International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 17, Issue 4 (Jul. – Aug. 2021), PP. 01-05

Blockchain Technology

Dr. (Mrs.) Pratibha Kumar
Associate Professor (Department of Mathematics)
Kirori mal College
University of Delhi, Delhi

Mr. Karan Chaudhry
Assistant Section Officer
Ministry of Defence
Government of India

ABSTRACT: *In this paper we study the concept of blockchain technology which is rapidly changing the way we transact information and do business. Discussing its origins and features, we will look into its various applications such as in finance, supply chain and healthcare.*

Date of Submission: 20-06-2021 Date of Acceptance: 05-07-2021

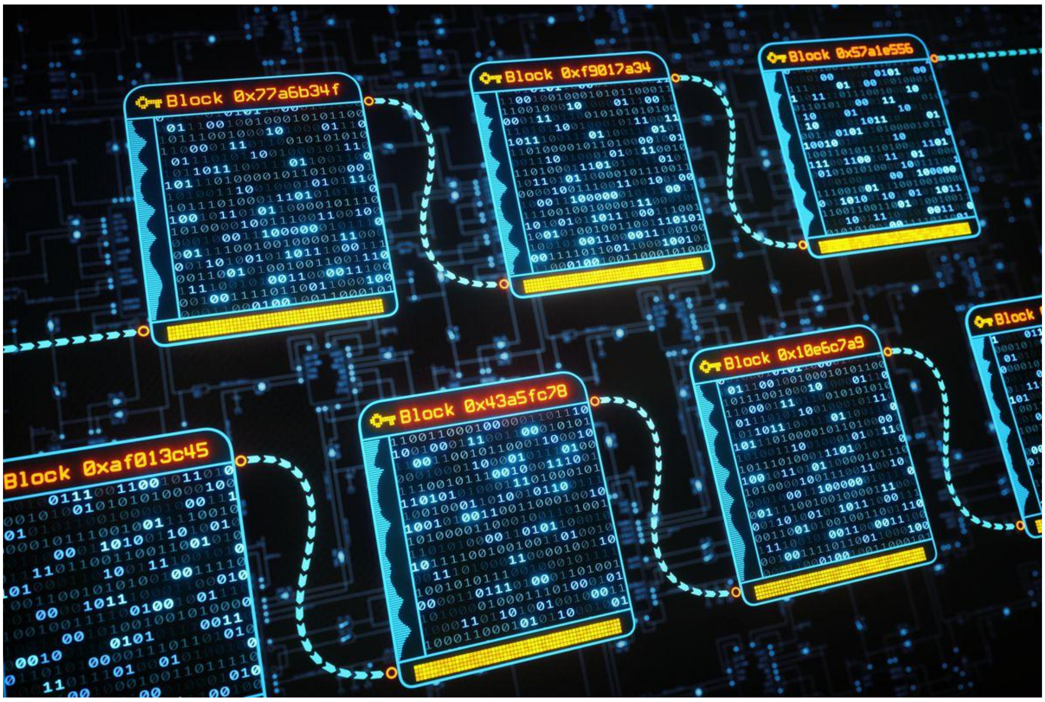
I. INTRODUCTION

Blockchain is the most disruptive and revolutionising technology in the digital space today.

In the simplest terms, Blockchain is a specific type of database.

("A database is a collection of information that is stored electronically on a computer system." Information in databases is typically in table format allowing for easier access and search and filter operations.)

However, it differs from other typical databases in the way it stores information. Blockchain collects information in groups or blocks that are chained together. So instead of data being stores in a table format, as in typical databases, data is stores in chunks (blocks) in blockchain.



Blockchain can be private or public or a hybrid of the two. A private blockchain is controlled by a single entity. However, a public blockchain is completely decentralised and is one of technology's most important attributes. As a distributed and immutable ledger, blockchain allows us to track almost anything, tangible or intangible.

Introduction of any new information on a blockchain is done by adding a new block to the already existing chain of blocks. Each block has specific amount of storage space. Once that space is taken up, a newly filled up block with its own information is chained to the end of the previous block. This makes the blockchain chronological in order.

This technology also makes blockchain create an irreversible timeline of data when implemented in a decentralised manner. Every block created is set in stone, is given an exact timestamp and becomes part of the unchangeable timeline.

Brief History of Blockchain:

Blockchain was originally created as the technology behind bitcoin in the year 2008. An individual or a group under the name of Satoshi Nakamoto published a then not so popular paper titled "Bitcoin – A peer-to-peer Electronic cash system". It showed how cash could be transferred digitally from one party to another directly without it going through a bank or any other third-party financial institution.

A few months later a new protocol was released with the Genesis block of 50 coins where anyone could install an open- source program in their computer and be part of the bitcoin per-to-peer network. From then the popularity of the technology and crypto currency in general has been increasing steadily.

Transparency and security

The blockchain technology being decentralise in nature makes it possible for anybody to view the data either through the personal nodes or by using block chain explorers which allow for seeing real-time transactions.
Blockchain's security and trust comes from the fact that any new block is added to chain after a consensus among the participating nodes. It is very difficult for data to be changed and altered without the majority being reached among the participating nodes.

There are three main features of blockchain:

Verifiability: with the attribute of it being decentralised, the block chain has a copy of all the data in its participating nodes. Therefore this makes verification of any transaction easy and secure as it is not tied on to a single point of failure.

Immutability: this feature helps maintain the integrity of the technology. It refers to the attribute that any new block added is in reference to the previous block, therefore making a permanent chain of blocks linked to each other.

Consensus mechanism: any new block is added to the blockchain via a distributed consensus as its protocol. Addition of a new block is only successful when majority of the participating nodes agree.

The immutability stems from the use of 'hash' in the blocks. Hashcodes are created by a mathematical function that transforms digital information into a string of letters and number. If by any chance this information is edited in any way, the hashcodes change as well and therefore trigger a response at every participating node. Further, header includes metadata such as block reference number, the exact time the block was created and a link back to the previous block. Whereas its content may contain a list of digital assets and instruments including amounts and the addresses of the parties.

For example, if a hacker tries to alter the blockchain in order to steal a bitcoin, he will have to alter his own single copy of the blockchain. However, that copy will not match the copy of the blockchain ledger with everybody else in the participating nodes. By cross-referencing their copies against each other, the copy of the hacker will stand out and will be denied processing.

Therefore, for the hacking to be successful, the hacker would have to have control over 51% of the blockchain nodes, which would require an immense number of resources and technological might as there would be a need for changing timestamps and hashcodes in all these participating nodes.

The case of bitcoin doing such an attempt would be insurmountable as it would be exceedingly expensive and would also make the network members fork-out into a new version of the team that has not been affected.

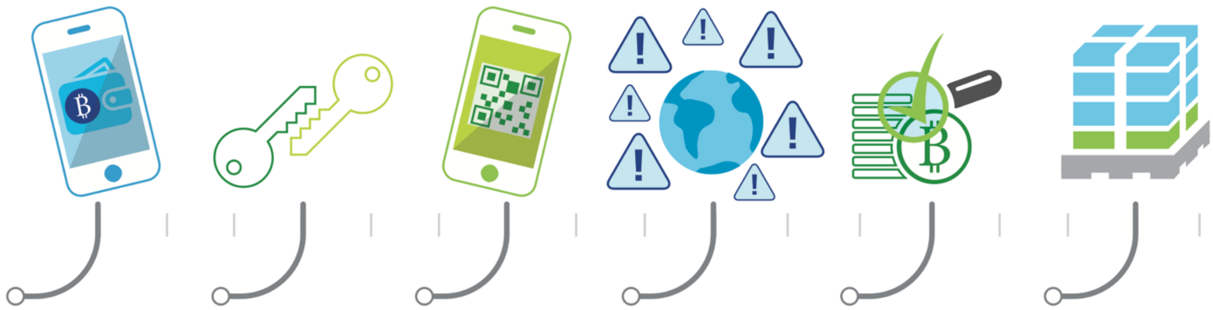
Blockchain and Bitcoin

In order to understand the decentralised attribute of blockchain, it is useful that we see how the most popular cryptocurrency Bitcoin functions. Bitcoin stores its data over the blockchain technology where every Bitcoin transaction ever made is stored. Unlike a company where the database of its employees and clients is stored over its sever, completely and centrally controlled by people working for the company, the data in Bitcoin is stored in thousands of computers spread out in different geographies globally. These computers and locations are called nodes of the Bitcoin network.

Each node has complete record of the data created since the inception of bitcoin and is completely decentralised, not controlled or operated by a single entity.

In an event of an error in one node, thousands of other nodes can help fix it immediately by pin-pointing the incorrect information lodged. This also prevents from one node to incorrectly alter data in other nodes. Therefore, the history of transactions and records are irreversible and immutable and fruits of such a hack would not mean anything as the value of bitcoin would crash and would give the hackers nothing in the end.

Figure 1. How the Bitcoin blockchain works



Bob owes Alice money for lunch. He installs an app on his smartphone to create a new Bitcoin wallet. A wallet app is like a mobile banking app and a wallet is like a bank account.

To pay her, he needs two pieces of information: his private key and her public key.

Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.*

The app alerts Bitcoin 'miners' around the world of the impending transaction. 'Miners' provide transaction verification services.

The miners verify that Bob has enough bitcoins to make the payment.

Many transactions occur in the network at any time. All the pending transactions in a given timeframe are grouped (in a block) for verification. Each block has a unique identifying number, creation time and reference to the previous block.

*Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

Graphic: Deloitte University Press. Source: American Banker[20]

Above is a real-world example of blockchain in Bitcoin works and executes secure transactions.

Applications

Today block chain technology finds applications in a wide righty of areas, be it financial or non-financial sectors, where the validity of transaction is on a third-party.

Banking and Finance: There are several limitations with the financial institutions which open only for a few hours on weekdays. There is also the issue of secure transaction of money and the fees paid for every transaction to these financial intermediaries. By integrating the block chain technology into the banks the consumers can access and process information immediately and these service can be provided 24x7, 365 days a year, regardless of holidays or time of day or week.

Also based on the amount of money being transferred the fee paid to these financial institutions is very high therefore blocking technology would not only make the transactions secure, immediate and seamless but will also help reduce the cost of transaction.

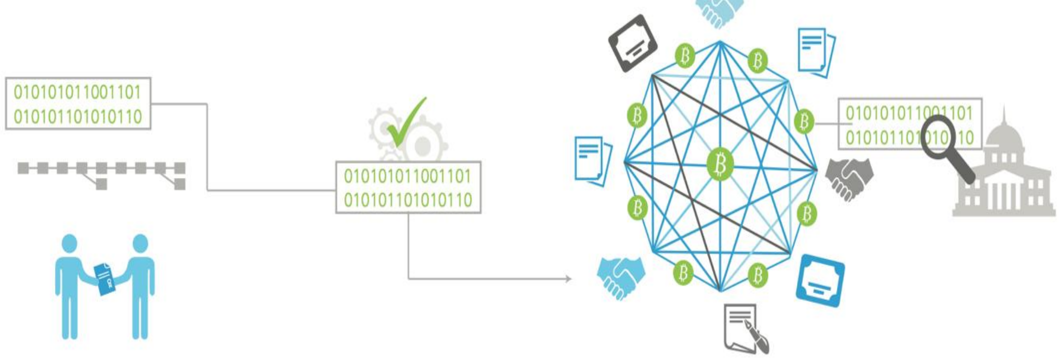
Currency: The issue of currency and it's printing by the Federal Reserve in the US and the Reserve Bank of India in India creates another important issue of inflation and the role of government and its responsibility in printing money without backing it up with gold reserves. This means that the value the money that the person holds with herself depends on the whim of the central bank which might not function appropriately in the event of an unstable government.

By spreading the operations in different geographies and different participating nodes, the decentralised and distributed ledger system under the blockchain can help remove the need of the central authority to print money. This removes the processing in transaction fee and also creates a more stable currency at the end which is not controlled by the wishes of one central authority. There are already cryptocurrencies such as Bitcoin and Litecoin can help people do transactions more transparently, speedily and securely thus removing the control of a central authority.

Smart Contracts: An important application of block chain technology is smart contracts that was invented by Nick Szabo in 1994. It is used to automatically execute contract between participating bodies. A smart contract is basically a computer code that is built into the block in order to facilitate, verify and negotiate an agreement between parties. These smart contracts normally operate under a predefined set of conditions and at the event of satisfying of these agreements the contracts are finalised automatically.

To give an example, a tenant who is planning to lease an apartment can use smart contract. Here the landlord would agree to give the tenant the door code as soon as the tenant pays the security deposit. Both the tenant and the landlord will send their respective information in the form of money and code. The contract would be successfully executed once the exchange of information completed. In case the tenant does not pay the security deposit, the contract would not be competed therefore ending the lease. This process will eliminate the fees and processing charges that are associated by a third-party mediator or entity.

Figure 2. Using the Bitcoin blockchain for smart contracts



1 An option contract between parties is written as code into the blockchain. The individuals involved are anonymous, but the contract is in the public ledger.

2 A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3 Regulators can use the block chain to understand the activity in the market while maintaining the privacy of individual actors' positions.

Graphic: Deloitte University Press, DUPress.com

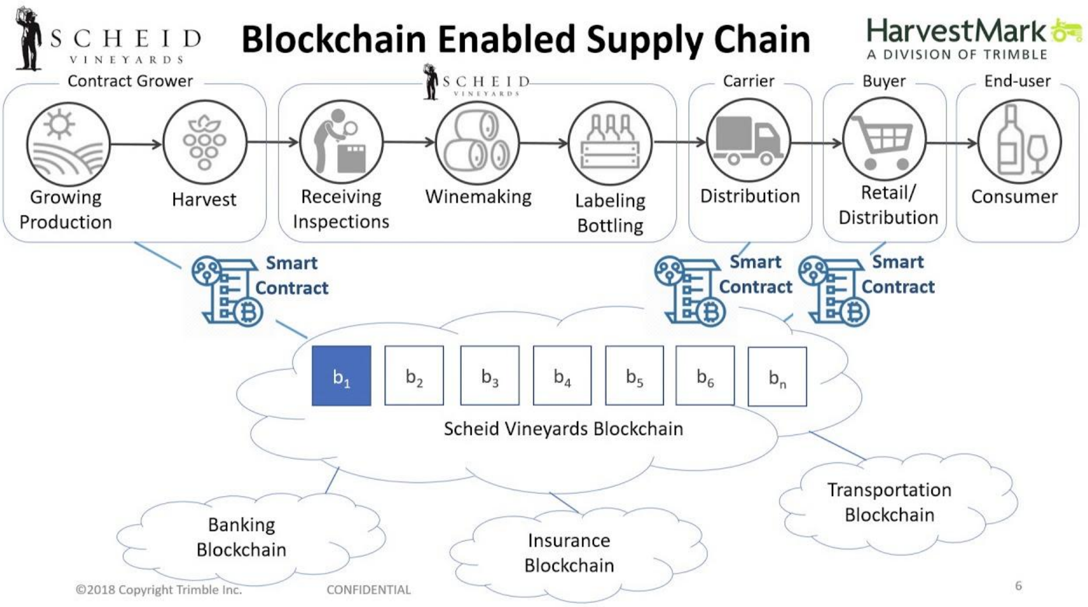
Healthcare Sector: In the healthcare sector blockchain technology can help securely store patient's medical records. Whenever a medical record is created and is approved by the medical practitioner, it can be written into the blockchain. This will provide patients with a proof and confidence in the treatment. It will also help in reducing misuse of personal medical data of patients.

Recording property rights: The process of recording property rights at any local magistrate's office is burdensome and inefficient. The requirement of physical deeds to be delivered to government employees and be manually entered into a central database attracts fraudulent activities.

The entire process is infested with human error and is also costly and time consuming. Blockchain technology can eliminate all that by scanning and putting the documents and its data into its database where the record is accurate and easily accessible.

Voting: Blockchain technology can help eliminate election fraud and boost voter confidence and turn-out by facilitating a secure modern voting system. It can make the rigging of elections nearly impossible by creating an immutable record. The blockchain protocol would also increase transparency by providing real-time data to the citizens which would eliminate the need for any recount or any other fraud threatening democracy.

Supply Chain: Blockchain technology has extensive uses for development of transparent and robust supply chain management. For example, with IBM Food Trust, suppliers can use blockchain to record the origin of materials therefore ensuring that the goods that are sourced are organic or fair or local. The food industry is also implementing the block chain technology increasingly in order to track and ensure food quality from the farm to the user during the entire journey.



Above is an example of blockchain used in the wine industry. The ingredients and packaging is all traced and continually kept in check for ensuring production and supply of high-quality products.

II. SUMMARY

The blockchain technology has revolutionised and disrupted the way data is stored and transactions are carried out in the digital sphere. It helps improve accuracy by removing human involvement in verification and creates a more transparent and decentralised systems which are harder to tamper. The transactions are secure, private and efficient and the data storage is immutable through creation of several participating nodes around different geographies globally. Even with high cost is associated with it, the blockchain technology is going to lead the advancements in digital technology for years to come.

Sources:

[1]. https://www.investopedia.com/terms/b/blockchain.asp
[2]. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-what-is-blockchain-2016.pdf
[3]. https://www.forbes.com/sites/forbesbusinesscouncil/2020/09/28/what-makes-a-blockchain-project-successful/?sh=7eb945982b44
[4]. https://www.youtube.com/watch?v=55aTGNx5vug
[5]. https://builtin.com/blockchain

Dr. (Mrs.) Pratibha Kumar, et. al. “Blockchain Technology." *International Journal of Engineering Research and Development*, vol. 17(04), 2021, pp 01-05.