D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji.

(An Autonomous Institute, Affiliated to Shivaji University, Kolhapur)

Accredited with 'A+' Grade by NAAC

Department of Computer Science & Engineering

2021-2022

SEMINAR REPORT ON

Blockchain

Under The Guidance Of

Prof. V.G.Khetade

Group Members-

1. SHREYASH UMED TEMBHURNE 19UCS130
2. DHAIRYASHIL DHANANJAY SHINDE 19UCS122
3. GOURAV SANJAY SHINDE 19UCS124
4. PRITESH SURESH SHETTY 19UCS121

D.K.T.E. Society's

Textile and Engineering Institute, Ichalkaranji

(An Autonomous Institute, Affiliated to Shivaji University, Kolhapur)

Department of Computer Science and Engineering

CERTIFICATE

This is to certify that,

Sr.	PRN	Name of Student
1.	19UCS130	SHREYASH UMED TEMBHURNE
2.	19UCS122	DHAIRYASHIL DHANANJAY SHINDE
3.	19UCS124	GOURAV SANJAY SHINDE
4.	19UCS121	PRITESH SURESH SHETTY

have successfully completed the Seminar work, entitled,

Blockchain

In partial fulfillment for the curriculum of T. Y. B. Tech Computer Science and Engineering. This is the record of their work carried out during academic year 2021-2022.

Date: 14/10/2021 **Place: Ichalkaranji**

Prof. V. G. Khetade	**Prof. Dr. D. V. Kodavade**	**Prof. Dr. P. V. Kadole**
[Guide]	**[H.O.D.]**	**[Director]**

Index

Introduction

Blockchain is the backbone Technology of Digital Cryptocurrency Bitcoin. The blockchain is a distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Each transaction verified by many participants of the system. It contains every single record of each transaction. Bitcoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first became known when a person or Group of individuals name 'Satoshi Nakamoto' published a white paper on "Bitcoin: A peer to peer electronic cash system" in 2008. Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction.

In recent years, blockchain technology has evolved far beyond bitcoin and is now being tested in a broad range of business and financial applications. However, blockchain technology is still emerging and has not yet been proven at enterprise scale, which is a fundamental challenge to blockchain's transformative potential. In addition, many accounting firms have undertaken blockchain initiatives to further understand the implications of this technology.

1. The term "bitcoin" is used when describing a bitcoin as a unit of account, whereas "Bitcoin" is used when describing the concept or the entire network designed by Satoshi Nakamoto.

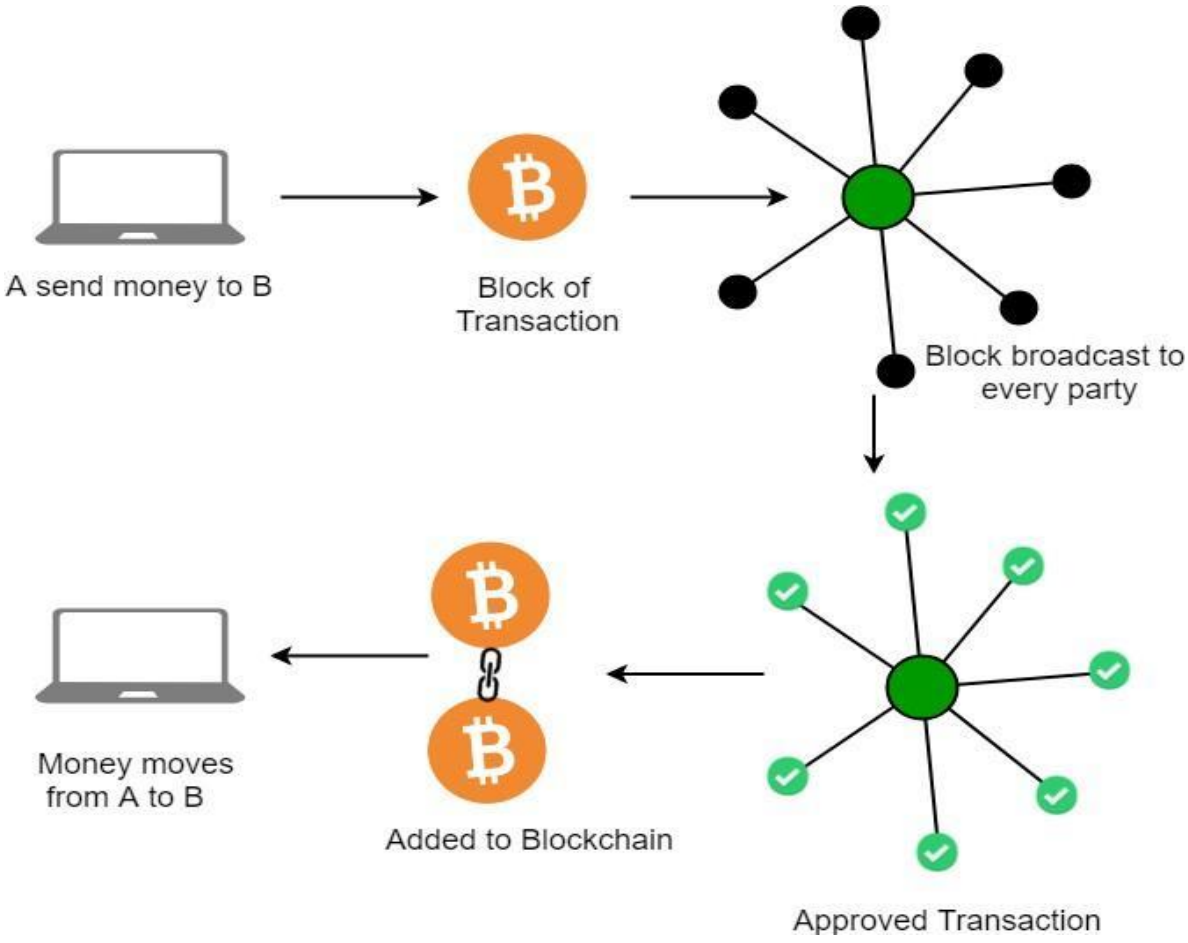
2. Digital currency can be defined as an Internet-based form of currency or medium of exchange (as distinct from physical currency such as banknotes and coins) that exhibits properties like physical currencies but allows for instantaneous transactions and borderless transfers of ownership.

3. Peer-to-peer computing or networking is based on a distributed application architecture that shares tasks among peers. All participants engage equally in the application to form a peer-to-peer network of nodes. 4 Modern cryptography uses mathematics, computer science and electrical engineering to enable secure communication between two parties in the presence of a third party.

What Is Blockchain Technology?

A blockchain is a digital ledger created to capture transactions conducted among various parties in a network. It is a peer-to-peer, Internet-based distributed ledger which includes all transactions since its creation. All participants (i.e., individuals or businesses) using the shared database are “nodes” connected to the blockchain, each maintaining an identical copy of the ledger. Every entry into a blockchain is a transaction that represents an exchange of value between participants (i.e., a digital asset that represents rights, obligations or ownership). In practice, many different types of blockchains are being developed and tested. However, most blockchains follow this general framework and approach. When one participant wants to send value to another, all the other nodes in the network communicate with each other using a pre-determined mechanism to check that the new transaction is valid. This mechanism is referred to as a consensus algorithm. Once a transaction has been accepted by the network, all copies of the ledger are updated with the new information. Multiple transactions are usually combined into a “block” that is added to the ledger. Each block contains information that refers back to previous blocks and thus all blocks in the chain link together in the distributed identical copies. Participating nodes can add new, time-stamped transactions, but participants cannot delete or alter the entries once they have been validated and accepted by the network. If a node modified a previous block, it would not synchronize with the rest of the network and would be excluded from the blockchain. A properly functioning blockchain is thus immutable despite lacking a central administrator.

How Blockchain works?



Blocks:

Every chain consists of multiple blocks and each block has three basic elements:

1. The **data** in the block.
2. A 32-bit whole number called a **nonce.** The nonce is randomly generated when a block is created, which then generates a block header hash.
3. The **hash** is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined**.**

Miners:

- Miners create new blocks on the chain through a process called mining.

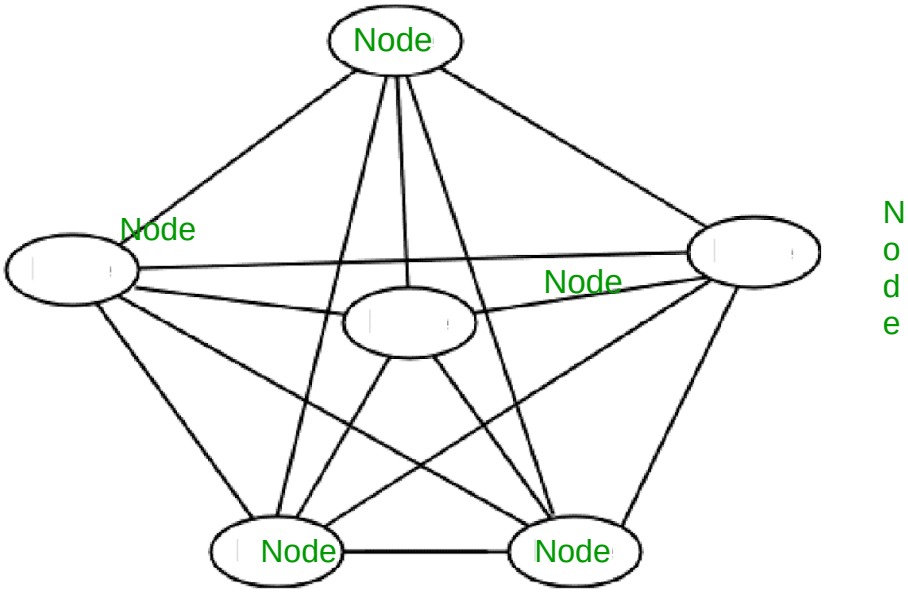
- In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block is not easy, especially on large chains.

- Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens, miners are said to have found the "golden nonce" and their block is added to the chain. Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all the blocks that come after. Therefore, it is extremely difficult to manipulate blockchain technology. Think of it as "safety in math" since finding golden nonces requires an enormous amount of time and computing power. When a block is successfully mined, the change is accepted by all the nodes on the network and the miner is rewarded financially.

Nodes:

- One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain. Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning.

- Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted, and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed. Each participant is given a unique alphanumeric identification number that shows their transactions. Combining public information with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users. Essentially, blockchains can be thought of as the scalability of trust via technology.


Node
Node
Node
Node
Node
Node

Evolution of Blockchain: -

1991-2008: Early Years of Blockchain Technology

- How did blockchain emerge? Stuart Haber and W. Scott Stornetta envisioned what many people have come to know as blockchain, in 1991. Their first work involved working on a cryptographically secured chain of blocks whereby no one could tamper with timestamps of documents.
- In 1992, they upgraded their system to incorporate Merkle trees that enhanced efficiency thereby enabling the collection of more documents on a single block. However, it is in 2008 that Blockchain History starts to gain relevance, thanks to the work one person or group by the name *Satoshi Nakamoto*.

- *Satoshi Nakamoto* is accredited as the brains behind blockchain technology. Very little is known about Nakamoto as people believe he could be a person or a group of people that worked on Bitcoin, the first application of the digital ledger technology.

- Nakamoto conceptualized the first blockchain in 2008 from where the technology has evolved and found its way into many applications beyond cryptocurrencies. Satoshi Nakamoto released the first whitepaper about the technology in 2009. In the whitepaper, he provided details of how the technology was well equipped to enhance digital trust given the decentralization aspect that meant nobody would ever be in control of anything.

Evolution of Blockchain:

Phase 1- Transactions

2008-2013: Blockchain 1.0: Bitcoin Emergence

- Most people believe that Bitcoin and Blockchain are the same thing. However, that is not the case, as one is the underlying technology that powers most applications of which one of them is cryptocurrencies.

- Bitcoin came into being in 2008 as the first application of Blockchain technology. Satoshi Nakamoto in his whitepaper detailed it as an electronic peer-to-peer system. Nakamoto formed the genesis block, from which other blocks were mined, interconnected resulting in one of the largest chains of blocks carrying different pieces of information and transactions.

- Ever since Bitcoin, an application of blockchain, hit the airwaves, several applications have cropped all of which seek to leverage the principles and capabilities of the digital ledger technology. Consequently, blockchain history contains a long list of applications that have come into being with the evolution of the technology.

Phase 2- Contracts

2013-2015: Blockchain 2.0: Ethereum Development

- In a world where innovation is the order of the day, Vitalik Buterin is among a growing list of developers who felt Bitcoin had not yet reached there, when it came to leveraging the full capabilities of blockchain technology, as one of the first contributors to the Bitcoin codebase.

- Concerned by Bitcoin's limitations, Buterin started working on what he felt would be a malleable blockchain that can perform various functions in addition to being a peer-to-peer network. Ethereum was born out as a new public blockchain in 2013 with added functionalities compared to Bitcoin, a development that has turned out to be a pivotal moment in Blockchain history.

- Buterin differentiated Ethereum from Bitcoin Blockchain by enabling a function that allows people to record other assets such as slogans as well as contracts. The new feature expanded Ethereum functionalities from being a cryptocurrency to being a platform for developing decentralized applications as well.

- Officially launched in 2015, Ethereum blockchain has evolved to become one of the biggest applications of blockchain technology given its ability to support smart contracts used to

perform various functions. Ethereum blockchain platform has also succeeded in gathering an active developer community that has seen it establish a true ecosystem.

- Ethereum blockchain processes the greatest number of daily transactions thanks to its ability to support smart contracts and decentralized applications. Its market cap has also increased significantly in the cryptocurrency space.

Phase 3- Applications

2018: Blockchain 3.0: the Future

- Blockchain History and evolution does not stop with Ethereum and Bitcoin. In recent years, several projects have cropped up all leveraging blockchain technology capabilities. New projects have sought to address some of the deficiencies of Bitcoin and Ethereum in addition to coming up with new features leveraging blockchain capabilities.

- Some of the new blockchain applications include NEO, billed as the first open-source, decentralized, and blockchain platform launched in China. Even though the country has banned cryptocurrencies, it remains active when it comes to blockchain innovations. NEO casts itself as the Chinese Ethereum having already received the backing of Alibaba CEO Jack Ma as it plots to have the same impact as Baidu in the country.

- In the race to accelerate the development of the Internet of Things, some developers, so it fit, to leverage blockchain technology and in the process came up with IOTA. The cryptocurrency platform is optimized for the Internet of things ecosystem as it strives to provide zero transaction fees as well as unique verification processes. It also addresses some of the scalability issues associated with Blockchain 1.0 Bitcoin.

- In addition to IOTA and NEO, other second-generation blockchain platforms are also having a ripple effect in the sector. Monero Zcash and Dash blockchains came into being as a way of addressing some of the security and scalability issues associated with the early blockchain applications. Dubbed as privacy Altcoins, the three blockchain platform seek to provide high levels of privacy and security when it comes to transactions.

- The blockchain history discussed above involves public blockchain networks, whereby anyone can access the contents of a network. However, with the evolution of technology, several companies have started adopting the technology internally as a way of enhancing operational efficiency.

- Large enterprises are investing big in hiring professionals as they seek to gain a head start on the use of technology. Companies like Microsoft and Microsoft appear to have taken the lead when

it comes to exploring blockchain technology applications resulting in what has come to be known as private, hybrid, and federated blockchains.

2015: Hyperledger

- In 2015, the Linux Foundation unveiled an Umbrella project of open-source blockchain. They went on to call it Hyperledger, which until to date acts as collaborative development of distributed ledgers. Under the leadership of Brian Behlendorf, Hyperledger seeks to advance cross-industry collaboration for the development of blockchain and distributed ledgers.

- Hyperledger focuses on encouraging the use of blockchain technology to improve the performance and reliability of current systems to support global business transactions.

2017: EOS.IO

- EOS brainchild of private company block.one came into being in 2017, on the publishing of a white paper detailing a new blockchain protocol powered by an EOS as the native cryptocurrency. Unlike other blockchain protocols, EOS tries to emulate attributes of real computers including CPU and GPU.

- For that reason, EOS.IO doubles up as a smart contract platform as well as a decentralized operating system. Its main purpose is to encourage the deployment of decentralized applications through an autonomous decentralized corporation.

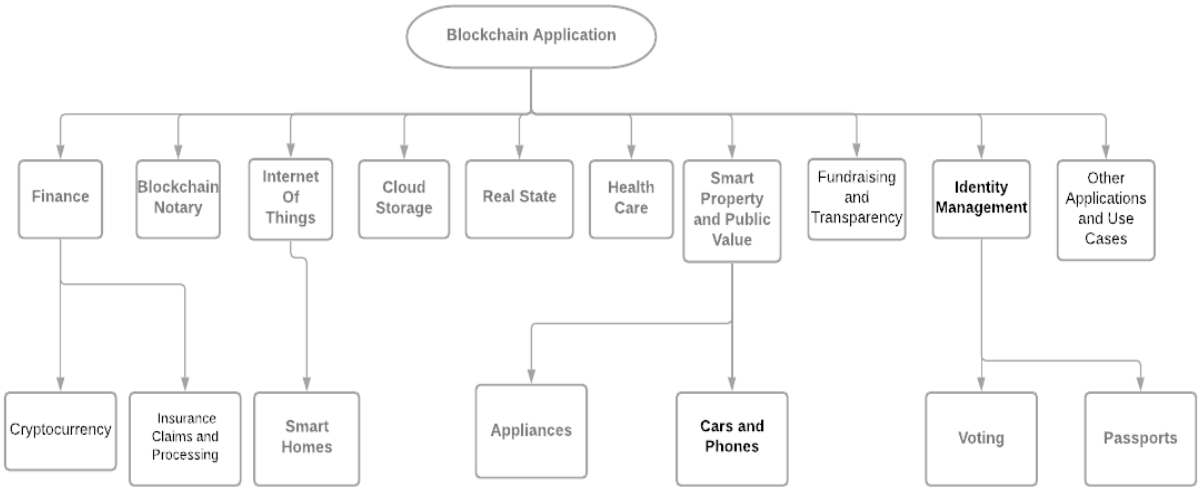
2020: Blockchain History & The Future

- The future of Blockchain technology looks bright, in part, because of the way governments and enterprises are investing big as they seek to spur innovations and applications. It is becoming increasingly clear that one day there will be a public blockchain that anyone can use.

- Advocates expect the technology to help in the automation of most tasks handled by professionals in all sectors. The technology is already finding great use in supply management as well as in the cloud computing business. The technology should also find its way into basic items such as search engines on the internet in the future.

- As the technology evolves, Gartner Trend Insights expects at least one business built on blockchain to come into being valued at more than $10 billion by 2022. Due to the Blockchain Digital Transformation, the research firm expects the business value to grow to over $176 billion by 2025 and exceed the $3.1 trillion by 2030.

Applications of Blockchain



- After successful implementation of Blockchain in Bitcoin because of its salient features, Blockchain has been proposed to be used in different applications and use cases. We present a brief overview of each domain in the following section.

1. Finance:

- Conventionally, an intermediary such as a bank, verifies and processes the financial transactions. Having such a centralized system puts immense work in the hand of intermediaries, meanwhile the transactions are prone to errors as multiple uncoordinated parties are required to keep the record and adjust them. Thus, the entire process is time-consuming and costly. The Blockchain simplifies such complications associated with financial services by introducing a distributed public ledger, where the transactions are verified by the miners using “proof-of-work.”

1.1 Cryptocurrency:

- Cryptocurrency, which holds a market cap in the billions of dollars, has been possible with the help of Blockchain. Specifically, the bitcoin, proposed by a programmer known as Satoshi Nakamoto, is based on cryptographic techniques that allows the recipient to receive money securely/genuinely without requiring a trusted third party, such as a bank or a company like PayPal. The Bitcoin network relies on a Blockchain—a distributed transaction public ledger—where a new block is generated by executing a consensus algorithm such as Proof-of-Work. It has been noted that it is practically impossible to get someone's private key from his/her public key which prevents users from impersonating attacks.

1.2 Insurance Claims and Processing:

- Insurance claim has been dealing with several fraudulent claims. Moreover, there must be updated policies and data associated with each claim to properly process an insurance claim which is difficult to handle in traditional approaches. With Blockchain technology, the process can be handled through Blockchain (distributed ledger technology) efficiently in a secure manner. Similarly, any fraudulent claims/transactions can be detected and dropped with a good confidence as multiple participants/miners need to agree on the validity of each transaction. This makes sure the insurers settle their claim which they deserve quickly and effectively.

2. Blockchain Notary:

- Blockchain using distributed ledger technology with cryptography replaces trusted third parties such as a notary. Blockchain helps the entire notary process by automatically executing processes in a cost-effective, transparent, and secure manner.

3. Internet of Things (IoT):

- With the massive number of devices interlinked to each other creates the Internet-of-Things (IoT). The IoT is expected to transform the way of lives where ideas like smart homes are feasible. While this new phenomenon is likely to make lives easier, having a massive number of heterogeneous devices connected to the Internet creates grave issues regarding cyber security and privacy. The Blockchain can be an important technology to secure IoT.

3.1 Smart Homes:

- Blockchain in the context of smart homes with IoT devices can help to have secure and reliable operations for smart home operations. However, implementation of Blockchain in such resource constrained IoT systems is not straightforward because of high resource demand required for proof-of-work, limited storage capacity, low latency, and low scalability.

4. Cloud Storage and Provenance:

- Metadata that records the history of the creation and all operations including file/data accessing activities can be kept in the Blockchain which can then be shared with all stakeholders. Data provenance through Blockchain is important for applications like accountability and forensics. For instance, when different users access and make changes in the collaborative documents such as files shared through Google document, users could make changes and those changes are stored in the blockchain.

5. Real Estate:

Blockchain technology as a distributed ledger database system can offer benefits for the real estate industry. Property title recording can be done using blocks with transactions in Blockchain rather than using traditional/current record keeping systems.

6. Health-Care:

- Personal health records are sensitive information and needs to be dealt with high security. Such personal records can be encoded and stored using Blockchain and provide a private key which

would allow only specific individuals to access the records. Similarly, the same protocol can be applied to conduct research where personal records are used via Health Insurance Portability and Accountability Act (HIPAA) laws to ensure confidentiality of the data.

7. Smart Property and Public Value:

All entities/property such as house, land, automobiles, stocks, etc. can be represented in the ledger technology and Blockchain can be used to keep the track of all operations and property records. Once the records are kept in the Blockchain they are shared with all the concerned or participating parties which can easily be used to establish contracts and verify them.

7.1 Cars and Phones:

Personal devices such as phones are protected using authentication keys. Similarly, cars are only accessible to the owners using smart keys. This kind of technology is possible with cryptography, and yet, such methods can fail if the authentication key is stolen or copied or transferred. Such issues can be fixed in the Blockchain ledger where users/miners can replace and replicate lost credentials.

7.2 Appliances:

Smart appliances are essentially electronic devices aided by a cyber system such that the cyber portion can communicate information regarding the environment around the device and the device itself. It is essentially about the idea of a "talking toaster" where a toaster can give its user information relevant to its usage. A home connected with smart appliances can be considered a smart home.

8. Fundraising and Transparency:

Transparency is one of the issues to be addressed in fund-raising activities to make the process trustworthy. Blockchain as a distributed ledger technology can ensure transparency, security, and integrity in fund-raising activities by leveraging Blockchain features such as immutability, verifiability, and security.

9. Identity Management:

In this section, we present a brief overview of different identity management-based applications and how they could benefit from Blockchain technology.

9.1 Voting:

Blockchain could offer many tangible benefits for verifiable secure voting systems in coming years. Current voting system has flaws and it is hard to verify votes. Thus, Blockchain with its features could provide an immutable, verifiable, and secure voting system where voter can cast their votes with highest confidence from anywhere in the world.

9.2 Passports:

The first digital passport was launched in 2014 which could help the owners to identify themselves online and offline. With this Blockchain technology, a user can take a picture and

share it via cryptographic communication, which can be used to share the picture and verify among the users via digital signatures.

10. Other Applications and Use Cases:

Blockchain technology can be used in any scenarios when a trusted third-party is not needed or a peer-to-peer system is needed for managing the transactions, with features like transparency, decentralization, integrity, immutability, security, and privacy. However, Blockchain has some limitations such as high delay introduced by consensus process, large size of the blocks in Blockchain, etc.

Advantages of the Blockchain

The Blockchain technology is decentralized system and it is the main benefit of this technology. Why it is important for our life? The answer to this question is very simple – it is not necessary to work with the third-party organization or with the central administrator. It means that the system works without intermediary and all participants of this Blockchain make the decisions. Each system has the database and it is important to protect this database, because when system is working with the third-party organizations, there is a hacking risk of the database or the data may turn up in the wrong hands. The process of the database security might take a lot of time and might spend a lot of money. If use the Blockchain technology can be avoided, because the transactions of the Blockchain have own proof of validity and authorization to enforce the constraints. Means that the transactions can be verified and processed independently

Disadvantages of Blockchain

If the Blockchain has advantages, this technology has disadvantages or challenges. The main disadvantage of the Blockchain is the high energy consumption. The consumption of power is needed for keeping a real-time ledger. Every time the new node is created and in the same time it communicates with each and every other node. In this way transparency is created. The network's miners are attempting to solve a lot of solutions per seconds in efforts to validate transactions. They are using substantial amounts of computer power. Every node is giving extreme levels of fault tolerance, ensures zero downtime and is making data stored on the Blockchain is forever unchangeable and censorship-resistant.

CONCLUSION

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 and Intel are all working to become early adopters of blockchain.Nearly $400 trillion across various industries is set to be transformed by blockchain.

REFERENCES

https://builtin.com/blockchain

https://101blockchains.com/history-of-blockchain-timeline/

https://lucid.app/lucidchart/f1d64650-adba-4cbc-9471-71e434054a87/edit?beaconFlowId=1F956F3203FF40E7&invitationId=inv_1ebff795-2f8a-4e46-8f2a-501752fd2680&page=0_0#

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwijq_vwhcXzAhU44zgGHZVIB0sQFnoECBkQAQ&url=https%3A%2F%2Fwww.stm-assoc.org%2F2017_04_27_Annual_Conference_Peck_What_is_Bitcoin.pdf&usg=AOvVaw0WjQeHouJiFV1tjAHt6bFK

https://www.researchgate.net/publication/330028734_The_Advantages_and_Disadvantages_of_the_Blockchain_Technology

https://link.springer.com/chapter/10.1007/978-3-030-27798-7_15

https://www.investopedia.com/terms/b/blockchain.asp

https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain