OUR HERITAGE
ISSN: 0474-9030 Vol-68, Special Issue-27 (Feb. 2020)
5th International Conference On "Innovations in IT and Management"
Organised by: Sinhgad Technical Education Society's
SINHGAD INSTITUTE OF MANAGEMENT AND COMPUTER APPLICATION (SIMCA),
Narhe Technical Campus, Pune, Maharashtra (India) 411041.
Held on 6th & 7th February 2020

Beyond Cryptocurrencies: Influence Of Blockchain in Future

Mrs. Smita S. Chavan
Assit.Professor SIMCA, Narhe Pune
smita.smitha@gmail.com

Abstract

Blockchain, the foundation of Cryptocurrencies, is known to be a disruptive technology in today's technological landscape. Blockchain is a distributed ledger technology, that provides a platform for all the network participants to have access to this ledger and its immutable records of transaction. With its immutable nature, none of the participants can alter or tamper with a transaction after its recorded into the shared ledger. Blockchain based application are not just being talked about, but are being implemented in many different sectors including financial services, IoT, Supply chain, Health care, to name a few. However, as there are is no governing authority to drive the implementations of Blockchain, there are still few challenges like scalability and security to be tackled for its faster and smother adoption across the industry.

This paper provides an overview of Blockchain, its architecture and the applicability across different industries, which is now just not restricted to Bitcoins and Cryptocurrencies.

Keywords: *Blockchain, Bitcoin, cryptocurrencies, Cryptocurrency Hash function*

1. Introduction

Since last few years, Bitcoin and cryptocurrencies have received a good hype across globe. People have seen the capital market of Bitcoin going from nowhere to its peak in late 2017. Bitcoin was the first application of the underlying technology, known as Blockchain, which was proposed in 2008 by the person or people pseudonym as "Satoshi Nakamoto". Blockchain is a growing list of blocks which are using cryptographic mechanism. Each block contains cryptographic hash of previous block, timestamp, transaction data. Though the first work for cryptographically secured chain of blocks was introduced in 1991 by Stuart Haber and W. Scott Stornetta, but the real implementation was done in 2009 for Bitcoin, where the design was done using a Hashcash like method to timestamp the blocks without requiring them to be signed by a trusted party. Blockchain acts as a public ledger, where all transactions are maintained in a list of blocks appended to form a chain of blocks. In order to maintain security and consistency, asymmetric cryptography and distributed consensus algorithms are used. The key characteristics like anonymity, auditability, persistency and decentralization makes Blockchain a very efficient and

secured technology.
Blockchain is also referred as Internet 2.0, as it advocates a decentralized, transparent, and more democratic version of the Internet. In the traditional internet which is guided by end-to-end design principle, there are several central points of trust and failures, which includes the cloud infrastructure service providers, servers for DNS (Domain Name System) and public key infrastructure which provides digital certificates like Certification authorities. End user do not have choice other than to trust these third party vendors who provide these services to the applications to be hosted. In contrast, the Block chain follows trust-to-trust design principle, where end user don't need to trust a centralized authority for anything; rather they can use the applications in a decentralized way.

There is plenty of literature available on blockchain and its challenges specifically in the usage of cryptocurrencies. Our paper will focus on the architecture of Blockchain, its applicability in various industries and the future trends.

2. Blockchain Technology Overview

People are thinking that Blockchain and Bitcoin are identical. The truth is that Bitcoin is one of the many applications.Blockchain Technology which has potential to revolutionize many sectors of the world economy. A blockchain is simply a distributed ledger (i.e. a distributed database allowing to record and share data across multiple data stores, the ledgers) with a linked list of blocks using hash pointers (i.e. pointers to where some information is stored, together with a cryptographic hash of the information), such that additions to the database are done through the procedure where transactions are grouped with other transactions to form a block & the network nodes determine collectively if the block is valid through a validation algorithm called a consensus mechanism. Once a block (each block containing the transactions, a hash of its own, a hash of the previous block, timestamp) is validated, it is added to the database and the blockchain is updated across the network.

2.1 Blockchain taxonomy

When the idea behind blockchain was introduced by Satoshi Nakamoto, he propounded it to be a Public decentralized ledger. With this theory, most of the implementations of blockchain came in existence vizBitcoin, Ethereum, etc. However, as the technology progressed and community started implementing this concept and technology across various industries, different types of blockchain were defined.

2.2 Based on access to blockchain data

Permissionless – Anyone with computing power can join
Public – All who access can modify
Permissioned –Approved users only

Private – Only those who are access they can write / modify
However, later it was observed that people started using Permissionless and Public interchangeably, and the same goes for Permissioned and Private.
In today's world, we will find more number of use cases for permissioned/ non-public blockchains. Buterin explains appropriately why certain real life situations demand nonpublic blockchains. Then further classifies the non-public blockchains into groupblockchains and Fully-Private blockchains. Consortium blockchains may be the option of choice when different institutions/organizations have common goals to achieve, wish to share the cost and are willing to share their data.

2.2.1 Public / Permissionlessblockchains

A public blockchain is a blockchain which is open for all, where anyone can join the network, can perform the transactions and see them included if they are validated by others in the same network by means of Consensus process. As a substitute for centralized trust which is provided by some designated authorities, public blockchains are secured by cryptoeconomics, which is the combination of economic incentives and cryptographic verification using different mechanisms like work proof or proof of stake, following a general principle that the degree to which someone can have an influence in the compromise process .

2.2.2 Non-Public / Permissioned blockchains

As opposed to public blockchains, Permissioned blockchains are built by organizations for their business needs which are specific to their individual organization or a group. Based on its applicability and usage it could further be categorized as Consortium blockchains or Fully-Private blockchains. In consortium blockchains, a limited group of trusted members mandatorily need to sign off a transaction. Where-as the fully private blockchain gives the write permission only to the central organization. This becomes easier in a private than a public one. There is also increased accountability as all the nodes are named. In the example of Public blockchain, namely Bitcoin, it approximately takes around 10 minutes to be confirmed and added to the blockchain. However, this disadvantage is not applicable in a private blockchain scenario, as oppose to bitcoin which adds up a cryptographic puzzle solving time & the network delays add to the transaction commit time. The network delays may however not be completely eliminated and may still exist, given that even private blockchain nodes may exist over the public cloud networks.

3. Blockchain Protocols

Blockchain eliminates the need of a centralized or third party authority to perform the transactions on any parties behalf. For this, some kind of consensus mechanism must exist between the parties being involved in the network to confirm and validate any transaction. The strength and security of the network is determined by how a given blockchain network implements its consensus mechanism. A strong consensus algorithm is required based on the business need to maintain the stability, security and consistency of data across all the participating nodes of the blockchain network.
There are primarily two problems with respect to digital currency, which any of the consensus

mechanisms try to address – Remove the problem of double spend and Eliminate Byzantine Generals problem.

There have been quite amount of research work done on blockchain protocols, there are some key algorithms explained in brief below, whose variations are being used to implement different applications of blockchain.

3.1 Proof of Work

A proof of work is piece of data which is difficult to produce but easy for others to verify and which satisfies certain requirements. In PoW schemes, miners participate in the network by contributing large amount of computing power. Bitcoin uses Hashcash proof of work system for block generation. The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by network to one every 10 minutes. Due to very low probability of successful generation. It makes it unpredictable which worker computer in the network will be able to generate the next block.

3.2 Proof of Stake

Proof of stake protocol block verification does not rely on excessive computations. Instead of splitting blocks across proportionally to relative hash rates of miners (i.e. their mining power), proof-of-stake protocols is split stake blocks proportionally to the current wealth of miners. In PoS-based cryptocurrencies creator of the next block is chosen via various combinations of random selection and wealth or age (i.e., the stake). Proof of stake must have a way of defining next valid block in any blockchain. Selection by account balance would result in (undesirable) centralization and single richest member have a permanent advantage. A number derived from product of the number of coins multiplied by number of days coins have been held.

3.3 Delegated Proof-of-Stake

DPoS has been introduced to the sight after PoS and stands for delegated proof of risk. The reason for this name is because there are participants, or nodes elected by votes to represent others and add new blocks to the chain. Not anyone can to stake and verify blocks. Users can vote for delegates, which they are trusted participants. DPOS meant to democratize PoS environments by creating an agreed upon trusted group of delegates responsible for validating the network.

3.4 Proof of Weight

Proof of Weight is another blockchain protocol gaining interest with projects that have more exact applications. For example, file storage project would most likely use a Proof of Weight. In PoS, stakers' effectiveness is judged by relative number of coins they hold, while in Proof of Weight takes into account number of coins in addition to the number of files (or any other measurable metric) hold for the network. With regards to a file storage project, the metric would be amount of IPFS (file) data users are storing. there is areason to hold coins and contribute meaningfully to the network.

3.5 Practical Byzantine Fault Tolerance

In distributed computing systems where components having chances to fail due to imperfect information Hyperledger utilizes the PBFT as its consensus algorithm. There are designated validator (primary) nodes are each associated with a group of nodes. The primary is responsible for multicasting requests to other replicas in its group. A service operation would be valid if it has received approvals from over 1/3 different replicas. Additionally, if a client does not receive the

replies, it will send the request to all replicas instead of only sending it to the primary in case the primary is faulty. A primary is responsible for ordering the transaction and each replica commits the transaction in the same order.

4. Blockchain components

In order to implement various applications based on Blockchain, there are different components which forms the framework to build and executed these applications. At high level, blockchain technology utilizes well-known computer science mechanisms and cryptographic primitives (cryptographic hash functions, digital signatures, asymmetric-key cryptography) mixed with record keeping concepts.

4.1 Cryptographic Hash Functions

Hashing is method of applying a cryptographic hash function to data, which calculates a relatively unique output, called as digest for input of nearly any size (e.g., a file, text, or image). It allows individuals to independently take input data, hash that data and derive the same result proving there was no change in the data. In many blockchain implementations cryptographic hash function used to secure 256 bits.Since there are an infinite number of possible input values and a finite number of possible output digest values.SHA-256 is said to be collision resistant, since to find a collision in SHA-256, one would have to execute the algorithm, on average, about 2128 times (which is 340 undecillions, or more precisely 340,282,366,920,938,463,463,374,607,431,768,211,456; roughly 3.402 x 1038).

4.2 Asymmetric Key Cryptography

Blockchain technology use asymmetric-key cryptography4 (also referred to as public key cryptography). Asymmetric-key cryptography uses pair of keys public key and private key that are mathematically related to each other. The public key is made public without reducing security of process, but private key must remain secret if data is retain cryptographic protection. Even though there is relationship between two keys, private key cannot efficiently be determined based on knowledge of public key. One can encrypt with private key and then decrypt with public key. Alternately, one can encrypt with public key and then decrypt with a private key. Asymmetric-key cryptography enables a trust relationship between users who do not know or trust one another, by providing a mechanism to verify the integrity and authenticity of transactions while at the same time allowing transactions remain public.

4.3 Addresses and address derivations

Some of blockchain networks can use of an address, which is contains a short, alphanumeric string of characters derived from blockchain network user's public key with the help of cryptographic hash function, along with additional data (e.g., version number, checksums). Most blockchain implementations make use of addresses as "to" and "from" endpoints in transaction. It is necessary to provide method of accessing a smart contract once it has been deployed within blockchain network. For Ethereum, smart contracts are accessible via special address called a contract account. This account address is created when a smart contract is deployed (address for a contract account is deterministically computed from the smart contract creator's address). This contract account allows for contract to be executed whenever it receives a transaction, as well as create additional smart contracts in turn.

4.4 Ledgers

A ledger is a collection of transactions. From the past history, pen and paper ledgers have been used to keep track of the exchange of goods and services. In today's world, ledgers have been stored digitally, often in large databases owned and operated by a centralized trusted third party. Due to possible trust, security, and reliability concerns related in case of centralized databases, there is growing interest in exploring having distributed ownership of the ledger.

4.5 Blocks

Blockchain network users is submit candidate transactions to blockchain network via software. The software sends these transactions to node or nodes within the blockchain network. The chosen nodes may be non-publishing nodes as well as publishing nodes. Transactions are added to blockchain when publishing node publishes a block. A block contains block header and block data. The block header contains metadata for this block. The block data contains list of validated and authentic transactions which have been submitted to blockchain network.

4.6 Chaining Blocks

Blocks are chained together through each block containing hash digest of the previous block's header, thus forming blockchain. If previously published block were changed, it would have a different hash. This in turn would cause all subsequent blocks to also have different hashes since they include hash of previous block. This makes possible to easily detect and reject altered blocks.

5.Blockchain Challenges

Though blockchain appears to have great potential to become future Internet System, there are lots of challenges it will have to overcome, viz:

1) Throughput: The blockchain protocols express throughput in terms of blocks appended to the blockchain per second. This transaction metric depends on applicable consensus algorithm, which specifies how nodes communicate to ensure validity of appended transaction and consistency of each copies of shared ledger. Consensus algorithms like PoW requires huge amount of infrastructure resources to create blocks by the virtue of mining. Due to this, there is a high latency of transaction validation which takes places and counts for around 7 tps (transactions per second), as oppose to other transaction processing networks alike VISA (2000 tps) and Twitter (5000 tps).

2) Scalability: There has always been a key consideration for the scalability of any application or technology being adopted. In blockchain, as the complete data (including metadata, provenance, transaction and audit information) is replicated across all the nodes of the blockchain, each node has to maintain the complete copy of the shared ledger, which contains data across all blocks from the start of blockchain. With the adoptability of blockchain in the industries like healthcare, where the history records keeps on growing day by day, it is very challenging to maintain this size of data as the user grows.

3) Size and bandwidth: The size of Bitcoinblockchain has experienced consistently high level of growth since its inception, reaching approximately 242 GB in size as of Sept 2019. When throughput increases to levels of VISA, Blockchain could grow 214 PB in each year. The Bitcoin

community assumes that size of one block is 1MB, and block is created every ten minutes. Therefore, there is limitation in the number of transactions that can be handled. In order to support the numbers supported by say VISA, the size and bandwidth supported by blockchain must be increased.

4) Security: With the consensus algorithms, Blockchain has the possibility of a 51% attacks. In a 51% attack, a single entity would have complete control of the network's mining hash-rate and would be able to manipulate blockchain. More research should be done to address the security aspect of Blockchains.

6. Blockchain Applications beyond Cryptocurrencies

The blockchainhas capacity to revolutionize security, stability and transparency of networks is need, provided applied appropriately and only if needed, because it is not a panacea for all security applications.

Blockchain in Asset Management - It is all about securely transferring assets within business network. An asset could be a physical one like a server, computer or laptop or an intangible one like software and services. The blockchain isoffers shared ledger capability means full visibility from end to end into business network. The blockchain is employed right from serialization being deployed on the floor and focuses only on five key events.

Blockchain in Finance – A very important process becomes quite expensive and sluggish. Due to the presence of unnecessary middlemen is cross-border payments. It takes several banks before the money can be collected. Services like Western Union can be used which are faster and expensive. The blockchain can speed up and simplify this process and cutting out the unnecessary middlemen. At same time, it makes money remittance more affordable. Until now, the costs of remittance were 5-20%. The blockchain reduces costs to 2-3% of the total amount and provides guaranteed, real time transactions across borders.

Blockchain in the IoT - IoT solutions using blockchain can be built to maintain, a continuously growing list of cryptographically, secured data protected against alteration and modification. For instance, as an IoT connected (e.g. RFID) asset with sensitive location and temperature information moves along various points in a warehouse or in a smart home [18], this information could be updated on a blockchain. This permits all involved parties to share data and status of the package as it moves among different gatherings to guarantee the terms of an agreement are met [19], [20].

Blockchain in Healthcare – A blockchainis based management of patient's health records is proposed in 22. The patient's medical history is stored on a decentralized system and accessible to the treating doctors and medical insurance providers.

Conclusion

Blockchain has become a disruptive technology by changing the way of performing transactions in a secured and decentralized manner. This paper presents a deep dive into blockchain, its characteristics, its challenges and the applicability of it other than mere cryptocurrencies based

applications. There is a huge potential for its adoption by addressing its few key challenges and defining some standards to be followed across industries, so that more and more contribution is made by researchers, so that this technology is rolled out across every industry seemlessly.

References:

https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends
https://www.researchgate.net/publication/332139853_Blockchain_And_The_Future_of_the_InternetA_Comprehensive_Review
https://www.semanticscholar.org/paper/Trust-to-Trust-Design-of-a-New-Internet-Ali/4dd0e4e86f173e0481f40344ce797064dc4f8b74
https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/
https://www.researchgate.net/publication/308877750
https://www.himss.org/blockchain-performance-throughput-and-scalability
https://en.wikipedia.org/wiki/Blockchain
https://en.bitcoinwiki.org/wiki/Bitcoin_history
https://pdfs.semanticscholar.org/3760/7b0b49b31d3ef5eeb6754a0529a1b6f5643c.pdf
https://hal.archives-ouvertes.fr/hal-02280279/document
https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf
https://en.bitcoin.it/wiki/Proof_of_Work
https://en.bitcoin.it/wiki/Proof_of_Stake
https://cryptomaniaks.com/blockchain-protocols-list-explained
https://www.researchgate.net/publication/326102908_Everything_You_Wanted_to_Know_About_the_Blockchain_Its_Promise_Components_Processes_and_Problems