International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

THE BLOCKCHAIN REVOLUTION: Analyzing Distributed Ledger Technology

Lakshay Swani[1]

[1] *Software Engineer, Globallogic Pvt. Ltd, Sector-144, Noida, UP, INDIA*

Abstract - *The Blockchain technology is considered to be a paradigm-shifting event in the history of rise of internet. This paper aims to cover the summary of the advantages and opportunities related to the use of blockchain technology in various aspects of business. Blockchain being a distributed, decentralized and public digital ledger is used to record the transactions across multiple computer so that these records cannot be altered or hampered. It is believed that one day, blockchain technology will facilitate majority of transactions all around the globe. Blockchain is generally considered as synonymous with Bitcoin. Bitcoin is just an implementation of blockchain technology as one of the solutions for many information exchange problems. Bitcoin being the very first coin based on the blockchain technology has achieved great deal of attention, but the impact of blockchain extends way beyond Bitcoin.*

***Key Words*: Blockchain, Distributed Ledger Technology Smart contracts, Consensus, Permissioned Permission less Blockchain**

1. INTRODUCTION

Blockchain is considered to be as impactful as the presently known Internet, thus it is referred to as a "Revolution". Originally built as an underlying technology for the Bitcoin, its application goes way beyond currencies. It indeed has the far reaching applications that can significantly change the way the transactions occur in financial markets and the way we interact with computers, artificial intelligence and technology.

Blockchain technology is the use of decentralised /distributed ledger to record, store and verify any information exchange, also referred to as a transaction. It makes possible for the transacting parties to send, receive & record information by creating a peer-to-peer network of computers. Among the wide range of application, Blockchain also acts as a platform for smart contracts that facilitate, enforce and execute agreements between the parties.

Many issues have been raised related to the privacy, security and risk involved in the use of blockchain technology in various sectors. This article identifies the different aspects of blockchain related to regulatory and technological dimensions. We will first gain insights regarding the basic concepts of the technology. Further, we will move on to analyse & understand the possible applications to the use of the distributed ledger technology. And finally we will conclude by addressing the regulatory developments that tend to impact the use of blockchain technology globally.

1.1 Hashes

Hash is a series of characters that represents a digital footprint of some digital data. Any data of infinite length can be converted to hash value which is of specific length and a particular digital data is always represented by same hash value. It is impossible to guess the value of hash due to the randomness in the character representation.

1.2 Blocks

A block is a group of valid transactions that collects and groups the valid transactions together in a bundle. Blocks to be valid, follow a predefined set of rules such as, they should not exceed a maximum size, should not contain more than a maximum number of transactions and should be referencing to the most recent valid block in the chain.

1.3 Blockchains

A blockchain is referred to as a set of blocks linked together. Each new block references the most recent valid block and gets attached to that block. The new block gets chained to the referenced block and is placed after the most recent one, thus forming a chain of blocks.

1.4 Coinbase

A blockchain records and consists specific types of transactions known as the Base transactions. Each currency transaction is validated on the basis of past transactions. The transaction occurs only if the contents of transaction actually exists. For example, in case of currency transactions, the transaction is validated by checking if the party transacting the currency actually holds that sum of currency. If the party doesn't contains any currency, the other transactions will be stopped. A coinbase transaction is referred to as a unique type of transaction that can created only by a miner. There are no inputs in this type of transaction, and there is one created with each new block that is mined on the network. This is the transaction that rewards the miner for their work.

1.5 Genesis Block

The genesis block is the very first block in the blockchain. This is the only block that has no references to any other previous block and is considered to be the least safe as its validity cannot be checked. The genesis block consists of a

coinbase transaction that allows for room for further transactions. For example, the in most popular blockchain based Bitcoin cryptocurrency, there is a coinbase transaction of 50 bitcoins. These bitcoins were the first ones to be transacted till other miners were rewarded for their work and received coinbase transactions.

1.6 Consensus & Mining

Consensus refers to how the blocks are to be validated. A consensus model defines how hard it is to validate a block, the ease to verify its validity and enforces a linear history.

Miners are the ones who validate the blocks by following the consensus model. Each time a new block comes in to be added to the blockchain, the miners compete with each other to validate the block. The first miner to successfully validate the block is rewarded with a small payment. For example, in Bitcoin blockchain, each miner who successfully validates a block first is provided with the transaction fee and newly issued bitcoins through a coinbase transaction. The number of Bitcoins issued is determined by the block number that is validated. The further the blocks in the blockchain, the lower is the reward.

1.7 Proof of Work

If the validation of a new block is easy, mining could be really rapid. If the mining process is not slowed down, many blocks will be created and miners will be rapidly given loads of rewards as coinbase transactions. To solve this issue, Bitcoin devised two new characteristics. The first is that only one new block will be created in a certain period of time and the other states that the miner will have to provide proof of work (PoW). PoW provides information that a miner has applied some computational power in validating the new block. For this, the signed blocks only are added to the blockchain. For example, a miner will be required to add a block to the blockchain whose hash starts with specific number of leading zeroes otherwise his validation of block will not be acknowledged.

1.8 Forks

When a Blockchain is split into two blockchains, it is referred to as Forking. The splitting of a parent blockchain could be either temporary or permanent.

The permanent splits occur only when the rules of blockchain are altered but the splitting of blockchain is not preferred as the child blockchains are weaker relative to mining power and clients.

A temporary split occurs frequently, usually when multiple miners mines a block and sends it for validation at the exact moment. The blocks will be assigned on top of the most recent valid block. When the next block comes for validation, there will be multiple most recent valid blocks and will be attached to either one of them. When one of the chains becomes larger than the others, the other chains are left behind and are referred to as orphans.

2. Distributed Ledger Technology

Distributed ledger technology refers to a digital system for storing transactions and providing the users with the ability to store and access data and information in a shared database known as a ledger which is distributed, thus providing it the capabilities to be operating without any central validation system or a third party administration. Unlike traditional databases, such a shared database has no central data store. In such a distributed ledger, each node on the network verifies each of the item, creating a new record for each item in the distributed database. It can be used to store static data such as personal information as well as dynamic data such as a transaction between two parties.

Ledgers are essentially records of data or transactions. In the era before the invention of computers, these records were stored in the form of paper which got digitization in the late 20th century. So far, a central authority verified and validated the records of the transactions being recorded. For example, the bank verifies each of the transaction taking place. With the distributed ledger technology, the traditional method of verification and validation will become obsolete as such a ledger will not be controlled or administered by any single authority but could be verified by any node on the network.

Blockchain is the perfect example that makes use of this technology and is built on top of it. A blockchain bundles the records of transactions into blocks that are chained together. These blocks are then broadcasted to all the nodes on the network thus the ledger gets distributed over to each node on the network and each node could verify the block's validity. The distributed ledger technology has high potential of speeding up the transactions as they remove the presence of any central authority meddling with the records. Also, it is considered to be much more secure, not being susceptible to hacking as each node on the network holds the records, creating a system that cannot be manipulated and attacked successfully. Much of the implementation of this technology has been around financial transactions, but its proponents believe its impact to be over a wider section.

3. Types of Blockchains

There are different types of blockchains each having their own purpose. We will briefly discuss two types of blockchains: anonymous and permissioned. The anonymous blockchains will be referred to as permission less blockchain. The category to which a blockchain belongs is defined by consensus. The validation of a blockchain can be done by private users which gets referred to as permissioned blockchain whereas if the blockchain can be validated by any user, the blockchain is permission less blockchain.

3.1 Permissioned Blockchains

If a blockchain can be validated by a defined group of verified user and owners, the blockchain is known as a permissioned blockchain. Only trusted users are allowed to participate. Since the users are verified, the proof of work is not necessary. These blockchain can be distributed across the open network, but it's not a necessity. It the blockchain is not distributed, it is considered as a private blockchain. Such a blockchain is centralized under an organization that has the controlling power to right to view and make transactions. In a private blockchain, there are chances of a hacker being able to hack out the login data of any of the verified user and use it to gain access to the blockchain and alter the existing chain, thus reducing the security aspect of the chain. The main advantages of private permissioned blockchains are privacy, better performance, faster evolvement and cost effectiveness.

3.2 Permissionless Blockchains

A blockchain in which every user is allowed to perform consensus and validate the blockchain, it is referred to as permissionless blockchain. In such a blockchain, each user is not a verified user and is considered anonymous, thus, the proof of work is required to ensure that the new block is valid in the chain and can be added to the chain.

This openness has advantages such as resistance against hacking or capital controls. It ensures that every user is allowed to see all balances and movements of all the incurring transactions, thus ensuring security. An added advantage such a blockchain is that it safeguards the users from the developers by establishing rules that even the developers do not have the authority to change.

4. Smart Contracts

One of the innovations that are made on top of the blockchain technology is the smart contract. A smart contract is a type of contract which is defined and placed in one of the blocks of the blockchain. It is similar to any other contract that is made within the organizations but a smart contract can be executed and implemented only within the blockchain.

To explain it further, let us consider the example of a transaction that takes place between two parties. Before a transaction takes place, the balance of the debtor is checked and verified if there are enough funds available with the debtor or not. If the debtor has availability of sufficient funds to make the transaction successful, the transaction goes through. In case of non-availability of funds, the transaction is declined and is not processed further. In the provided case, the agreements of the defined contract are whether the debtor is having sufficient funds to make the transaction successful or not. The transaction between the debtor and the creditor is the obligation of the contract. Smart contracts in a blockchain automatically enforces the obligation f the contract if and only if the agreements defined in the smart contract are successfully met. The provided example is done in banks for transferring money among different parties. When a transaction takes place between parties A & B in a bank, the bank checks and verifies the balance of the debtor, if there are sufficient funds available with the party. Then the bank debits from the account of party A and credits the amount in the account of party B and then it updates its ledger. In such a case, the parties have to trust the accountability of the bank for the transaction to take place. In case of any inconsistency, the parties will have to take the case to the bank and the bank will have the upper hand in deciding the proceedings further.

The same case can be implemented and executed in blockchain with the use of smart contracts placed in the blockchain. The agreements of the smart contract can be contain the availability of sufficient funds in the account of the debtor. If the agreement conditions are met, the transaction is made successful as per the obligation of the smart contract. This can be executed without any human interaction thus saving a lot of time and work. Replacing the scenario with a smart contract enabled blockchain has added advantages. Apart from saving work and time, the smart contracts provides the freedom to the users to not trust any single third party entity such as the bank since all the transactions can be verified using the distributed ledger.

There are a lot of applications of having the smart contracts in the blockchain and we will be discussing a couple of them.

In general, business is done between two companies, say company A is the client company that hires the company B to work and deliver a project. They agree to the terms and conditions of the agreement they made which states that the company A will be paying half of the fee when half of the work of the project is done and the other half to be paid on successful completion and delivery of the project. For company A, it is important for them that the project is done properly and timely and thus are resistant on paying out the fee whereas, it is in the better interests of the company B to obtain their part of the fee as soon as possible. This difference in the interests and expectations of the companies results in constant arguments between the companies where the company B argues that half of the project is completed and their half payment is due. On the other hand, the company A argues that their expectations as per that stage were different and they expected more to be delivered. Such nagging between the companies leads to a wastage of resources and time. Placing a smart contract in between could be a solution to the problem statement. It would automatically enforce the obligations stated in the contract as and when the agreement terms are completed and fulfilled. The rules of the project could be defined in the smart contract which cannot be bend as they would have been recorded in the blockchain.

The other example that we will be discussing briefly is regarding a problem scenario in the mortgage sector. In a general scenario, when a person applies for a mortgage, they

have to apply for the same to a bank by providing their personal and financial information. The bank in turn, reviews the information provided by the person applying for mortgage and on the basis of different scenarios decides whether to accept the mortgage request or to decline it. This step revolves for around weeks and could stretch up to months. The reviewing of the personal information is not time consuming. What is time consuming, is the human interaction that revolves around this particular process. An application submitted for mortgage is usually reviewed at different levels and rechecked just to be sure. This repetition of same steps leads to wastage of time and resources. If the records were to be maintained in the blockchain and checking these records be put in the agreements of the smart contract which obligated the person to be provided the mortgage if the records checked out to be correct, this lengthy process could be substantially minified thus saving resources and time. Using this, getting a mortgage could be as simple as going to the bank, identify themselves to the bank and in a matter of few minutes, the mortgage would be approved or rejected.

Smart contracts as compared to the traditional contracts are far cheaper, faster and fair. The wastage of time and resources involved in many cases in different sectors could be resolved through the use of smart contracts. These contracts not only define the agreements and the penalties around the contract, but also enforces the obligations of the contract.

5. Applications & Future Aspects

For most people, the entry point into the blockchain market is considered to be through cryptocurrencies such as bitcoin, etherium, dash and ripple. But sooner or later, the world will realize the potential of the blockchain technology and that there is more to blockchain than just cryptocurrencies.

This technology is helping the innovators create and design solutions in various industries such as retail, supply chain, healthcare, manufacturing, real estate, government and more.

This section will describe some aspects of the blockchain technology as how it could be implemented in different fields and where has it reached in the current scenario.

5.1 Financial Markets

One of the most promising application of Distributed Ledger technology such as blockchain is the payment transactions as done in banks. Currently, all the payment transaction clearances are handled by third party intermediaries. The implementation of blockchain technology to replace the current payment scenario will provide numerous advantages. So far, many companies have incorporated this technology in their business while some are on verge of integrating the same. Following are few of the examples that have taken a step forward in keeping up with the latest trends in technology.

Aeternity - This Company has implemented the concept of smart contracts and developed smart contract applications that are targeting IOT, video gaming and payment transactions. The users registered to the company will be able to exchange their value through the use of smart contracts on their mobiles.

Maersk - This company has been, in conjunction with Microsoft, trying to implement blockchains so as to manage marine information. Various trials are being conducted on the application. The main intent behind the implementation was to help the marine companies to predict the risk factors associated with the blockchain.

Augur - It is one of the decentralized ecosystem providing a forecast tool for the production markets by providing a peer-to-peer prediction marketing platform.

Barclays - Barclays being in the run for over a longer period of time, they have tried multiple scenarios with blockchain initiatives. They are trying to identify thefts and improve the finance and trade sector. They have been looking into ways to introduce blockchain based identity management for their branches. For providing better trading platform, Barclays have started a new Wave platform for secured way of signing and transfer of trades.

5.2 Real Estate Industry

There have been multiple attempts to introduce the blockchain technology into the real estate sector. The applications of this technology can be applied to both private as well as public real estate sectors. So far, the land registry records and public land ownership records are maintained as hard copy or stored in digital databases controlled, administered and accessible by the government itself. These land registry and ownership records can be put on blockchain allowing the public and stakeholders with the updated and real time access to these records as and when they require it. This will considerably reduce the disputes that arise due to ownership discrepancy and eliminate the need and use of middlemen required to authenticate the documents and resolve disputes. With the ownership records present on blockchain, one could resolve such discrepancies by backtracking to the original owner of the property easily, thus ultimately saving cost and time for the customers [7].

In respect to the public records, blockchain could be involved in the private real estate sector as well. Residential contracts and rental agreements between private parties can be placed on Blockchain and their execution could be done through the use of smart contracts. This is one of the ways to streamline private contracts and eliminate the use of third party agencies to facilitate the agreements between the counter-parties.

By making all the relevant processes and documentation involved in real estate sector automated over a decentralized network, the blockchain based real estate platform could

help cut down additional charges incurred due to the presence of third party agencies, inspection costs, loan fee charges and other non-vital charges and also speed up all these processes which currently utilize high amount of time to successfully process each of them. All these services and processes will be safe and secure and enforceable by the use of smart contracts.

5.3 Health Care Industry

Multiple applications of Distributed Ledger Technology based blockchain have been introduced into the healthcare industry. The health care industry requires high level of transparency at each level. Blockchain can be applied right from the start during the trials conducted for testing of a particular drug to the end stage where the drugs are manufactured in the factory to the part when they are supplied globally. At each level, the data can be stored over the blockchain and the steps involved measured as transactions.

Let us consider one of the examples of the implementation as how could it be helpful if moved over to the blockchain technology. When a batch of drugs is shipped from the factory floor, the batch record is validated and authenticated at the time and placed as a record on the blockchain. This batch is then subsequently authenticated, stamped and recorded on the blockchain at each intermediate point of delivery. This allows for tracking of drug as it makes it way from the factory floor to the distributer thus preventing the drug to fall into the wrong hands. This would streamline the process of distribution and tracking of drugs thus reducing the possibility of the customer receiving a counterfeit drug [4] as well as price manipulation and delivery of expired drugs.

Following are few examples of how the blockchain technology has already entered or about to enter the healthcare industry.

MedRec - The process of maintaining medical records is slow and cumbersome. So as to speed up the process of electronic medical records, MedRec has been developed by MIT Media Labs that aims at providing a blockchain solution for maintaining electronic medical records.

BlockVerify - As discussed above, blockverify is one of the applications that is being built to provide blockchain based anti-counterfeit product analyzer. This application will be able to verify the validity and authenticity of any product reaching the end customer.

5.4 Smart Governments

The most beneficial use of the blockchain technology could be to the government agencies by having instantaneous and simultaneous access to the database of public records stored over a distributed network. It could have many diverse applications. One of the most prominent would be identity management wherein a person's identity could be verified and authenticated through the public records available on the distributed database. Though there needs to be considerate amount of work to be done so as to implement this application, yet enabling this could impact many services that requires multiple days to verify and validate the identify of a person. The Estonian government has been experimenting with the identity management solutions on the blockchain technology.

Another application that could prove to be useful for the government as well as the public is in Regulatory and Taxation services. Many financial institutions are looking forward to place their personal and institutional transactions on the blockchain [6]. The regulators can impose various restrictions on the transaction execution which can be enforced with the help of smart contracts that can be placed into the blockchain. This could help bring down the effort of compliance and auditing leading to considerable save in the resource utilization and reduces the need of various intermediary processes involved.

Another interesting application that can be brought is in the field of foreign aid. The foreign aid can be much more effectively distributed in a far more efficient way to reach its intended audience in the disaster zones or war zones [5]. This would result in a timely delivery of the foreign aid and considerably reduces the middlemen involved and eliminates the channels for corruption and misuse of the aid provided.

One last yet important use of this technology in the creation of a smart government is to integrate it in the voting system of the country. Using an anonymous blockchain, each citizen can submit their vote without revealing their identity to the parties and the different parties can together determine the results through a consensus [3]. This would eliminate considerable voting environment overhead.

3. CONCLUSION

A lot of research work is being done on the integration of blockchain technology into businesses of varied kinds, yet implementing a full-fledged system based on top of this technology in different fields require huge amount of research to be done further. Most use cases discussed and developed so far are public permissioned blockchains. There needs to be global blockchain standards so as to create and enhance the concurrent and coherent development of systems and to prevent the potential misuse of the distributed ledger technology. It is a technology that is evolving every day holding huge transformative potential in wide range of sectors. The main challenge to be faced is to strike the right balance between the safety and integrity of the system while paving the way for innovation and development of this rapidly evolving technology.

REFERENCES

[1] Andreas M. Antonopoulos, Mastering bitcoin, unlocking digital cryptocurrencies, 1st edition, December 2014

[2] Imran Bashir, Mastering bitcoin, unlocking digital cryptocurrencies, 1st edition, March 2017

[3] Melanie Swan, Blockchain: Blueprint for a New Economy

[4] Blockchain Technology Could Help Solve $75 billion Counterfeit Drug Problem

[5] Deloitte, Blockchain: Disrupting the Financial Services Industry

[6] Forbes – The Tiny European Country that became a global leader in digital government - http://www.forbes.com/sites/dell/2016/06/14/the-tiny-european-country-that-became-a-global-leader-in-digitalgovernment/#45fc179a4c7f

[7] Reuters News - http://in.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515

BIOGRAPHY

Lakshay Swani
A tech-savvy person, eager to gain knowledge about the latest technologies.