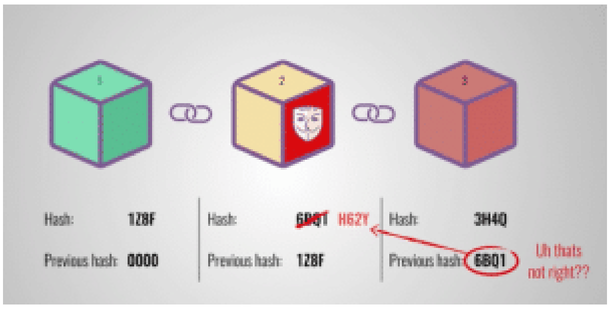


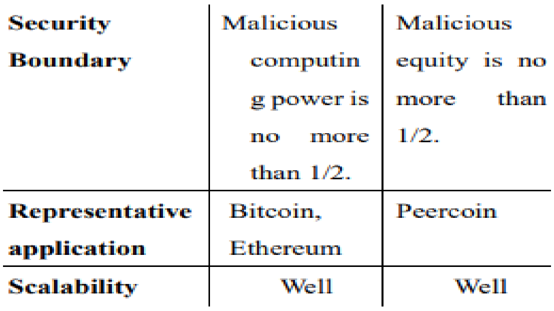
Fig. 2: Altered Block [Ref.: 17]

- **Network:** It can be defined as a collection of nodes or peers each containing a complete record of all the transactions on a blockchain. There is no centralised governing body that has control over the entire blockchain. Each node is referred as trustless node and data integrity is maintained by the blockchain being replicated on all of the node.[17]

- **Consensus:** this algorithm agrees with one consistent blockchain state, as it includes multiple copies on each network node. Consensus algorithm is used in order to validate any transaction within the network.

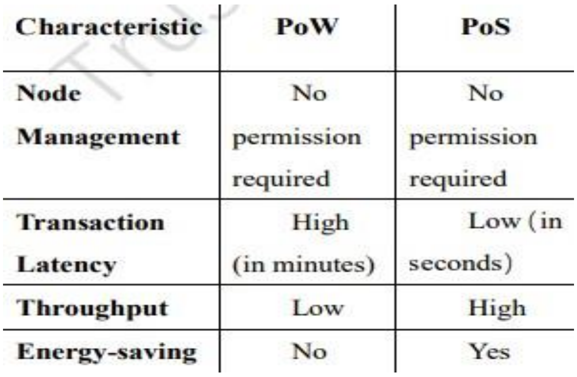
Within a network details of each transaction in public ledger goes to each node and using consensus protocols with majority of verification/ votes will decide whether the transaction will be accepted or there is double spending. To accomplish this, different schemes are used, such as:

- Proof-of-Work (PoW)
- Proof-of-Stake (PoS)



Security Boundary	Malicious computing power is no more than 1/2.	Malicious equity is no more than 1/2.
Representative application	Bitcoin, Ethereum	Peercoin
Scalability	Well	Well

Fig. 3.1: PoW v/s PoS[Ref.: 1]



Characteristic	**PoW**	**PoS**
Node Management	No permission required	No permission required
Transaction Latency	High (in minutes)	Low (in seconds)
Throughput	Low	High
Energy-saving	No	Yes

Fig. 3.2: PoW v/s PoS[Ref.: 1]

The interconnectivity of blocks within blockchain is based on **Merkle Tree** where the genesis block represents the root node, all the child nodes and leaf nodes represents the remaining blocks of blockchain and recently added transaction on the blockchain. The leaves contain the stored values, and each internal node is the hash of their two children.

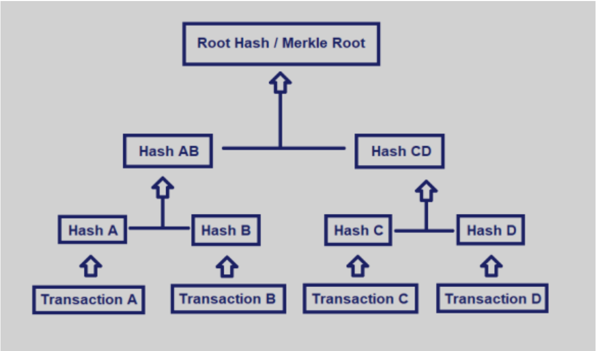


Fig. 4: Merkle Tree [Ref.: 21]

The process of adding transactions to the larger distributed ledger of existing transactions is known as **Mining**. It is used to protect and validate bitcoin transactions. Mining involves **Blockchain Miners** who are responsible for creating and adding the blocks with transaction data to network with past transactions. Blocks are protected in the ledger by the blockchain miners.[5] The miners uses advanced tools and the computing power of their own computers to validate the transaction.[8] The processing power or the computation power required is very large. Hence the miners who are utilizing so much of electricity and computational power are compensated with some rewards. In Blockchain after every 10 minutes a block is created which holds verified transaction record(copies). Thus, miners are responsible for developing blocks, verification of block and making transactions between two parties smooth and trustworthy.

Mining Pools are basically considered as a group of cryptocurrency miners who come together and share their computational power and resources over a network. A particular individual contributes its computational powers with others in order to find the block and get rewards quickly. The miners in the mining pool will be rewarded based on who finds the block first by calculating the hash code for the block and contribute to the blockchain. Mining pools consist of a pool manager who takes care of proper management of the pool. They take cuts of the reward for their work. For receiving the reward, individual miner who successfully found the block must show proof of work. All the mining pools are not the same i.e. they function differently and have different protocols. Setting up these mining pools can be very expensive, since for establishing such a pool requires lots of hardware equipment such as ASIC (Application Specific Integrated Circuit), CPU, GPU, FPGA (Field Programmable Gate Arrays). Mining pools generates revenue using the following formula:

MINING_REVENUE = BLOCK_REWARD

+ TRANSACTION_FEE

Some of the most common mining pools are as follows:

1. Proportional Mining Pools
2. Pay-per-share pools
3. Peer-to-Peer mining pools Mining Incentive can be calculated as follows:

If revenue > cost then:

Profit = revenue - cost

All the blocks in the blockchain are connected to each other through hash value. These hash values are calculated using Cryptography **Hash Functions**. Each block in the network consist of hash function of its previous block which is calculated as:

prevBlockHash = H(prevBlockHash)

They are specially designed in order to provide collision resistance property which plays a very important application of information security. A cryptography hash function increases the security and efficiency of a digital signature. In proof of work systems like blockchain, the **nonce** is used to make it more difficult to generate a valid hash for a given block. A hash value consists of 256-bit output. Miners must find a nonce value that, when plugged into the hashing algorithm, generates an output that meets certain requirements (a certain number of leading zeros).[18] Various hash functions used in symmetric key cryptography are either SHA-256 or SHA-

01. Hashing a block in the blockchain makes the block immutable as if anyone tries to tamper the block the hash value changes and the whole chain is affected and the future chains too, since the network won’t verify the blockchain as its history will be different. Nonce is considered as **partial preimage hash puzzle** since one part of the input will be given and other part of the input is to be calculated. Double hashing technique is used in bitcoin mining so that quantum computers cannot reverse the hash value and generate the information. In double hashing public key is first hashed with SHA-256 and then with RIPEMD 160 (which shortens the address size from 256 bit to 160 bit). It is possible to generate value of ‘n’ in Q = nP of private key from the value of ‘n’ of public key. This problem is known as **Elliptic Curve Discrete Logarithm Problem.**

Timestamp is used to check when the block was published in order to form a chain. Timestamp is used to prevent selfish miners. Each block will be timed and mostly issued after 60 seconds. If blocks in competition are received in roughly same time span, say 120 seconds of each other, then the block with fresh timestamp will be picked by miners. This increases the profits from 25% to 32%. A selfish miner with higher computational power like 40% could easily break this defence.

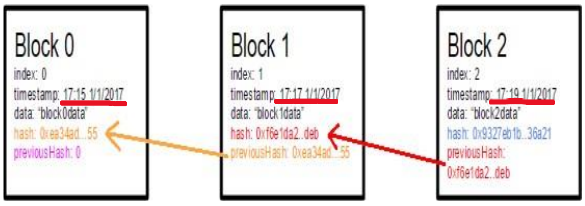


Fig. 5 Timestamp Blockchain [Ref.:19]

Byzantine Generals Problem: It is referred as a component in a distributed system. It was first introduced and published by Leslie Lamport in 1982 in his thesis titled “The Byzantine Generals Problem”. The concept behind the problem is whether a group of generals of different nations who are surrounding a hostile nation will reach to an agreement of attacking strategy by communicating with each other under the circumstance where some of them might betray and spread false information. Thus, it questions whether any consensus can be established among groups based on communication and transmission of false information within a distributed system. According to the problem:

- Each general has to decide either attack or retreat
- Once the decision is made it cannot be changed
- All the generals have to agree on the same decision and act accordingly

Hence two-third generals among which the information is transmitted must be saying the truth in order to solve this problem and this way we shall achieve consensus as a whole.[8] Similarly in context of Blockchain, let us consider each general as a node and all the generals (i.e. nodes) within a distributed network. Then in order to make distributed network execute properly consensus protocols are used such as PoW, PoS etc. Putting in simpler terms, majority of the nodes must reach to consensus on the current state of system which will provide authenticity and mutual approval.

Implementation: One node (general) will generate a message telling to attack or retreat and broadcast it. Since there are chances that the message can be tampered, that node will then generate a hash value for this message by hashing the message + nonce (for more strong hash value) and will broadcast it also. This hash value will become as a **hash target** for other nodes. The other nodes will simply hash the broadcasted message and will compare their hash value with the broadcasted hash value i.e. hash target. If the value is same, hence the message is broadcasted properly. Hashing happens very fast, the sender node has to spend time, recourses and computational power to produce the required value of nonce in order to generate the hash value. The concept of finding the nonce is referred as Proof-of-Work. If the malicious node even thinks of tampering the message then it first has to change the hash value which means to regenerate the nonce. This can be very time consuming and would require lots of recourses and computational power. This method is said to have solved possible extend of the Byzantine Generals Problem.

3. 2nd Generation of Blockchain

Ethereum Blockchain: in general, there are two approaches to create a consensus protocol to incorporate the advanced Blockchain-based applications. The following are the two protocols:

1. Creating an autonomous network and
2. Developing a protocol on top of an existing blockchain

The following solution however needs to automate an individual blockchain as well as check the requisite state transfer and networking code and most implementations will be too limited to merit their own blockchain.

Ethereum was first introduced in late 2013 and launched in 2015. It provides a blockchain with completely-fledged Turing-complete programming language that can be used to construct “contracts” that can be further used to encode arbitrary sate transition functions, enabling users to build new blockchain systems and decentralised applications simply by writing a few lines of code.

It currently is not using Zero-Knowledge proof but by making some necessary functionality changes for zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) a type of Zero- Knowledge proof is included in it.[30]

Ethereum Accounts: In Ethereum, the state is made up of objects called "accounts". There are two types of accounts in Ethereum:

1. Externally Owned Accounts (EOAs) and

2. Contract Accounts.

EOAs are simple accounts that have no linked code or data storage. They are governed by the private keys and used via software that is external to the Ethereum platform such as a wallet application. Contract accounts are managed by the contract code. It has a smart contract code but does not have a private key. Contract Accounts are owned (and supervised) by the logic of its smart contract. Once a message is received by the contract account, its code is allowed to read and write to internal storage and send certain messages or create contracts.

Ether (ETH): is the intrinsic currency of Ethereum to incentivise the computation within the network. The smallest sub denomination of Ether is the Wei. One Ether is defined as 10^{18} Wei.

Gas: It is a crucial part of Ethereum’s anti- denial of service model. Impedes any form of computational loss in the code. Each transaction on Ethereum is required to set a **STARTGAS** and a **GASPRICE**.

STARTGAS represents the maximum number of computational steps permitted for execution of a transaction. GASPRICE represents the fee the sender pays per computational step. “Gas” is the fundamental unit of computation. A computational step can cost 1 or more gas, depending on the how computationally expensive each step is. The transaction data also contains a charge of 5 gases for each bit.

Code Execution: The code in Ethereum contracts is written in a low-level, stack- based bytecode language, referred to as "Ethereum virtual machine code" or "EVM code". The code is composed of sequence of byte, where each byte is an operation. Code execution is usually an infinite loop consisting of repeatedly executing the procedure at the current program counter (starting at zero) and then incrementing the program counter by one until the process ends or an error or STOP or RETURN instruction is detected.

Smart Contract: A “Smart Contract” is a program which runs on Ethereum. Because it controls valuable things like Ether and digital assets, it is called a “contract”. They are unalterable computer programs that. Run as part of the Ethereum network protocol deterministically within the context of an Ethereum Virtual Machine. They’re written in high level language like solidity. They are compiled into low-level bytecode running within the EVM. Contracts can run only if they are called by a transaction (which can be initiated from an EOA).

Ethereum 2.0: Ethereum 2.0, ETH2 or Serenity is the next major upgrade of the Ethereum protocol. It intends to bring Sharding, Proof of Stake, a new virtual machine (eWASM) and more. With this it will speed up the transactions per second in order to increase the trade and with low fees. It will be introduced with main objective of moving the ETH's network from Proof-of-Work to Proof-of-Stake algorithm.

4. Enterprise Blockchain

A. Hyperledger Fabric

Hyperledger protocol was introduced for business-to-business and business-to- consumers transactions. It allows for acquiescence with regulations while supporting the varied requirements that arises when completing businesses work together on the same network. The network consists of some central elements such as smart contracts, digital assets, record repositories, a decentralised consensus- based network and cryptographic security.

[12] Since the traditional blockchain network was fallen short of meeting the requirements inherited in complex world of business transaction, challenges and threat to confidentiality for private transactions were extreme and to make business transaction trust-worthy, Hyperledger was introduced to meet the varied demands of modern marketplace.

Hyperledger is a permissioned blockchain with shared ledger. It takes novel approach towards traditional blockchain model by controlling and managing the admission/ participation of the participants within the network. Hyperledger responds to industrial use cases requirements by providing a secure, robust and scalable model for identity, auditability and privacy. Hyperledger is also useful in saving computational cycles. Hyperledger is considered as an open source community which focuses on developing suite of stable framework, tools and libraries for enterprise blockchain deployment. It was hosted by The Linux Foundation in December 2015. It is considered as an enterprise-grade, open-source distributed ledger framework. Since it is a permissioned blockchain, large enterprises adopted it and started private transactions, sharing confidential documents and other utmost important businesses. For private industries using Hyperledger fabric, identity of the participant is the primary requirement. It uses Smart Contracts, also called chaincode, which comprises the distributed logic processing and agreement of the system. It also controls the overall transaction process over the network. It can be drafted according to the demands of the business. Hyperledger uses X.509 certificates to generate public keys. There are in total two types of consensus algorithms i.e. SOLO which developers usually use to play with the Hyperledger Fabric Networks [31] and KAFKA which is used for production. Since it is Crash fault tolerant, not Byzantine fault tolerant, it prevents system from reaching agreement in the event of malicious or defective nodes. [31]

Hyperledger uses "Open Governance" model where the hyperledger Technical Steering Committee (TSC) is final authority. This committee has 11 members and is changed every year. The new team is selected from hyperledger environment's active contributors and maintainers through voting.

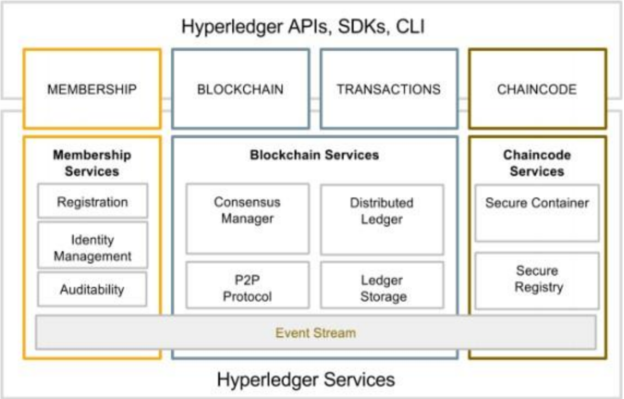


Fig. 6: Hyperledger Reference Architecture [Ref.: 12]

Hyperledger Fabric also provides a feature called plug-and-play of various components. This allows to reuse any existing feature and ready-made modules. For e.g.: if participant verification function already exists, then an enterprise network simply has to plug-in and reuse the existing module instead of designing a new one.[29] The hyperledger greenhouse hosts various projects from hyperledger labs for developing business for codes which are ready for production.

Hence hyperledger fabric is a codebase combined with Digital Assets, Libconsesus from Blockstream and OpenBlockchain from IBM and Hyperledger sawtooth developed at Intel's Incubation group.[32]

B. R3 Corda

Corda is a distributed ledger which aims to provide a platform for decentralised app development. Corda is drafted in such a way that it automize all the real-world transactions in a legitimate manner and executes the following on an open network where various other applications can be implemented with smooth interoperation. It does this by putting identity, finality of transactions, privacy and open governance at its heart.[34] It is built from the ground up to record, manage and synchronise agreements and legal contracts designed for use by regulated enterprises.

Corda is defined as a P2P network of nodes. Every node serves as a legitimate entity (a person or a company). Every legitimate node is running the corda programs (an occurrence of corda and multiple corda applications is termed as CorDapps). All of the nodes within the network are able to connect with each other. But they only consider a transactions between a group of parties. There are no global broadcasts as in the Bit**II.**in blockchain. This ensures privacy of data.

State artefacts are an arrangement among two or more parties which is controlled by smart contracts. Every node within the ledger is considered as immutable since corda follows UTXO model which is referred as Unspent Transaction Output model. States may hold random data, which would allow them to portray facts of any kind. The ledger expands over a period of time with the flow of transactions. Such transactions accumulate current state objects and create new state objects.

Consensus: To determine if a transaction is valid, there are two different types of consensus: Validity Consensus and Uniqueness Consensus.

1. **Validity Consensus**: Transaction is valid only if it has all the signatures of the involved parties and it is contractually valid. The smart contracts accepts the transaction as an input and decides if the transaction is legitimate according to the contract. Once it is approved, the state will be changed and added to the ledger. Contracts thus enforces laws over time on the evaluation of states.
2. **Uniqueness Consensus**: It is important to rectify whether the transaction proposed is true or not, in order to prevent double spending attack. Uniqueness Consensus is provided by notaries. Each state has an appointed notary cluster – an observer predetermined to be a group of mutually trustless individual. The transaction which is proposed will be signed by the notary cluster only when they verify whether the proposed transaction is authentic or not. Corda ha a feature called “pluggable” consensus which gives notary cluster a facility to decide which consensus algorithm will be a best fit depending on their requirements in terms of privacy, compliance with the legal system, scalability and algorithmic agility criteria.

The uniqueness consensus is not required to check the validity of the transaction itself. This means that the full contents of any transaction need not be seen by the uniqueness services which significantly increases the privacy and scalability of the system in comparison with other distributed ledgers and blockchains.

5. Innovation and Hidden Dangers

A. Innovation Opportunities in Blockchain

With more and more advancement in Blockchain Technology, various industries and multi-nationals are investing in this technology by contributing towards blockchain source code and developing projects. A report of an survey conducted by GitHub in 2010 there were less than 1% projects on Blockchain and in 2017 the numbers ran up to 11%. Various companies have developed multiple open source platforms or ecosystems for developers such as Bitcoin, Ethereum, Hyperledger and Ripple. Various international alliances have emerged such as R3 Corda, Hyperledger Blockchain supported by Linux Foundation, Enterprise-level Ethernet Alliance (EEA) and so on.[1] Apart from cryptocurrencies blockchain has various decentralised applications such as:

1. **Cryptokitties**: It’s the first ever Blockchain game on the internet developed using Ethereum framework. This game allows user to buy, breed and sell virtual kitties.[20]
2. **Notary Public**: Various legal documents can be authorised using blockchain technology which will eliminate the middle man and the centralised body. All these documents can be digitally coded using smart contracts and using consensus protocols we can make sure the documents are highly secured and protected

from any cyber-attack.[8]

3. **Entertainment Industry**: Decentralised application (Dapps) can be created in order to store the authenticity of any record in order to protect it from plagiarism. Ownership rights, Authenticity etc. can be protected using blockchain technology.[8]
4. **Election System**: Blockchain technology can be used in order to present the data for voters during elections. It will terminate the fake accounts since the data within the blockchain cannot be tampered.
5. **Blockchain based Anti-forged Solution:** Blockchain technology can be used to improve the current anti- forged mechanism. One can visualise a scenario where various product owners store the certificate of authenticity of their product over a blockchain network so that in case of any plagiarism the real owner can prove the authenticity of their product.[8]

Some of the other applications of blockchain can be considered in financial and non-financial services since Blockchain Technology is the backbone of various financial services such as Cryptocurrencies. The concept of Smart Property can be used to control the ownership of various physical as well as non-physical properties and assets via Blockchain using Smart Contracts. Blockchain Technology also has endless non-financial applications. We can visualise putting various consensus algorithms in order to prove the existence of various records like legal documents, music albums, shifting of ownerships, notary, highly classified government documents etc. within a blockchain network. Blockchain can also be used to provide decentralised storage. Storj [37] is a peer-to peer cloud storage network that allows users to transfer and share data without reliance on a third-party storage provider. In decentralised IOT platforms, blockchain can serve as the general ledger to keep a authenticated record of all the information exchanged between smart devices.

B. Hidden Dangers of Blockchain Technology

With less than a decade after introducing Blockchain Technology it is already becoming the most secure network protection technology worldwide. But this technology is still very young and it has different hidden dangers related to security of application, stability, business model and many more. The following are some of the major problems concerning blockchain technology:

1. The outcome cannot satisfy the tree requisites of “high quality low energy”[1]
2. Blockchain has very low transaction throughput and higher frequency service is difficult to meet.[1]
3. Considering the consensus algorithms used by blockchain such as PoW is not economical since it requires lots of energy, high maintenance etc. This results in resources exploitation.[1]
4. Since blockchain is a brand new technology hence it’s applications are undeveloped in certain provinces.[1]
5. As of security, blockchain is facing some problems in application security like privacy policies protection, harmful information, smart contact vulnerabilities, consensus mechanism and private key protection.[1]

Apart from the above mention dangers there are some other threats or attacks to blockchain technology such as:

1. **Double Spend Attack**: If a node say P1 wants to buy goods worth of 20 BTC (bitcoins) from 2 other nodes (i.e. P2 and P3) and has 10 BTC, then P1 ask P2 to update his ledger and similarly asks P3 to update hisledger. This way P1 will be double spending.
2. **Sybil Attack**: When a person creates multiple identities as node within a network to cast votes in its favour for miscellaneous transaction.
3. **50% Attack**: When a network consists of a dominated group of miners which can be achieved if the computational power of group of or individual miners is more than the entire network then the blockchain is forged/attacked and these miners will now control the blockchain.
4. **Goldfinger Attack**: If a bet is made on the fall of value of the BTC and using double spending attack one can make it happen to gain profit.
5. **Censorship Attack**: These are mainly attacks over a particular node within a network which is already under attack. It is further classified into 3 types:

a. Blacklisting

b. Punitive Forking

c. Feather Forking

The process in which a blockchain is diverged into two different parts due to network's transaction history or new rule in deciding what makes a transaction valid or due to selfish mining(attack) is called **Forking.**

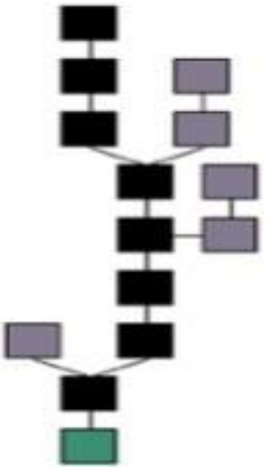


Fig.7: Forking in Blockchain [Ref.:8]

6. **Selfish Mining:** Suppose a miner found a block and instead of publishing it within the network he will hold it and try to add another block which makes two blocks in a row with miscellaneous data before any other miner then he will be able to create a longer chain and can fool the network.

6. Conclusion

Blockchain is one of the most developing and innovative technology which is expanding its horizon just not in the field of cryptocurrency but also in variety of fields like energy, entertainment, banking, notary and many more. Blockchain restores the entire power of the transaction network to the network users, rather than any centralised authority. This provokes the ideology of decentralization. Decentralisation ideology has changed the way users used to interact with the internet and this made blockchain a key part of Web

3.0 revolutions. We introduced about what blockchain is. Leveraging on it, we listed key terms such as hashing, network, blocks, mining, timestamps, miners, hidden dangers, attacks, innovation opportunities, application in the field of Bitcoins, Ethereum, Hyperledger, R3 Corda.

With the above discussion we can conclude that innovation and development of blockchain technology looks very promising.

References

[1.] http://www.caict.ac.cn/english/yjcg/bps/201901/P020190131402018699770.p df

[2.] https://www.slideshare.net/bhargavamin1/whitepaper-on-new-research-on-hashin

[3.] https://bitcoin.org/bitcoin.pdf

[4.] https://www.quora.com/What-is-SHA-256

[5.] https://intellipaat.com/blog/tutorial/blockchain-tutorial/what-is-bitcoin- mining/

[6.] https://www.investopedia.com/terms/m/mining-pool.asp

[7.] https://bitcoin.stackexchange.com/questions/11471/what-are-the-advantages-and-disadvantages-of-pooled-mining

[8.] Blockchain Exhumed by Dr. Dhiren Patel, Mr. Jay Bothra, Mr. Vasudev Patel

[9.] Securing Images with Fingerprint Data using Steganography and Blockchain by S. Pramothini, Y.V.V.S. Sai Pavan, N. Harini

[10.] https://blockgeeks.com/guides/hypothetical-attacks-on-cryptocurrencies/

[11.] Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

[12.] https://blockchainlab.com/pdf/Hyperledger%20Whitepaper.pdf

[13.] https://github.com/ethereum/wiki/wiki/White-Paper#ethereum

[14.] https://ethereum.org/wallets/

[15.] https://consensys.net/blog/news/90-ethereum-apps-you-can-use-right-now/

[16.] https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf

[17.] https://generanetworks.com/blockchainforlotteries/

[18.] https://www.quora.com/What-is-the-concept-of-nonce-in-blockchain

[19.] https://medium.com/@lhartikk/ablockchain-in-200-lines-of-code- 963cc1cc0e54

[20.] https://en.wikipedia.org/wiki/CryptoKitties

[21.] https://hackernoon.com/merkle-trees-181cb4bc30b4

[22.] https://lightrains.com/blogs/what-is-meant-by-forking-blockchain

[23.] https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained

[24.] https://medium.com/wolverineblockch ain/blockchain-the-byzantine-generals-problem 2f17097bad73

[25.] https://github.com/ethereum/wiki/wiki/White-Paper

[26.] https://ethereum.org/

[27.] Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood

[28.] https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0- phases/

[29.] https://www.investopedia.com/terms/h/hyperledger-fabric.asp

[30.] https://blog.ethereum.org/2016/12/05/zksnarks in-a-nutshell/

[31.] https://jktech.com/insight/blogs/consensus-in hyperledger-fabric/

[32.] https://www.hyperledger.org/about

[33.] https://docs.corda.net/

[34.] https://www.r3.com/white-papers/the-cord platform-an-introduction-whitepaper/

[35.] https://www.r3.com/white- papers/corda technical-whitepaper/

[36.] Blockchain Technology: Beyond Bitcoin - http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

[37.] https://storj.io/storjv2.pdf