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- Available at www.ijraset.com

A Survey Paper on Blockchain Technology

Deepa Mahajan[1], Sarika Kadam[2]
[1, 2]*Computer Department, SPPU PuneUniversity*

Abstract: Block Chain is mainly used for Cryptocurrency i.e Digital Currency which is used in verification and currency units of Fund transfer are independently operated without a central bank. Characteristics of block chain are explained in this paper. There are 4 types of characteristics such as Decentralization, Persistency, Anonymity, and Audit ability. A Consensus algorithm is used in blockchain. Key factors of blockchain are introduced such as Decentralized & distributed, Secure, Next smart contract, consensus & immutable. Here block structure and hierarchical layer explained in blockchain example: Data Layer, Network Layer, Consensus Layer, and Incentive Layer, contract Layer & application Layer. , Also some features of blockchain are explained which are Public Distributed Ledger, mining, Proof of work and hash encryption. We have explained the types of blockchain viz. Public Blockchain, Private Block Chain & consortium. we have explained the applications of block chain.
Keywords: Block chain, Distributed Ledger, Crypto currency, security, consensus,

I. INTRODUCTION

Block chain is a distributed digital ledger that is open, shared and highly secured, which means, all the records are immutable and verifiable[8]. ledger is commonly used in the banking operations as it is the official record keeper used to verify data transactions. Blockchain technologies are not just only single one technique, but contains Cryptography, and economic model, combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronize problem. Blockchain has a public ledger and all transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have implemented for user security and ledger consistency[5]. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity, and auditability. In a blockchain, smart contract is a code fragment that could be executed by miners automatically. There are two general high-level categories for blockchain approaches that have identified: permissionless, and permission. In a permissionless blockchain network, anyone can read and write to the blockchain without authorization. Permission blockchain networks limit participation to specific people or organizations and allow finer-grained controls. Blockchain technology is the foundation of modern cryptocurrencies [3]. Users utilize public and private keys to digitally sign and securely transact within the system. For cryptocurrency based blockchain networks which utilize mining users may solve puzzles using cryptographic hash functions blockchain technology is more broadly applicable than cryptocurrencies architecture. Section 2 shows concept of blockchain and principal of blockchain [7]. Section 3 introduces feature of blockchain and also explain key attrubute. Section 4 summarises the different type of blockchain Section 5 discuss characteristics and taxonomy of blckchain and Section 6 concludes the paper and feature scope of blockchain technology.

II. BLOCKCHAIN

Blockchain is decentralized and Distributed Digital ledger system used transaction record and store across many computers in a peer o peer networks. Blockchain was originally designed for the crypto-currency Bitcoin . Blockchain can be applied to record track and confirm transaction for virtually anything of value without the need for a central authority. Blockchain is unique it creates trust in the data before a block array to the chain. Blockchain technology is such as a game changer no more intermediate, currently, when doing business with one another it's don't show the other personal financial and business record listed. They rely on trusted intermediaries such as bank or lawyer to view our record and keep this information confidential. These

Intermediaries build trust between the parties and able to verify. Blockchain technology is not a single network it can be implemented in many different ways. It is completely public and open to everyone to view and access other can be closed to a select group of the authorized user as a group of bank or government agencies. Blockchain is secure and tamper-proof. it reduces risk and cost.

A. Key factor of Block chain technology

1) *Decentralized and Distributed:* conventional database in which data is stored in a central data server, the data in a blockchain is stored in multiple computers across the network. Any valid updates made to data on one computer is distributed to all the computer across the network. This makes it impossible for someone to corrupt or manipulate the data.

2) *Secure*: Each block of the blockchain is encrypted using advanced encryption techniques. Each block is linked to the previous block making transaction tamper-proof. Blockchain can be permissioned or permissionless. The access level of each participant in the blockchain network can be controlled.
3) *Smart contracts:* Smart contracts are rules that govern a transaction that participants can carry out in the blockchain. Smart contracts are stored on the blockchain and are executed automatically as a part of a transaction. The smart contract ensures that all parties adhere to the rules, that are present on the blockchain
4) *Consensus:* there must be an agreement between all relevant parties before a transaction can be executed. The transaction is verified and committed to the ledger through various means of the consensus algorithm.

Consensus Algorithms as

a) Proof of work
b) Proof of shake
c) Practical Byzantine Fault Tolerance(PBFT)

5) *Immutable*: Blockchain technology make it impossible transaction to tamper with transactions. If a transaction is tampered with, then the hash of the block changes. This hash will not match with reference on the next block of the blockchain. if the tampered block is distributed to the blockchain network, the nodes on the network will recognize this as a tampered block and will reject.

III. RELATED WORK

A. Concept of Block chain Block

Blockchain store transaction records in blocks. Blocks are linked together to a form of a chain. Hence the name block chain. Each block contains the following data. The hash that uniquely identifies the block.

Block tructure

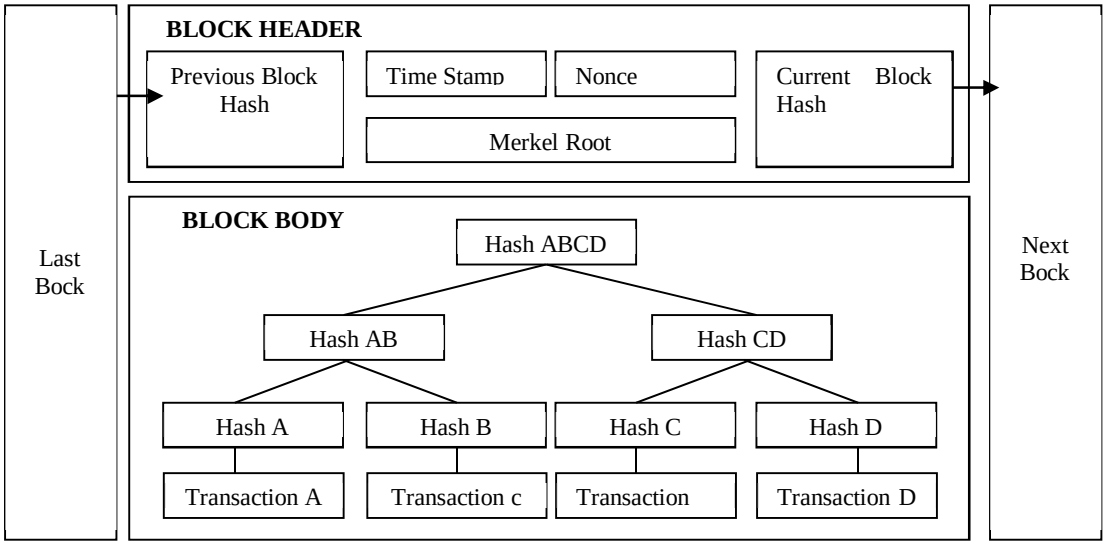

Fig 1: structure of Blockchain Block

Block structure has two parts block header and block body Blockchain is a data structure formed by a time sequence of blocks[6]. The block is a collection of data containing related information and records. The data structure of the blockchain is mainly composed of a block header and a block body, blocks are interconnected into a chain that records all of the transaction information across the entire network. These data blocks are broadcast in real time to the entire shared network. Block header stores metadata and size are 80 bytes. the block header contains the hash value of the previous block, which is used to connect the previous block to ensure the integrity of the blockchain. Block body stores business data and size is variable. Block body contains the main information of blocks (such as transaction record) timestamp is related as mining competition and also same as a nonce. Markle tree is a hash of binary tree which is validating of the integrity of the data structure. It requires a hash node pair as a leaf node, making node pair hash and inserting a new hash node. The hash process generates a unique Markle root. which is used for business record[10]

B. The Principle of Block chain

Block chain is a combination of a variety of technologies. hierarchical architecture of a blockchain has six layers from bottom to top: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer

1) *The Data Layer:* Encapsulates the data blocks, this layer related to data encryption and time stamp[7].
2) *The Network Layer:* Included distributed networking mechanism, data propagation and verification mechanism[7].
3) *Consensus Layer:* Encapsulates consensus algorithm of the network node.
4) *Incentive Layer:* Integrate economic factors which is including economic incentive and distributed mechanism[7].
5) *The Contract layer:* Is the main encapsulation algorithm and the smart contract, which is the basis of the blockchain programmable characteristic[7].
6) *The application layer:* Encapsulates the various applications[7] of the blockchain such as time-stamped blockchain, economic incentives depend on consensus computing.

IV. FEATURES OF BLOCKCHAIN

A. Public Distributed Ledger

Publicly available for anyone to access and view which means everyone has access to all the records. if the user wants, they can access all the records from the time the blockchain was created Any additions to the block are permanent means any change, major or minor is recorded into a new block and can not be altered. The ledger is distributed and it can not be altered by hacking into the central authority. Any changes have to approved by a majority of the people in the network. The blocks can contain transaction details for assets other than money like property, vehicles[8]

1) *Proof of work:* PoW is a work called mining in Bitcoin. Network participants calculate a hash value by adding anyone (any given value) to the collection of transaction data delivered to them. It is required to obtain a value smaller than a certain value,14 and the participants have to continue calculations by using different nonces until they obtain the value as required. When anybody obtains the relevant value, network participants mutually confirm the correctness of the value and the collection of transaction data used for the calculations is approved to be official transaction results as a new block[10]. Then, bitcoins are granted as a reward to the person who succeeded in obtaining the correct value through the calculations. After that, all participants go on to the next mining using transaction data that were not included in said block and the newly created transaction data[8].Bitcoin employs PoW to create a mechanism that can prevent falsification of data and duplicate payments without a central authority and can maintain the system against any attacks by malicious users

A block contains a number of different transactions. Each block has its own hash, transaction details, nonce, and previous hash.

a) *Previous hash*: The previous hash is the hash value of the previous block of the blockchain.
b) *Transaction Details*: This field contains the details about the various transaction that is to take place[5].
c) *Nonce:* A nonce is a random value that is used to variate the hash value[5].
d) *Hash:* The hash obtained is a hex value that has both number and letters. Any change to the nonce transaction details or the previous hash will completely change the outcome of the hashing function[5].

2) *Mining:* The person who finds the nonce that satisfies the hash requirement for the block is awarded the 12.5 bitcoins. The last transaction in every block assigns 12.5 BTC to the miner as a reward. This is the only ways to generate new bitcoins.
3) *Hash Encryption:* Blockchain uses cryptography to ensure the blocks are kept secure from unauthorized access and alteration. Blockchain uses SHA256 for encryption to validate users, blockchainalso make use of the digital signature. Each user has their own public and private key. The public key is used to uniquely identify the user. The private key gives the user access to everything in the account.

V. KEY ATTRIBUTES OF BLOCKCHAIN TECHNOLOGY

A. Centralized

Centralized architecture there is a central coordination system and every node connecting to the central coordinator system and whatever information they want to share the information will be shared by this central coordination system. If the central coordinator platform fails then all of this individual node will get disconnected. The centralized system will move towards a decentralized system so, in this decentralized system have few coordinators rather than a single coordinator and all these coordinator cooperative with each other and individual nodes connected to this coordinator. So in this particular architecture, if the node fails or multiple nodes fail then the coordinator can connect to other individual nodes can connect to other coordinator and can share the information using that coordinator[9].

B. Decentralized

Decentralized network works in a different location. It has the ability to provide both efficiency and innovation. Efficiency save cost and time and it should provide a better result[9].

C. Distributed

This network is not as a centralized architecture. all the nodes participate in the computation of the information sharing process. they coordinate with each other and collectively share the information among them. Centralized platform good but not scalable they are not robust to failure[9].

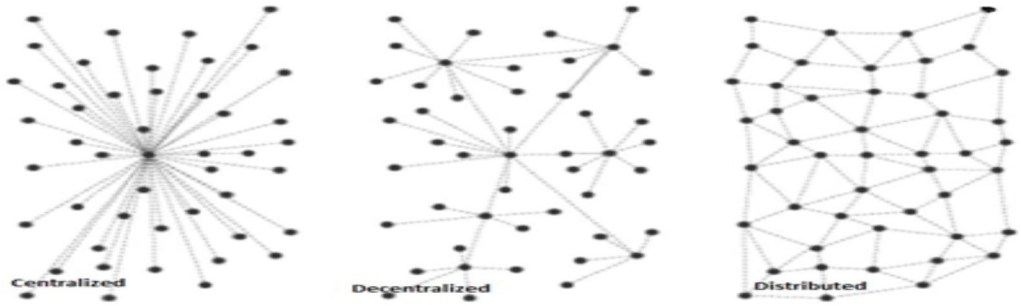

Fig 2: Centralized, Decentralized, and Distributed Network

VI. PUBLIC AND PRIVATE CONSORTIUM BLOCKCHAIN

Blockchain is of three types

A. Public Blockchain

Ledger is visible to all the users on the internet and any user can verify and add a block of a transaction to the blockchain. Participation in a network (building a consensus and conducting mining) is open to anyone. Methods of building a consensus are important in order to eliminate malicious participants.[4]

1) Example: Bitcoin and Ethereum.

B. Private Blockchain

Ledger is visible to all the users on the internet but only specific users in the organization can verify and add a transaction. A blockchain is used while building a consensus only among members who can be trusted with each other to some extent, such as members of a specific company group[4]. Building a consensus is easier as participants are all identified

1) Example: Blockstack.

C. Consortium Blockchain

Consensus process is controlled to be only specific nodes. However, the ledger is visible to all the participants in the consortium Blockchain. A blockchain is used only within a specific organization[4]. Building a consensus is quite easy as the mechanism is open only to the relevant organization

1) Example: Ripple

Property	Public Blockchain	Consortium Block Chain	Private Block Chain
Consensus Determination	All miners	A selected set of Nodes	One Organization
Read Permission	Public	Could Be public	Could Be Public
Immutability	Nearly Impossible to tamper	Could be Tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus Process	Permissionless	Permission	Permission

Table 1 : Comparison of Public, Private and Consortium Blockchain

VII. KEY CHARACTERISTICS OF BLOCKCHAIN

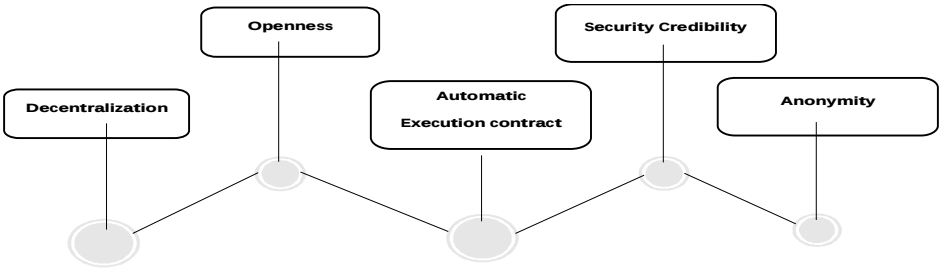

Fig ; 3 - characteristics of blockchain

Key characteristics of blockchain

Blockchain has the following key characteristics**.**

A. Decentralization

Each transaction Should be validated through the central trusted agency a transaction in the blockchain network communicated between two peers (P2P) network without the authentication by the central agency. [7].

1) *Persistency:* Each transaction confirmed and recorded in block distributed in the network and spreading across the network. Each block validated by other node and transaction will be checked.
2) *Anonymity***:** Each user can interact with the blockchain network with a generated address. User generate many addresses to avoid identity. any central trusted party doesn't keep users private information[7]. This technique preserves a certain amount of privacy on the transactions included in the blockchain. due to constraint blockchain cannot guarantee perfect privacy preservation**.**
3) *Audit Ability:* Each transactions validated and recorded with a timestamp, users will verify and trace the previous records through accessing any node in the distributed network[7]. In Bitcoin blockchain, each transaction traced to previous transactions. It improves the traceability and the transparency of the data stored in the blockchain.

VIII. APPLICATIONS OF BLOCKCHAIN

A. Finance

Financial services and Enterprise transformation:- blockchain systems such as Bitcoin has a tremendous impact on traditional financial and business services. Blockchain technology applied to many areas including clearing and settlement of financial assets In financial and business services, blockchain helps traditional organizations to complete the enterprise transformation. As an example of postal operators communicate between merchants and customers. blockchain and cryptocurrency technology can help POs to extend their simple roles with the provision of new financial and un-financial services.[3]blockchain technology offers business opportunities for POs in identity services, device management, and supply chain management.

B. Internet of Things (IoT)

1) *Internet of things (IoT):* Blockchains can also be used in the IoT field. The expected utilization method is one where sensors, etc. predetermined processing tasks work independently without involving a central server. Such services as ADEPT by IBM the transaction of a smart property based on blockchain and smart contract.Distributed autonomous corporations (DAC) is a decentralized. Transaction entity. DACs is basically obtain for coins and exchange sensor data without involving any third party.

C. Public and social services

Blockchain used in public and social services.

IX. BLOCKCHAIN CHALLENGES AND OPPORTUNITIES

A. Land registration and Energy Saving

Land information such as the physical status and related rights could be registered and publicized on blockchain technology. if, any changes made on the land, such as the transfer of land or the establishment of a mortgage should be recorded and managed on blockchains.[3] blockchains can be used in green energy. A solar coin is a kind of digital currency., solar coins granted by the solar coin foundation as long as generate solar energy.

B. Reputation system and Academics

The reputation of a person evaluated on his or her previous transactions and interactions with the community. There are number of cases of personal reputation records falsification. For example, in e-commerce, many service-providers huge number of fake customers to achieve a high reputation. blockchain-based distributed system used for educational record and reputation. each institution and an intellectual worker is given an initial award of educational reputation currency.transactions are stored on the blockchain, all the reputation change detected easily.

C. Security and privacy

Blockchain technologies used to improve the reliability of security infrastructure Blockchain help to improve the security of distributed networks. anti-malware environment named BitAV, in which users can distribute the virus patterns on the blockchain. , It is shown in Noyes that BitAV can improve the scanning speed and enhance the fault reliability (i.e., less susceptible to targeted denial-of-service attacks example, conventional public key infrastructures (PKIs) are often susceptible to single point of failure due to the hardware and software flaws or malicious attacks[3].

X. CONCLUSION AND FEATURE SCOPE

The blockchain is a decentralized infrastructure and peer-to-peer nature. Blockchain has some key characteristics: decentralization, persistency, anonymity, and auditability. In this paper, we present a comprehensive survey on the blockchain. We first give an overview of the blockchain technologies including blockchain block and taxonomy of the blockchain. We discuss the typical consensus algorithms used in the blockchain. Blockchain technology is a new tool with potential applications for organizations. secure transactions without the need for a central authority.

In feature scope Blockchain technologies will be work on the various sector such as Greek economic environment, Currency, Intellectual property rights, Smart Property, banking, public sector, media industry, energy trading, health care.

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, a nd Future Trends" 2017 IEEE 6th International Congress on Big Data.
[2] In-Chang Lin, Tzu-Chun Liao, “A Survey of Blockchain Security Issues and challenges” International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017.
[3] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, "Blockchain challenges and opportunities: a survey”Int. J. Web and Grid Services, Vol. 14, No. 4, 2018
[4] Ibrar Ahmed1, Shilpi2, Mohammad Amjad, “ Blockchain Technology A Literature Survey” International Research Journal of Engineering and Technology (JET) Volume: 05 Issue: 10 | Oct 2018.
[5] Gareth W. Peters , Efstathios Panayi, “Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective” August 15, 2015
[6] A Survey on Blockchain Technology- Taxonomy, Consensus Algorithms, and Applications, International Journal of Computer Sciences and Engineering, Vol.-6, Issue-5, May 2018.
[7] Jiangsu and Nguyen Khoi Tran, “Application of Blockchain Technology in Sustainable Energy Systems: An Overview, 2 August 2018; Accepted: 26 August 2018; Published: 28 August 2018.
[8] Alex Kibet, Prof. Simon Maina Karume, “A Synopsis of Blockchain Technology", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 11, November 2018.
[9] Sayani Chandra, “A STUDY ON BLOCKCHAIN SECURITY ISSUES AND CHALLENGES”, 2018 IJNRD | Volume 3, Issue 5 May 2018 | ISSN: 2456-4184.
[10] Zibin Zheng, Shaoan Xie Hong-Ning, Dai Huaimin Wang, Xiangping Chen, "Blockchain Challenges and Opportunities: A Survey” Fall October 23, 2018.
[11] Sunny King, Scott Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake”, August 19th, 2012.
[12] Urvi Dilipkumar Rajguru, “ A review on challenges and opportunities in Blockchain Technology, Rajguru Urvi Dilipkumar; International Journal of Advanced Research and Development.
[13] 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.
[14] N. T. Courtois and L. Barack, ―On subversive miner strategies and block withholding attack in bitcoin digital currency," CoRR, vol.abs/1402.1718, 2014.
[15] B. W. Akins, J. L. Chapman, and J. M. Gordon, “A whole new world: Income tax considerations of the bitcoin economy,” 2013. [Online]. Available: https://ssrn.com/abstract=2394738