BLOCKCHAIN TECHNOLOGY

Srishti Jain[1], Jasmine Singla[2], Anubhav Sharma[3], Indu Khatri[4]
[1,2,3] B.tech Student, [4]Assistant Professor
Department of Computer Science Engineering
Mahavir Swami Institute of Technology, Sonepat

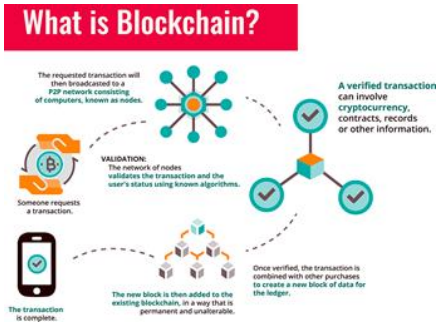
Abstract: - Blockchain is the technology that can lead to significant changes in our business environment and will have great impact on the next few decades. It can change the way we perceive business processes, and can transform our economy. Blockchain is a decentralized and distributed ledger technology that aims to ensure transparency, data security and integrity, since it cannot be tampered or forged.

Most of the current research related to Blockchain Technology is focusing on its application for cryptocurrencies, such as Bitcoin and only a limited number of re- search is targeted at exploring the utilization of Blockchain Technology in other environments or sectors. Blockchain Technology is more than just cryptocurrency, and it can have several applications in government, finance and banking industry, accounting and Business Process Management. Therefore, this study attempts to investigate and explore its opportunities and challenges for the current or future applications of Blockchain Technology. Thus, a large number of published studies were carefully reviewed and analyzed based on their contributions to the Blockchain's body of knowledge.

Keywords: - Blockchain Technology, Ledger, Applications, Business

1. INTRODUCTION

Blockchain technology is easily defined as a demo- graphic, distributed environment that records digital access to digital assets. With a natural design, the data in the blockchain cannot be changed, making it a legitimate distraction in industries such as payments, internet security and health care. Blockchain, called Distributed Ledger Technology (DLT), makes the history of any digital asset unchangeable and transparent. Through decentralization and cryptographic hashing. A simple analogy to understand blockchain technology is Google Doc. When we create a document and share it with a group of people, the document is still being distributed instead of being copied or transmit- ted. This creates a nationwide distribution chain that gives everyone access to the document at the same time. All changes in the document are recorded in real time and are completely transparent changes. Of course, blockchain is much more complex than Google Doc, but the analogy is appropriate because it reflects three critical technological perspectives: Blockchain is a promising and flexible technology because it helps reduce risk, eliminates fraud and exposes the fastest way to multi-use.



Blockchain technology is a flexible digital com- puter protocol recording and storing information on multiple computers or locations. One of the most important Blockchain features is the so called "Ledger", which similar to the Walport related website. Blockchain is a list of an encrypted digital record or transaction, called a block. Each block then "Bound" in the following block, in sequence, in chronological order, using a cryptographic signature. Blocks contain a copy of last transaction since the last block was added. So, a shared block, or ledger, is connected to all participants using their computers network to verify or confirm a transaction, eliminating the need for a third party Blockchain is used to protect and distribute data in a new and unique way. The elimination of a central in- stance in the distributed network implies a radical shift to direct transactions between non-intermediaries or intermediary services. Therefore, Blockchain can only be updated by the agreement between the participants in the system and the transaction will never take place changed or deleted. Its distributed data is not available can be avoided, used or distorted in the same way as traditional, central website with user-controlled access system.

In other words, the data does not change and once it has been written a Blockchain, no one, not even a system administrator, can fix or remove it from the ledger. As such, each data block has a time stamp and is linked to a chronology with cryptographic sig- nature Walport. Blockchain Technology can be used for almost any type of work, including value, such as money, property, land ownership, medical records or votes.

Blockchain does not require data migration to a project; all relevant activities the data will be stored in a manual and the status will then be taken from it. Since, Blockchain is a distributed system without central control or authority and is not controlled with a single control center as there may be system management there is not a single point of failure. So, in business, theoretically, there would be no need for an IT professional to monitor security in the blockchain database.

Despite these opportunities, it is important to emphasize that Blockchain is very large new technology. As a result, there are only a limited number of cases which technology is used in Aru. Proven example, Bitcoins which is a successful launch of Blockchain Technology, and it has proven to be an effective solution in creating trust an unreliable ecosystem without central authority.

Blockchain is a website that stores encrypted data blocks and integrates them together to form a single true source of data sequencing. Digital assets are distributed instead of being copied or transferred, creating a fixed asset record. Assets are categorized, allowing full real-time access and transparency to the public Transformation ledger preserves the integrity of the document, which creates an asset trust. Blockchain environment security measures and public book making it an advanced technology in almost every single sector.
The whole point of using a blockchain is to allow people - especially, people who do not trust each other to share important data in a secure, uninterrupted manner.

2. CHARACERISTICS OF BLOCKCHAIN

Blockchain Technology has the following characteristics:

- **Resilience:** Blockchain is often replicated architecture. The chain is still operated by most nodes in the event of a massive attack against the system.
- **Time reduction:** In the financial industry, blockchain can play a vital role by allowing the quicker settlement of trades as it does not need a lengthy process of verification, settlement, and clearance because a single version of agreed- upon data of the shared ledger is available be- tween all stack holders.
- **Reliability:** Blockchain certifies and verifies the identities of the interested parties. This removes double records, reduces rates and accelerates transactions.
- **Unchangeable transactions:** By registering transactions in chronological order, Blockchain certifies the inalterability, of all operations which means when any new block has been added to the chain of ledgers, it cannot be re- moved or modified.
- **Fraud prevention:** The concepts of shared in- formation and consensus prevent possible losses due to fraud or embezzlement. In logistics-based industries, blockchain as a monitoring mechanism act to reduce costs.
- **Security:** Attacking a traditional database is the bringing down of a specific target. With the help of Distributed Ledger Technology, each party holds a copy of the original chain, so the sys- tem remains operative, even a large number of other nodes fall.
- **Transparency:** Changes to public blockchain are publicly viewable to everyone. This offers greater transparency, and all transactions are immutable.
- **Collaboration:** Allows parties to transact directly with each other without the need for mediating third parties.
- **Decentralized:** There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated and all valid transactions are added one by one.

3. HOW DOES BLOCKCHAIN WORK?

Blockchain consists of three important concepts: blocks, miners and nodes.

BLOCKS
Each chain has many blocks and each block has three basic features: Data in the block. A whole 32-bit number called a nonce. A nonce is generated randomly when a block is formed, and then produces a block title hash. The hash is a 256-bit number married to a nonce. It should start with a large number of zeros (i.e., be very small). When the first chain block was built, the nonce produced a cryptographic hash. Data on the block is considered signed and permanently bound again hash unless excavated.

MINERS
Miners build new blocks in the series through a process called mining. In blockchain each block has a nonce with its own unique hash, but also refers to the hash of the previous block chain, so digging a block is not easy, especially on large chains. Miners use special software to solve a complex mathematical problem in a surprising way to find a nonce that has adopted a hash. Because the nonce is only 32 bits too hash is 256, with approximately four billion nonce-hash com- pounds to be excavated before it can be found prop- erly. When that happens they are called miners to find a ”gold nonce” and have their block added to the chain. Making changes to any block earlier in the se- ries requires re-mining not just a block with a change, but all subsequent blocks. That is why it is so it is very difficult to use blockchain technology. Think of it as ”mathematical safety” as finding gold nonces requires a lot of time and computer. power. If the block is successfully mined, the change is accepted by all nodes in the network and the miner is rewarded financially.

NODES
One of the most important concepts in blockchain technology is distribution. No single computer or organization can own a series. Instead, it is a distributed ledger with nodes connected to the chain. Nodes can be any type of electronic device that stores blockchain copies and keeps the network running. Every node has its own copy of the blockchain and the network must algorithm accept any newly excavated block in order for the chain to be updated, trusted and verified. As blockchain are transparent, all actions in a book can be easily viewed and viewed. Each participant is assigned a unique alphanumeric ID number that shows their transaction. Combining public knowledge with the evaluation system and balance helps the blockchain maintain integrity and build trust between users. In fact, blockchain can considered as an

in- crease in technological trust.

4. HISTORY

Although blockchain is a new technology, it already boasts a rich and interesting history. The following is a brief timeline of some of the most important and notable events in the development of blockchain.

2008
Satoshi Nakamoto, a pseudonym for a person or group, publishes "Bitcoin: A Peer to Peer Electronic Cash System."

2009
The first successful Bitcoin (BTC) transaction occurs between computer scientist Hal Finney and the mys- terious Satoshi Nakamoto.

2010
Florida-based programmer Laszlo Hanycez completes the first ever purchase using Bitcoin — two Papa John's pizzas. Hanycez transferred 10,000 BTC's, worth about $60 at the time. Today it's worth $80 million. The market cap of Bitcoin officially exceeds
$1 million.

2011
1 BTC = $1USD, giving the cryptocurrency parity with the US dollar. Electronic Frontier Foundation, Wikileaks and other organizations start accepting Bit- coin as donations.

2012
Blockchain and cryptocurrency are mentioned in pop- ular television shows like The Good Wife, inject- ing blockchain into pop culture. Bitcoin Magazine launched by early Bitcoin developer Vitalik Buterin.

2013
BTC market cap surpassed $1 billion. Bit- coin reached $100/BTC for the first time. Buterin publishes "Ethereum Project" paper suggesting that blockchain has other possibilities besides Bitcoin (e.g., smart contracts).

2014
Gaming company Zynga, The D Las Vegas Hotel and Overstock.com all start accepting Bitcoin as payment. Buterin's Ethereum Project is crowdfunded via an Initial Coin Offering (ICO) raising over $18 million in BTC and opening up new avenues for blockchain. R3, a group of over 200 blockchain firms, is formed to discover new ways blockchain can be implemented in technology. PayPal announces Bitcoin integration.

2015
Number of merchants accepting BTC exceeds 100,000. NASDAQ and San-Francisco blockchain company Chain team up to test the technology for trading shares in private companies.

2016
Tech giant IBM announces a blockchain strategy for cloud-based business solutions. The government of Japan recognizes the legitimacy of blockchain and cryptocurrencies.

2017
Bitcoin reaches $1,000/BTC for the first time. Cryp- tocurrency market cap reaches $150 billion. JP Mor- gan CEO Jamie Dimon says he believes in blockchain as a future technology, giving the ledger system a vote-of-confidence from Wall Street. Bitcoin reaches its all-time high at $19,783.21/BTC. Dubai announces its government will be blockchain-powered by 2020.

2018
Facebook commits to starting a blockchain group and also hints at the possibility of creating its own cryptocurrency. IBM develops a blockchain-based banking platform with large banks like Citi and Barclays signing on.

2019
China's President Ji Xinping publicly embraces blockchain as China's central bank announces it is working on its own cryptocurrency Twitter Square CEO Jack Dorsey announces that Square will be hir- ing blockchain engineers to work on the company's future crypto plans The New York Stock Exchange (NYSE) announces the creation of Bakkt - a digital wallet company that includes crypto trading

2020
Bitcoin almost reaches PayPal announces it will allow users to buy, sell and hold cryptocurrencies The Ba- hamas becomes the world's first country to launch its central bank digital currency, fittingly known as the "Sand Dollar" Blockchain becomes a key player in the fight against COVID-19, mainly for securely storing medical research data and patient information

5. TYPES OF BLOCKCHAIN

There are several types of Blockchains, some of the most important are:

- Public Blockchain
- Private Blockchain
- Permissioned blockchain networks
- Consortium Blockchain (Hybrid Blockchain).

Each type has its advantages and disadvantages, allowing them to meet the needs of various applications .

PUBLIC BLOCKCHAIN
Using Public Blockchain, anyone can transact on the network transactions which are transparent and are anonymous. A Public Blockchain, such as bitcoin, is completely decentralized. The system operates based on users' consensus; there is no central point of failure. However, Public Blockchain is vulnerable to system attacks. For instance, an attacker could recreate and properly chain all the blocks that had been modified, without being detected by the participants. Drawbacks might include substantial

computational power required, little or no privacy for transactions, and weak security. These are important considerations for enterprise use cases of blockchain.

PRIVATE BLOCKCHAIN

A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the net- work, controlling who is allowed to participate, execute a consensus protocol and maintain the shared ledger. The transactions are secret, the data is not avail- able for public view, but the members are known. In a private Blockchain network, a participant cannot read or write the Blockchain unless the participant has a Permission or an invitation to join the network.

Private Blockchain is usually used by large companies with permissions defined between various stake- holders of the enterprise Blockchain. For instance, a bank can have its own Blockchain network for its private use with restricted access to its various stakeholders such as customers, employees and suppliers.

Depending on the use case, this can significantly boost trust and confidence between participants. A private blockchain can be run behind a corporate fire- wall and even be hosted on premises.

PERMISSIONED BLOCKCHAIN NETWORKS

Businesses who set up a private blockchain will generally set up a permissioned blockchain network. Even public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what transactions. Participants need to obtain an invitation or permission to join .

CONSORTIUM BLOCKCHAINS

Consortium Blockchain is a hybrid model of both Public and Private Blockchain. Choosing this model, enterprises or institutions can have their own Private Blockchain network to share the data among the consortium participants such as banks, institutions and other enterprises or firms.

Multiple organizations can share the responsibilities of maintaining a blockchain. These pre-selected organizations determine who may submit transactions or access the data. A consortium blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.

USES

MARKETS

- Billing, monitoring and Data Transfer
- Quota management in the Supply Chain Network

GOVERNMENT SECTOR

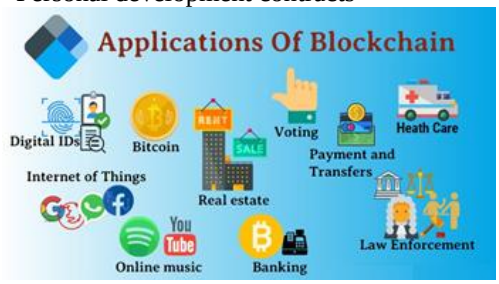
- Transnational personalized governance services Voting, propositions P2P bond,
- Digitization of documents/ contracts and proof of ownership for transfers
- Registry Identify
- Tele-attorney service
- IP registration and exchange
- Tax receipts Notary service and document registry

IOT

- Agricultural drone sensor networks
- Smart home networks
- Integrated smartcity.
- Smart home sensors
- Self-driving car
- Personalized robots, robotic component
- Personalized drones
- Digital Assistants

HEALTH

- Data management
- Universal EMR Health databanks
- QS Data Commons
- Big health data stream analysts
- Digital health wallet Smart property
- Health Token
- Personal development contracts



Science Art

- Supercomputing
- Crowd analysis
- P2P resources
- Digital mind fit services

Finance Accounting

- Digital Currency Payment
- Payments Remittance
- Decartelized Capital markets using a network of the computer on the Blockchain
- Inter-divisional accounting
- Clearing Trading Derivatives
- Bookkeeping

LIMITATIONS

Higher costs: Nodes seek higher rewards for completing Transactions in a business which work on the principle of Supply and Demand

Slower transactions: Nodes prioritize transactions with higher rewards, backlogs of transactions build up .

Smaller ledger: It not possible to a full copy of the Blockchain, potentially which can affect immutability, consensus, etc.

Transaction costs, network speed: The transactions cost of Bitcoin is quite high after being touted as 'nearly free' for the first few years.

Risk of error: There is always a risk of error as long as the human factor is involved. In case a blockchain serves as a database, all the incoming data has to be of high quality. However, human involvement can quickly resolve the error.

Wasteful: Every node that runs the blockchain has to maintain consensus across the blockchain. This offers very low downtime and makes data stored on the blockchain forever unchangeable. However, all this is wasteful, because each node repeats a task to reach consensus.

MYTHS vs REALITY

MYTHS	REALITY
• *It solves every problem.*	• *No, it is just a database.*
• *Trustless Technology*	• *It can shift trust and* also spread trust.
• *Secure*	• *It focuses integrity* and not confidentiality.
• *Smart contracts are* always legal.	• *It only executes parts of* some legal contacts.
• *Immutable*	• *It only offers* probabilistic immutability.
• *Need to waste* electricty.	• *Emerging blockchains are* efficient.
• *It is inherently* unusable.	• *Emerging blockchains are* scalable.

6. CONCLUSION

Blockchain technology is revolutionary. It will make life simpler and safer, changing the way personal information is stored and how transactions for good and services are made. Blockchain technology creates a permanent and immutable record of every transaction.

This impenetrable digital ledger makes fraud, hacking, data theft, and information loss impossible. The technology will affect every industry in the world, including manufacturing, retail, transportation, healthcare, and real estate Companies as Google, IBM, Microsoft, American Express, Walmart, Nestle, Chase, Intel, Hitachi, and Dole are all working to become early adopters of blockchain. Nearly $400 trillion across various industries is set to be transformed by blockchain.

REFERENCES

- https://www.dcvelocity.com/articles/43584-hybrid-blockchain-the-best-of-both-public-and-private-blockchain
- https://www.oreilly.com/library/view/blockchain/9781491920480/ch07.html
- https://developer.ibm.com/technologies/blockchain/
- https://ivedix.com/the-enormous-potential-of-blockchain-technology/
- https://www.garyfox.co/how-blockchain-works-infographic/amp/
- https://devopedia.org/types-of-blockchains
- https://www.dcvelocity.com/articles/43584-hybrid-blockchain-the-best-of-both-public-and-private-blockchain
- https://l3cos.com/permissioned-blockchain.html
- https://www.researchgate.net/Typical-Application-of-the-Blockchain-Technology

