A Brief Analysis of Blockchain Technology

Arushi Gupta
Dr. Akhilesh Das Gupta Institute of Technology & Management
New Delhi ,India
arushigupta568@gmail.com

Gaurav Kumar
Dr. Akhilesh Das Gupta Institute of Technology & Management
New Delhi
laxaman.pal@gmail.com

Nishtha Kapoor
Dr. Akhilesh Das Gupta Institute of Technology & Management
New Delhi
nishthakapoor2017@gmail.com

Saijal Gupta
Dr. Akhilesh Das Gupta Institute of Technology & Management
New Delhi
saijalgupta92@gmail.com

***Abstract*—Technology has affected every part of our lives and that also includes our financial systems. Terms like cryptocurrencies and Bitcoin are more popular than ever and Blockchain Technology is one of it's basic foundations. Block chain, in simple terms, is a decentralized and distributed ledger system that ensures the integrity and immutability of document by recording the provenance of a digital asset. In this paper we discuss both basic and advanced concepts regarding the working and functioning of the Blockchain technology and the challenges it faces in the current scenario. We also discuss the future prospects of blockchain technology in financial services, Internet of Things, Trade Processing, personal identification and so on.**

Keywords—Decentralized, ledger system, block chain, immutable, scalability.

I. Introduction

Since and after it's tremendous reach of $19,783.06, Bitcoin [1] has been the talk of the wall street even after more than a decade. During this whole journey, it has seen it's highs and lows and it still is one of the most widespread and popular cryptocurrency ever created . Now, if something is this popular, there has got to be something special about the mechanism it's working upon. The technology Bitcoin works upon, Blockchain technology, introduced in the year 2009 , is simply a decentralized and distributed ledger system that records the provenance (place of origin) of a digital asset.

It makes the history of any digital asset unalterable and transparent through the use of concepts like decentralization and cryptographic hashing [2]. In contrast to a centralized system, a decentralized system provides every node present on the network with an equal status and responsibilities.

The goal of a blockchain is to let people share assets in a secure and tamper proof way. Since it is a decentralized system, a single party won't have authority over the whole chain. Every individual device over the network called nodes has their own copy of blockchain and can update, verify and validate the record independently. This brings transparency to the whole network. As each transaction occurs it is put into a block. Each block is connected to the one before and after itself. Groups of transactions are blocked together and fingerprint , i.e., hash of each block is added to the next thus creating an irreversible chain. It makes it impossible to alter the blockchain thus making the system immutable and enhance trust and integrity of the system. Blockchain also eradicates the use of an intermediary in any kind of operation, thus it has been proven to be a vital technology in the field of financial transactions and literally any other field that requires a ledger system.

The rest of this paper is organized as follows. Section II shows the characteristics of blockchain technology. Section III summarizes the architecture of blockchain. Section IV gives the classification of blockchain technology. Section V explains the working of a blockchain. Section VI discusses the various consensus models and algorithms in the industry. Section VII introduces the challenges faced by blockchain technology. Section VIII summarizes the applications to blockchain in the various sectors and countries. Section IX discusses the future aspects and trends possible in the blockchain technology and Section X concludes the paper.

II. Characteristics of Blockchain

The three main pillars of Blockchain Technology [3] which have helped it gain widespread acclaim are as follows:

- Decentralization
- Transparency
- Immutability

A. Decentralization:

In a centralized system all the intermediation, ie, one or few trusted parties carry out most of the intermediation tasks for vast network of users, thus limiting all the power in the hands

of central party only. In contrast, in a decentralized system all the nodes in the network carry out the tasks. There is no need for a third party to maintain data consistency.

B. Transparency:

Blockchain technology is nothing but sequence of blocks and each block is linked to the previous and next block. . It records all sequences of transaction from beginning to end thus recording the provenance of each transaction. A transparent ledger of changes preserves integrity of the document, which creates trust in the asset.

C. Immutability:

Immutability [2], in the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with.

Blockchain uses cryptographic hash function to achieve immutability in hashing algorithm , the system takes a piece of data of any length and creates a unique fingerprint of a small fixed length.hashing function almost uniquely compresses a data input. Bitcoin uses SHA-256(Secure Hashing Algorithm 256). A good cryptographic hash function is concealing, deterministic, and has a high "Avalanche effect".thus changing a tiny bit of input can alter the hash dramatically.

III. Architecture of Blockchain

A blockchain can be defined as a family of decentralized record keeping systems in which each transaction created is distributed over the network as shown in fig. 1. Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Blockchain technology is based on three main concepts which are explained below:

A. BLOCKS :

To conserve computing power, most blockchains use the concept of " Batch processing". Nodes group pending transaction into blocks [3]. A block consists of the data ,ie, transaction. In particular, a block is divided into two parts- Block header and Block body. Block body comprise of the transaction data whereas block header contains a randomly generated 32 bit whole numbers called nonce and a 256 bit hash value that points to the previous block (parent block) as shown in Fig. 1. The first block in the chain which has no parent block is called the genesis block.

Block header also includes:

(i)Block version: indicates which set of block validation rules to follow.

(ii)Merkle tree root hash: Transactions within a block are not necessarily stored on first come first serve basis. It is organized in a merkle tree structure. It contains the hash value of all the transactions in the block.

(iii) Timestamp: current time as seconds in universal time since January 1, 1970.

(iv) nBits: target threshold of a valid block hash.

After the digital signatures of blocks are verified and all the transactions are validated, the block is then published and appended to the chain.

B. IDENTITIES:

An identity consists of a pair of public-private keys[9]. Most implementations of the blockchain, particularly public blockchain like bitcoin and ethereum use public key cryptography to maintain a certain level of anonymity.Both keys can be used to encrypt data that you generate. Data encrypted with public key can only be decrypted with private key and vice versa. Private key are used as a digital signature whereas public key is considered as the address.The typical digital signature is involved with two phases: signing phase and verification phase.Suppose, if someone wants to send data over the network then in signing phase data is encrypted with their private key and the signed data can only be decrypted by public key. Now in verification phase, the receiving node verify the sending node's public key. You can create as many identities you want and can store them in a digital wallet. But this also creates a challenge of malicious nodes, especially in public blockchains.

C. NODES:

One of the most important aspects of Blockchain technology is decentralization. Nodes can be considered as an electronic device spread across the network that maintains copies of blockchain. Nodes are responsible for generating and verifying the transaction. After validation of block is done they broadcast the block over the network. The nodes that create the blocks are called miners and the process is called mining.

IV. Classification

Blockchain technology can be classified in a number of ways, ie, on the basis of data it can take or the level of accessibility and data transparency: Here we discuss the latter criteria in detail.

Blockchain categorized on the basis of level of accessibility and data transparency takes into account the facts that to whom the data is visible and to what degree it is. On this criteria, blockchain can be broadly classified into three categories:

1. Public Blockchain:

In this classification, participation of nodes is not restricted and anyone can join the network. In this, a node is responsible for providing intermediation services like transaction verification to the client users. Since anyone can participate

and all the participants are pseudonymous, it leads to a large number of nodes and makes the system prone to inconsistent data. Hence a complex consensus mechanism is required to maintain a unified chain records kept by all the nodes. It also increases the time required in transaction processing. In a public blockchain, nodes are called miners and all of them are given equal opportunity to read or write blocks.Most cryptocurrencies rely on public blockchain for their mechanism. Eg, Bitcoin, Litecoin, etc.

2. Private Blockchain:

In private blockchains, access to blockchain is restricted to few trusted people only. This is mostly used for enterprises and allows them to implement distributed ledger systems without making data public. In private blockchains all the validation decisions are made by single authority only. To determine the trustworthy validator, vetting is performed. No other complex consensus mechanisms are required since the final data is shared or broadcast by one node only.

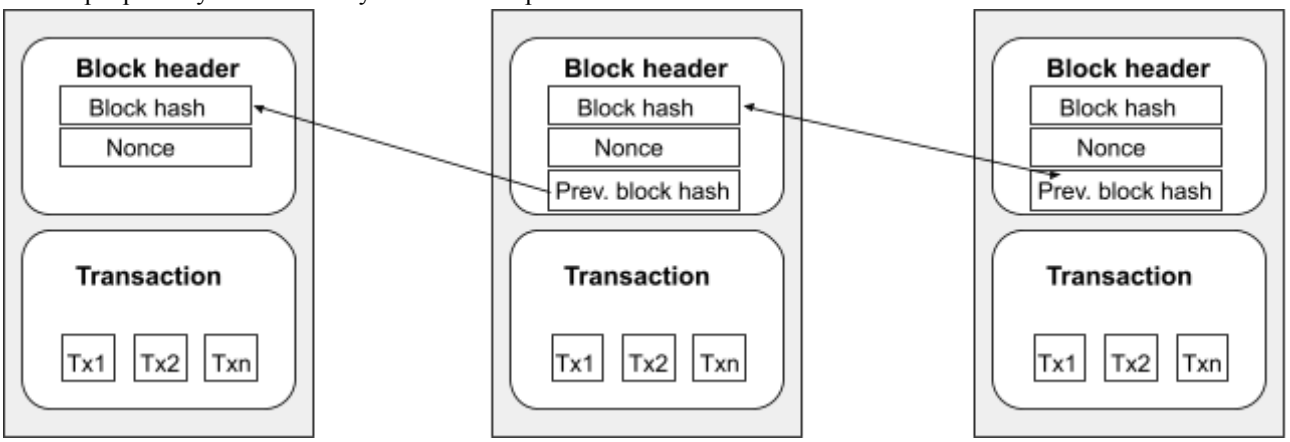

Fig. 1: Illustration of Blockchain Architecture, Blocks in a blockchain with 2 vital seperate parts: Block Header and Block Body (with the transaction information)

3. Permissioned Blockchain:

This classification can be considered to be a combination of public as well as private blockchain. In this, like a public blockchain, data is visible to everyone but, like a private blockchain, access is controlled by just one authority. The consensus process is pretty simple because just like a private blockchain, permission is required for a node to participate in one such blockchain. Some enterprise focussed cryptocurrencies use permissioned blockchains like Ripple, Corda, Hyperledger fabric [6], etc.

V. Working of Blockchain

It is the unique and prominent working structure of the blockchain technology that contributes to its massive success and strong character. The basic building parts of a blockchain are blocks.

A block is basically an electronic entity which contains bits of data, nature of which depends upon the application blockchain is being used in. But there are some fundamental pieces of data in blockchain, that characterize a block in a network.

The first data in a block is the data associated with the properties, the blockchain is being used for. For example, in the application of blockchain in the financial sector, this data is the details of the transaction the block represents. This includes the initiator and receiver of the transaction, date/ timestamp of the transaction as well as some other details.

The other key aspect data that exists in a blockchain is the hash code of the previous block in the chain. A hashcode is a code, generated using a hash function. A hash function is an algorithmic/ mathematical function, that takes in a variable length input and gives out a constant length output. This hash function is the building block of the security concept of blockchain technology. Standard hash functions provide immutability in the fact that even a slight change in the input string, changing the case of a single letter for instance, drastically changes the output string of the function. Thus, when a block consists of the hash code of the block preceding this one in the chain, it results in the formation of a secure chain. For example, if a person tries to tamper with a block's data, he/ she will have to change the hash code of the previous block to, which in turn requires a change in the hash code of the previous block, and so on. This is why blockchain technology is one of the most trusted technology across various sectors.

When one such blockchain is developed for a single purpose, it is usually distributed to multiple people across the internet. Each recipient of this blockchain is called a node, and

every node contains their own copy of the same blockchain. This distributed aspect of the blockchain provides it the characteristics of decentralization and transparency.

When the blockchain is shared to multiple users across the internet, the concept of one single hosting spot of data, centralization is eradicated, and rather, everyone contains their own copy of the blockchain. Thus there is no chance of a single point of failure, or that of the client-server mechanism. Thus, there is no single authority providing details to the participants across the networks, or accepting input from them. Every individual or node present on the network can view or add blocks to the network.

Any blockchain, in general, consists of mainly 3 components.

1. User Applications - This component includes the wallet or any service in that matter, which generates or initiates a transaction.
2. Blockchain Network - A Peer-to-Peer (P2P) Network, is the part of blockchain where all the transaction processing is done using any of the suitable consensus. Blockchain Network, Data and Transaction Processing, as discussed below in detail, are what forms the basis of the blockchain network.
3. Database - This stores the data regarding every aspect of the transaction in form of 256 binary bits or 64 hexadecimal bits.

A. Blockchain Network and Data Processing:

Data transmission is simple in centralized blockchains.If you're using a relatively centralized blockchain with a limited number of nodes like Ripple, this process is also easy. You just broadcast the data to all the nodes simultaneously and they'll receive and process the data in a relatively short time frame. By contrast in a distributed system data usually flows via a peer to peer network.

In a distributed system, unlike a centralized system there are thousands of nodes so instead of sending it to the entire network, miners broadcast the transaction data to a few miners that are closest to them in terms of network latency. The miners will propagate the data on the network using what's called a gossip protocol. It is a more efficient way for transaction propagation.

B. Transaction Processing:

Many blocks use a scripting language to process incoming data. Any client application can generate a transaction script,i.e., a programming code for the blockchain node to execute.It's a simple script with some inputs and outputs. The input has a hash pointer containing the hash of a previous transaction whereas output consists of the hash of the next as shown in the Fig.2. Client publishes the transaction throughout the network of nodes. Nodes then execute the script to verify the validity of the transaction.

VI. Consensus Model

In blockchain,Consensus protocols exist to address the Byzantine generals problem. Once a system becomes decentralized,a major downside of this setup is that different nodes are likely to receive different information. Since transactions are not propagated to all nodes at the same time due to network latency, it is possible that at any point of time, different nodes will have different data records.

Consensus is an algorithmic [12] process to ensure that there exists a single copy of records shared by all nodes but it doesn't guarantee that data copy is more secure than its centralized counterpart..The goal is to reduce these different data copies into one unified copy shared by all the nodes. This can easily be achieved by simply imitating a centralized system.

A. CENTRALIZED CONSENSUS MODEL

The idea behind this consensus model is that we designate a central node and whatever data the central node has is going to be the official copy. In fixed intervals, central node collects all the transactions it has received into blocks and then validates them. The final copy is then broadcast to all the nodes. Once it's posted, the rest of the nodes simply assume a

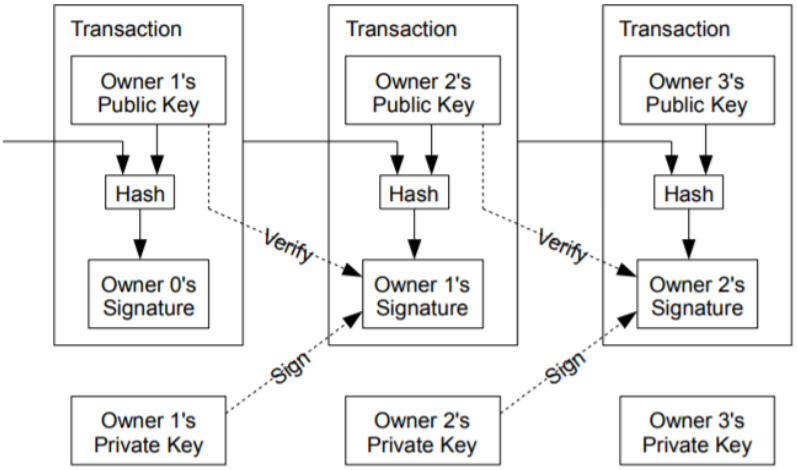

Fig. 2: Illustration of Transaction Processing in a simple Blockchain

much more passive role by verifying the crypto signatures for the transactions in the block and accept them. A simple variation of this approach is the majority vote. In this process, the nodes simply post their transactions and transactions that have been heard by a majority of the nodes are automatically accepted onto the blockchain. This central node setting is unbeatable in terms of efficiency and since only central node takes the validation decision, it is fast as well. There's no need for any mining or complex computation . This kind of consensus model is often used for private and enterprise focussed blockchain for eg, Ripple.

But this kind of defeats the purpose of blockchain as a distributed system as in this case all power is in the hands of central node only. Only the Central node can make decisions about validation of a block and other nodes act more passive. Also vetting is required to decide a trustworthy validator. This vetting process has to take place off the blockchain using traditional legal means which is quite expensive and consequently, the central validator process is not applicable to public blockchains where the nodes are more or less equal and all of them are anonymous.

B. RANDOM CONSENSUS MODEL

As we see in the central consensus model, all the power of validation of a block lies in the hands of central validator at every interval and this creates the need of vetting. In random consensus model we consider what if vetting is impossible, like in public blockchains where all the nodes are equally anonymous to each other. So in this case, we just randomly select a node and let it broadcasts its pending block. If all the transactions in the broadcast are valid then other nodes will accept the block and add to the chain. But if it's not valid then another node is randomly selected and the block is rebuilt. So at the end of every interval, we're going to throw a dart at the board of nodes and randomly select one node to post this block. And here again the rest of the nodes assume a more passive role and simply verify the validity of transactions in the block, like having the right crypto signatures etc. But this mechanism only ensures that every node in the network would have the same chain of data blocks. It doesn't address the issue of malicious nodes. If a fake node gets picked in a period then it can compromise the system. Since in public blockchains all nodes are pseudonymous and one can create as many fake identities, it is easy to carry out double spend attacks. Hence to create a more robust consensus mechanism, in the process of randomly selecting the node, we can weigh it by something that is hard to fake,i.e., computing power or total wealth.

VII. CONSENSUS ALGORITHMS

There are various consensus algorithms developed out there and all have their own pros and cons. Here, we have discussed a few of them in detail.

A. PROOF OF WORK

PoW (Proof-of-work) or Mining is a consensus mechanism used in the Bitcoin network [1]. In this strategy, nodes are weighed based on their computing power. Ergo , this makes a successful consensus attack economically infeasible and makes the system less vulnerable to Sybil attack.The proof-of-work consensus is by far the most widely used consensus protocol.
The most widely used proof-of-work consensus is based on SHA-256 and was introduced as a part of Bitcoin. Others include Scrypt, SHA-3, scrypt-jane, scrypt-n, etc.

The main idea behind this algorithm is that nodes have to compete to solve complex mathematical problems in order to mine the next block. This mathematical puzzle requires a lot of computational power. The solution to the problem is called

hash value of the block header. The nodes that calculate the hash values are called miners. Miners append a random nonce value to the block to find a fixed hash of leading 0's. The nonce is 32 bits and hash is 256 bits. This gives roughly four billion possible nonce-hash combinations that must be mined before the right one is found. Brute forcing is only an option in this case. When a miner finally calculates the required hash value, it broadcasts the block to the whole network along with nonce and other nodes verify the solution and block validity. After validation, the block is appended to the blockchain.

But this approach has its own limitations.If a controlling entity owns 51% or more than 51% of nodes in the network, the entity can corrupt the blockchain by gaining the majority of the network.Also Since brute forcing is the only option, it is a time consuming process as well.Miners consume high amounts of computing power in order to find the solution to the hard mathematical puzzle. It leads to a waste of precious resources(money, energy, space, hardware).

B. PROOF OF STAKE

Proof of stake is considered to be the most common alternative to POW algorithm. Many blockchains adopt PoW [2] at the beginning and transform to PoS gradually.For instance, ethereum has shifted from POW(Ethash) to POS(Casper).

Proof of stake(POS) or virtual mining weighs the node on basis of the amount of cryptocurrency you invest. It is the more direct form of mining. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, miners stake their identities directly with cryptocurrencies. Consequently, miners become direct stakeholders of cryptocurrency. This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age based selection, randomization process) to make the selection fair to everyone on the network. In PoS algorithm Nodes make transactions. The PoS algorithm puts all these transactions in a pool. Each node places a cryptocurrency stake to bet on its block. Probability of a node being selected to post the block is directly proportional to the miners bet. The selected node then broadcasts the block across the network and other nodes verify the blocks validity. Once the validation is done the block is added to the chain. The miner that forges the block is rewarded with a transaction fee. This approach does not require miners to solve any complex mathematical problems, thus consuming less time. This also increases the efficiency as well as significantly lessens the energy and resource requirements of the system.

The major drawback of this approach is that If a group of validator candidates combine and own a significant share of total cryptocurrency, they will have more chances of becoming validators. Increased chances leads to increased selections, which lead to more and more forging reward earning, which lead to owning a huge currency share. Therefore in the long run, the system can become significantly centralized thereby defeating the purpose of decentralization in blockchain.

C. PRACTICAL BYZANTINE FAULT TOLERANCE (pBFT)

pBFT consensus algorithm is designed to work in an asynchronous system. The Byzantine Fault Tolerance (BFT) [10] defines the dependability of distributed computing [13] [14] systems where components may fail and result in imperfect information. Achieving BFT is one of the most difficult challenges addressed by blockchain technology.The objective of a BFT mechanism is to safeguard against the system failures by employing collective decision making(both – correct and faulty nodes) which aims to reduce the influence of the faulty nodes.

pBFT [15] tries to provide a practical Byzantine state machine replication that can work even when malicious nodes are operating in the system. Nodes in a pBFT enabled distributed system are sequentially ordered with one node being the primary(or the leader node) and others referred to as secondary(or the backup nodes). The goal is that all honest nodes help in reaching a consensus regarding the state of the system using the majority rule. If needed, a majority of the honest nodes can vote on the legitimacy of the current leading node and replace it with the next leading node in line.

A practical Byzantine Fault Tolerant system can function on the condition that the maximum number of malicious nodes must not be greater than or equal to one-third of all the nodes in the system.

pBFT consensus rounds are broken into 4 phases:The client sends a request to the primary node which broadcasts the request to all the secondary nodes.The nodes perform the service requested and then send back a reply to the client. The request is served successfully when the client receives 'm+1' replies from different nodes in the network with the same result, where m is the maximum number of faulty nodes allowed.

pBFT is an energy efficient approach to achieve consensus as it does not require any complex calculations. Every node takes part in responding to the request by client and hence every node can be incentivized leading to low variance in rewarding the nodes that help in decision making.

The pBFT consensus model works efficiently only when the number of nodes in the distributed network is small due to the high communication overhead that increases exponentially with every extra node in the network.The pBFT mechanisms are susceptible to Sybil attacks, where one entity(party) controls many identities.

D. DELEGATED PROOF OF STAKE

Delegated Proof of Stake (DPoS) is a consensus algorithm developed to secure a blockchain by ensuring representation of transactions within it. DPoS is designed as implementation of technology based democracy to protect the system from malicious nodes. Stakeholders elect their delegates to generate

and validate blocks. With significantly fewer nodes to validate the block, the block could be confirmed quickly, leading to the quick confirmation of transactions.
Meanwhile, the parameters of the network such as block size and block intervals could be tuned by delegates.
Additionally,users need not to worry about the dishonest delegates as they could be voted out easily. DPoS is largely considered to be the most decentralized approach to consensus mechanism. It also is an energy efficient and time saving method that has strong protection from double spend attacks. Cryptocurrencies that use DPoS include Lisk, Steem, EOS and BitShares.

VIII. Challenges of Blockchain Technology

In Spite of having such a remarkable performance over the years, blockchain technology still faces some major challenges in the industry. A few of those challenges are implementation dependent and some are for the general working of the technology. Both of these types of challenges are collectively discussed below:

A. Scalability:

Blockchain technology uses the concepts of decentralization and transparency as it's core features. Thus, it is obvious that it supports a large network of nodes. This large number of simultaneous users, in turn, increase the cost and reduce the throughput of the blockchain [5]. They make the blockchain bulky and as a result decreases the number of transactions.

These scalability issues can be addressed via majorly two modes:

1. Lighting Network - It is a two layer protocol that offers an off chain settlement among the participants which aims at processing those transactions first which have low cost and faster processing time.
2. Sharding - It is a method in which subsets of nodes are grouped into smaller networks, often referred to as shards. Shards are responsible for a transaction specific to a particular shard.

B. Security:

Blockchain as a whole is a very secure and immutable record system [11]. Also, on the other hand, if a few users are involved in false or malpractices, this could put the whole blockchain in jeopardy. Thus, this does not guarantee transactional safety as the transaction details and balances publicly visible.

C. Selfish Intents:

Some nodes on the network, with selfish intentions, do not show their mined blocks to the network. This private branch is only made public when certain requirements are fulfilled. This leads to the honest miners waste their time on mining the already mined blocks, with the selfish miners [8] having access to majority or all parts of the blockchain.

This issue can be solved by an approach where all the users are allowed to follow a branch. Using random beacons and time stamps, honest miners can select fresh blocks. This poses another issue, the fact that timestamps can be forged, which can be overcome by issuing a specific time for a block to be generated and accepted in the network.

IX. Applications of Blockchain Technology

Blockchain has received immense popularity and support over the years it has been around and thus there have been numerous applications concerning various sectors in the industry. Following are discussed some of the applications of blockchain technology in various parts of the world.

1. Food Sector:

The food sector has seen some tremendous approaches with blockchain as the market suffers from its own problems of traceability and sustainability. The fact that blockchains are immutable and distributed ledger systems, gives the food producing and quality assurance agencies an easy hold on checking the source of bad food products and the consumers to track the source and path of their commodity, in order to ensure its sustainability.
Small level farmers face the problem of getting capital for their produce and the data sharing and distributed properties of blockchain help them in obtaining funds from trusted investors.

2. Election Commission:

India, along with many other countries, has invested in the blockchain technology to smoothen out and improve the election procedures. The fact that every block ever created in a blockchain is unique, with its own unique hash code, and is thus immutable, that is, it cannot be tampered with, provides the level of trust and security that an activity as important and prime as election requires. Since everyone on the network of a block chain can view all the contents of each and every block, this provides the transparency factor that is a key factor in the election procedure.

3. Crypto currency:

Bitcoin has been recognized as one of the world's most popular crypto currency and it has got blockchain to owe to it's massive success. The three pillars of blockchain technology: Immutability, Decentralization and Transparency gives Bitcoin and other cryptocurrencies all the desired features that are responsible for it's huge outreach.

4. Health sector:

Storing patients records unhindered by outside influence yet available for all concerned people to easily keep track of everything makes blockchain a boon for the health industry.

5. Smart contracts and Notary:

The fact that once a block has been registered in any given blockchain, it or it's data cannot be tampered with just makes blockchain a suitable technology behind smart contracts [4] [7] and e-notary.

X. Future Aspects of Blockchain Technology

Blockchain, as discussed in this paper, has a lot laid out for its future days, and we are sure to see it getting a lot of advances in the coming days and years. Following are discussed some of the future trends that can be included with the blockchain technology to give it the further push it requires.

A. Big Data Analytics:

Blockchain can be combined with Big Data as its model is that of the decentralized and distributed along with being secure. Thus, it can ensure that the data stored in it is original. A study of the transactions taking place on the blockchain can provide the data analytics with the details and information required.

B. Centralization.

One of the most major technology patterns is the centralization concept of the data, giving authority over the data to a single entity/server. Blockchain technology, in its decentralization approach, stands tall to give this conventional concept of the internet a hard challenge. Despite this feature miners are centralised in the mining pool. According to a recent report, the top 5 mining pools together own larger than 51% of the hash value in a bitcoin network. But blockchain is not intended to serve only a part of the organisation. Hence, this is a problem blockchain has to overcome in order to go against the centralization concept.

XI. Conclusion

Blockchain is a revolutionary technology, in it's novice state. It has certain problems but not without a lot of potential. It has the capability to transform the industry with its leading aspects of audability, decentralization, persistence and anonymity. This paper presents a basic overview of blockchain which comprises blockchain architecture, algorithms and characteristics of blockchain . Furthermore, its applications and challenges are also included here. Blockchain applications are increasing tremendously and it has a huge potential to come out as technology of its time.

References

[1] Satoshi Nakamoto ,"Bitcoin: A Peer-to-Peer Electronic Cash System"

[2] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang ,"An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends", in press

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

[4] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, 2014.

[5] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, "Blockchain technology: Beyond bitcoin"

[6] "Hyperledger project," 2015. [Online]. Available: https://www.hyperledger.org/

[7] 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.

[8] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.

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

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

[11] Dr. Divyakant Meva "Issues and Challenges with Blockchain: A Survey" in INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING, December 2018, in press

[12] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.

[13] Sujaya Maiyya, Victor Zakhary, Divyakant Agrawal and Amr El Abbadi, "Database and Distributed Computing Fundamentals for Scalable, Fault-tolerant, and Consistent Maintenance of Blockchains" in Proceedings of the VLDB Endowment, Volume 11, Issue 12

[14] M. Castro, B. Liskov, et al. Practical byzantine fault tolerance. In OSDI, volume 99, pages 173–186, 1999..

[15] Xu Hao, Long Yu, Liu Zhiqiang, Liu Zhen and Gu Dawu, "Dynamic Practical Byzantine Fault Tolerance" in Proceedings of

2018 IEEE Conference on Communications and Network Security (CNS),