Blockchain and its Applications

Manbir Singh
Information Systems Security
Concordia University,
Montreal, Canada
manbir.singh@mail.concordia.ca

Jaskaran Singh
Information Systems Security
Concordia University,
Montreal, Canada
singhjaskaran7171@gmail.com

Jagmandeep Singh
Information Systems Security
Concordia University,
Montreal, Canada
Jagmandeepsingh756@gmail.com

Ashish Singh
Information Systems Security
Concordia University,
Montreal, Canada
ashish.singh@mail.concordia.ca

Money Saxena
Information Systems Security
Concordia University,
Montreal, Canada
moneysaxena5@gmail.com

Gurpreet Kaur
Information Systems Security
Concordia University,
Montreal, Canada
2812gurpreetkaur@gmail.com

Tanmya Rampal
Information Systems Security
Concordia University,
Montreal, Canada
Tanmyar@gmail.com

***Abstract*—Blockchain technology has become an innovative idea for electronic commerce and record-keeping. It has many uses in many different sectors and is a decentralized, safe, and transparent method of storing and transferring information. We have Analyze various software or projects which use bitcoin as underling technology.**

Keywords—Blockchain , Bitcoin , NFT , Medical records, BE vote, My vote, dApps, Lightning Network, OpenBazaar, Counterparty

I. INTRODUCTION

Blockchain has been one of revolutionary technology with wide range of application. Bitcoin, a digital currency that uses blockchain technology to record transactions and keep track of ownership, is one of the most well-known blockchain applications. Blockchain technology is also being used in voting systems, where it has the ability to increase the reliability and openness of the voting process. Blockchain technology is used by non-fungible tokens (NFTs), a class of digital asset, to guarantee the exclusive possession and authenticity of digital goods like music, artwork, and other collectibles. A secure and transparent method of storing and sharing patient data is provided by medical blockchain systems, allowing for improved provider cooperation and better patient outcomes.

By providing a decentralized, secure, and transparent method of storing and transferring information, blockchain technology has the potential to revolutionise a number of different sectors. This technology will probably have a big effect on how we vote, own and trade digital assets, conduct transactions, manage healthcare data, and own and trade digital assets in the future.[1]

II. HOW BLOCKCHAIN WORKS

Blockchain is a distributed ledger that is completely open to anyone. Once some data is recorded inside a blockchain, it becomes very difficult to alter it. Each block contains some data, the hash of the block, and the hash of the previous block. The data present inside a block depends upon the type of blockchain. The Bitcoin blockchain for instance stores the details about a transaction that is the details of the sender, receiver, and the number of bitcoins involved in the transaction. The hash of the block is unique, just like fingerprints. The hash is calculated once a block is created. If any changes in the block are there, the hash is also changed. These hashes are also used in the detection of any changes in the block.

Blockchain works as a distributed database for the transaction of records that are checked and updated by a network of computers. The records are managed by a broad community unlike a single unit in power which means not one single person has power over it. Transaction history can never be edited or erased. The distributed property of blockchain makes it difficult for an entity to alter. Blockchain access to everyone else's entries on the network makes it difficult for one central body to take control of the network. The transaction is checked after it is sent to the network of computers. The authenticity or originality of the transaction is checked during this phase. After verifying the originality, this transaction is connected to its preceding transaction creating a whole new transaction chain which is called blockchain

Blockchain ArchitectureDecentralization is the main characteristic of Blockchain technology. The databases are connected in a distributed manner and the copy of the databases are the same.

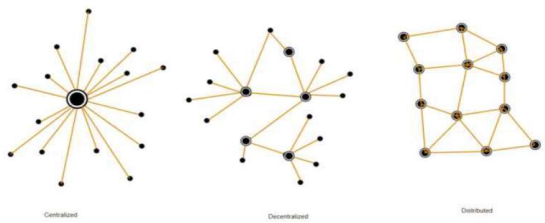

Fig Ways of managing data [1]

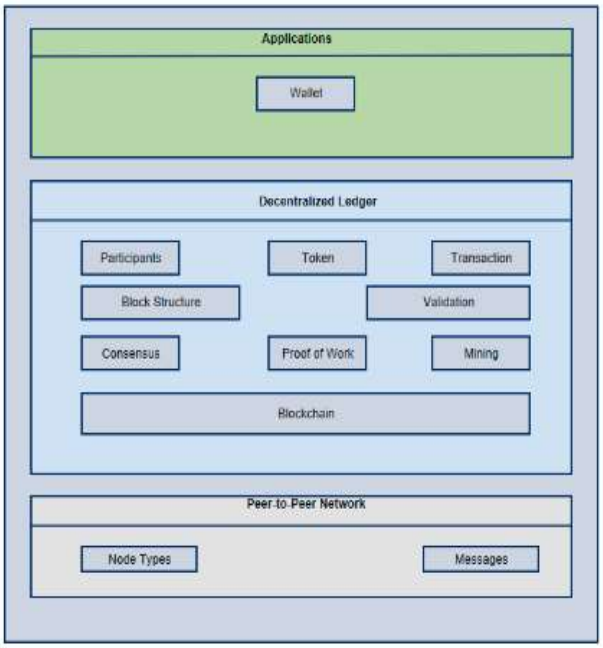

Fig Architecture of Blockchain [1]

Blockchain manages its data in a decentralized manner, making it secure over various computer networks, unlike other technologies that maintain their data in a centralized manner that does not offer security. The architecture of blockchain comprises three parts-

- Applications
- Digital Ledger
- Peer to Peer network.

The application layer in blockchain runs decentralized applications. It is the outermost layer in the blockchain architecture. These decentralized applications are used by the end-users to interact with the blockchain network.

The Decentralized ledger is responsible for storing all the transactions. This ledger is controlled and maintained by multiple computers, unlike a centralized ledger in which a single entity controls everything. The communication between the two entities is put inside the block that is secured using various cryptographic algorithms.

Peer-to-Peer network (or P2P network) works on the principle of decentralization. A P2P network allows an uninterrupted exchange of information between two entities. In this network, all the nodes are allowed to freely transfer bitcoins without any third party involved.
So, the above three components complete the architecture of blockchain.

A. Blockchain working

The following diagram the working of blockchain – How a transaction is added to the chain of transactions.

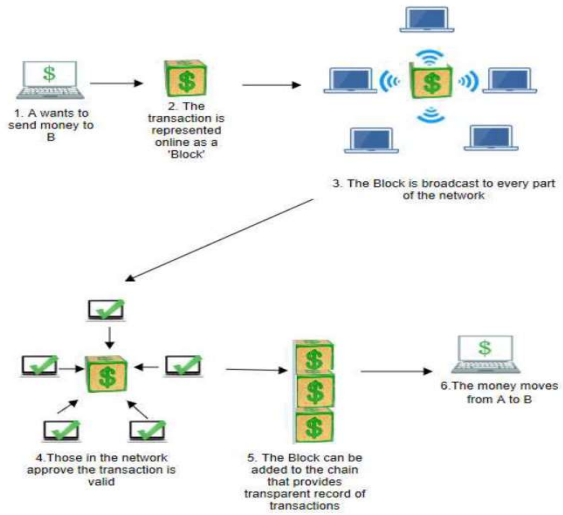

Fig Working of blockchain[1]

B. Tiers of Blockchain

The tiers of blockchain are explained as follows.
c.1 Blockchain 1.0: This blockchain is used for managing and controlling the transaction of cryptocurrencies which means bitcoins are traded and mined under this blockchain.

c.2 Blockchain 2.0: All finance-related services and organizations implement this blockchain to manage their finances, bonds, swamps, etc.

c.3 Blockchain 3.0: This blockchain is regarded as the most efficient blockchain offering higher security than blockchains 1.0 and 2.0. It also provides good scalability and is also adjustable.

c.4 Generation X: This allows everybody to use the blockchain service as it follows the concept of singularity. This blockchain will be accessible to everyone and run by autonomous agents. [2]

III. HOW BLOCKCHAIN IS USED FOR BITCOIN

The blockchain of Bitcoin is basically “a distributed ledger that records all transactions made within the Bitcoin network”. Each deal has one or more characteristics.
Transaction outputs (the operations that resulted in the user receiving Bitcoins) and transaction inputs (users to send the Bitcoins to). The current owner of a bitcoin transfers ownership by approving a transaction from the inputs to one or more new owners chosen by the outputs. The coins are then transferred to the following person by the new owner by repeating this procedure.
Thus, it is possible to think of bitcoins as a series of digital signatures, whose authenticity and ownership can be checked at each stage by navigating the public ledger and tracing the coin's creation.[3]

A. Verification

After the coin's owner broadcasts their transaction into the peer-to-peer network, it must go through a procedure called "mining" to be verified and is validitated.

A section of the public ledger. blocks of transaction are made for efficiency's reasons and verification, hence the term

blockchain. The process of validation of transaction is then carried out by miners that use their computing capacity to crack a cryptographic puzzle. This mechanism serves as "proof of work." This is done in Bitcoin by locating a hash value which is made by SHA256, produces a hash that starts with a specific amount of zero bits.

The system decides how many zero bits are needed, and it self-adjusts because the complexity of the puzzle increases exponentially with the quantity of zero bits needed. This guarantees that the average proof of work time for a block is 10 minutes, regardless of changes in the number of mining nodes and the miners' increasing processing capacity as hardware improves over time..

The process of verification is competitive because miner who solve the problem first is given mining reward for correctly solving to problem . To prevent double spending, The network's other nodes will only accept a block if the deals are valid and the inputs have not already been used.. The remaining nodes in the network signal their acceptance of the broadcasted block by giving up on trying to solve the proof-of-work issue for the current block in favour of constructing the chain's subsequent block.[3]

The proof of work mechanism is built in such a way that nodes with more resources have a better chance of solving the problem first. The longest chain in the network, that utilizes the highest resource expenditure by proof-of-work, represents consensus on the authenticity and balance of the blockchain..

B. Incentive for mining bitcoin

Currently, 25 Bitcoins are given to the miner of an approved block. This is the only method to create new Bitcoins and acts as a motivator for people to mine blocks.
Contrast this with a centralized strategy, where a central authority can issue currency to be circulated.
The incentive system is also intended to lessen the likelihood of blockchain assaults. Blockchain is virtually immutable by design, preventing forgery.

To change the contents of a previous block, an attacker has to recreate the proof of work for the specific block as well as all subsequent blocks up to the present block.. Attackers who possess such computing power are encouraged by the incentive system to mine Bitcoin legally instead. The incentive system is also intended to lessen the likelihood of blockchain assaults. Blockchain is virtually immutable by design, preventing forgery.[4]

C. Decenterlation and double spend problem

The verification procedure prevents Bitcoin owners from trying to send same coin for different transaction. The remaining nodes in the network will reject a node's proof of work puzzle if it is completed a coin that has already been expended is included in the block.. As a result, the blockchain will not be updated.

However, for this to work, a significant portion of nodes must be trustworthy, which is supported by the incentive mechanism mentioned above. Additionally, the decentralised nature of Bitcoin produces a dependable system without a single point of failure, unlike a system with a central authority that acts as the system's supervisor. Finally, due to its transparency, coins can be tracked back to their original creation and the authenticity of a coin can be determined through visual examination.

D. Scalabilty of bitcoin block chain

Blocks can only contain 1Mb of transaction and header data, which is the subject of much debate at the moment. As blocks must be mined every 10 minutes, there is a potential cap of 7 transactions per second (TPS). This limit became a serious issue as Blockchain gained popularity and The quantity of transactions increased as more nodes joined the network.. A backlog of transactions could be created if the creation rate of transactions exceeds that at which they are added to the database.[5]

A number of solutions have been put forth to address this (such as raising the block size limit), but nothing has yet been put into practise because the community cannot presently agree on the best course of action.

IV. Application of Blockchain

A. Voting protocols based on Bitcoin- BEvote

One of the promising applications of blockchain technology is to support electronic voting (E-voting) in extensive-scale distributed decision control systems centered on mobile terminal devices (MTDs). The motivation behind the use of Blockchain technology in E-voting and the challenges involved is ensuring ballot secrecy and voter identity privacy as blockchain technology can help address these challenges by offering transparency, traceability, and verifiability of voting results. By utilizing blockchain technology, the traceability of transactions can increase the feasibility of voting results verification, transaction transparency can provide the open-audit capability, the tamper-resistance of blockchain can enhance the confidence of voters, and the pay-per-use feature of blockchain can incentivize organizers to organize voting services. There are potential benefits of using blockchain technology to support E-voting in various applications, such as medical intelligent diagnosis systems and property management. [6]

Blockchain technology’s biggest player Bitcoin's success is attributed to its online trading platform, which makes moving conventional voting to the Bitcoin platform a logical and feasible choice that can reduce costs. However, the two main challenges in implementing Bitcoin-enabled E-voting are anonymity and robustness. The solution to these challenges is a more secure Bitcoin-based E-voting application is BEvote. To achieve anonymity, before voting the system uses coin mixing techniques to separate a voter's genuine identity from their Bitcoin address, and this unspecified address is used throughout the voting process. To ensure robustness, the system adopts an E-voting protocol based on secret sharing that securely distributes voting rights and prevents voting numbers from being leaked.

1. Voting Scheme based on Bitcoin.

To facilitate the design of BEvote, we rely on certain assumptions that can be met through existing blockchain technologies and research. These assumptions include:

- A fixed block generation interval without forks
- Publicly auditable data on the blockchain, where the transaction history is readable, but only authorized

transactions can be written upon obtaining consensus.

- The consensus mechanism of the blockchain technology's proof-of-work cannot be destroyed by adversaries, ensuring the data's tamper-resistant nature.

a. System Model

Although the Bitcoin blockchain offers exchange anonymity, attackers can still use straightforward evaluation technology to probe all transactions documented in the chain nodes to reveal transaction parties' true identities. Coin mixing, which obscures the ownership of Bitcoin to disrupt the interlinkage of parties involved in a transaction, becomes a natural choice to ensure the anonymity of e-voting. Traditional coin mixing usually engages middlemen, allowing them to merge several transactions into one, substantially affecting its scalability. A scalable coin-mixing method divides the trading scheme into transferring and paying stages, improving the size of anonymous sets and execution efficiency.

Based on this, a coin-mixing three-tiered system model is formulated for Bitcoin-enabled e-voting. The Supervisor, Voter, Candidate, and Mixers are the system roles involved. The Supervisor validates each participant's qualifications and maintains member lists for each role. The Voter can spawn ballots and vote for preferred candidates. The Candidate is considered to be the one voting in the process. Mixers provide features for masking voter identities. Bitcoin blockchain is used for storage of data, recording all information describing the process of voting anonymously and tamper resistant. The workflow of BEvote involves registering, confusing voters' identities, generating ballots, voting, and counting.[6]

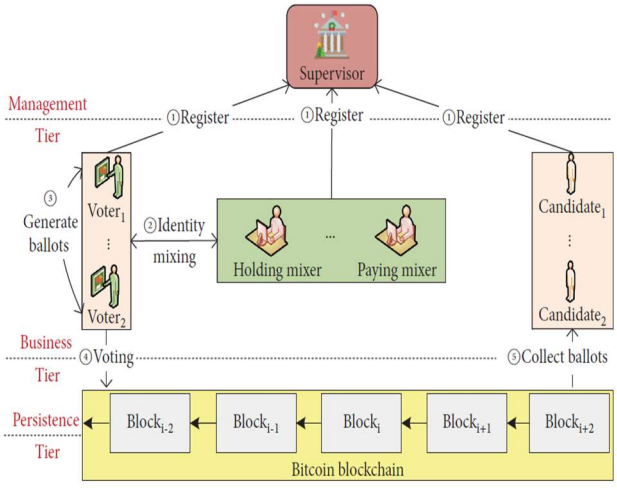

Fig- System Model

b. Confusion Strategy for voter's identity

This strategy is crucial for maintaining privacy when conducting Bitcoin transactions, using a process called coin mixing. The original coin mixing process can expose the identity of the person making the transaction if any of the mixers collude with adversaries. To address this vulnerability, a group blind signature was introduced which uses its unlikability feature to cut off the interaction between mixers. The process involves registering for a mixing service, receiving recommendations for two mixers, constructing a transaction to transfer Bitcoins starting from originating address to a hosting mixer's escrow address, receiving a voucher from the hosting mixer, forwarding the voucher for payment to the mixer to make a new transaction to transfer the Bitcoins to an anonymous address, and having the supervisor transfer the Bitcoins to the original paying mixer.

This process involves sending several messages to the hosting mixer and the paying mixer with deadline times for various steps in the process which involves blind SKLOGLOG and SKROOTLOG protocols to ensure privacy.

c. Construction Strategy for Voting Transaction

The voting transaction in the Bitcoin platform uses the script method, which allows numerous input and output scripts. In BEvote, a combination of P2PKH and M-N combined P2SH scripts are used. P2PKH includes the Check Lock Time Verify operator, while the M-N combined P2SH script stores the single or many signatures for the public key. The input script needs to include serialized redeem script and all private keys, and at least a specified number of public keys must have corresponding signatures.[6]

B. NFT

Non-Fungible Tokens (NFTs) are digital assets that can be used to represent digital and physical creative work. Each token is unique and cannot be exchanged with another, making them non-fungible. NFTs contain digital information like music, video, and images and their value can be determined in cryptocurrencies. Although NFTs are a part of Ethereum's blockchain unlike Ethereum coins as they can still be exchanged amongst other assets making them fungible. With technological advancements and growth come increased security risks related to authenticity as well.[7]

NFTs enable the uniqueness and non-fungibility of each asset, making it possible to trace each back to its owner. This eliminates the issue of customers being duped into buying counterfeit goods like tickets or artwork. Items can be traced easily by buyers back to their legal owners, providing peace of mind that their purchase was legal. NFTs have opened new markets for artists businesses which had previously struggled to establish online marketplaces in today's internet-based economy.

NFTs gained notoriety with the October 2017 launch of CryptoPunks and the subsequent record-breaking sale of Mike Winkelmann's art for almost USD 70 million. Since then, NFTs have seen steady growth, with artists and collectors taking notice. From being a niche within blockchain communities to having global sales reaching up to USD 1.2 billion by July 2021, their market has expanded significantly.[9]

Another exciting blockchain-based technology is the Metaverse, which enables people to interact with virtual avatars in a simulated world. This study will identify new uses of Non-Fungible Tokens (NFTs) within this virtual

environment, particularly how NFTs can assist with ownership rights management and identity management within it. This report provides an in-depth explanation of these NFT applications in Metaverse.

The key contributions of the study are summarized below:

1. We discuss the exponential growth of NFTs in usage and deployment since its creation.
2. We explore the numerous applications of NFT that exist across various domains.

We present the challenges of NFTs in the current technologies and legal atmosphere.

C. Non-Fungible Tokens (NFT) – A Primer

This section provides an overview of NFTs, the technologies associated with it, and some insight into how NFT marketplaces are developing.

A. Blockchain

Blockchain is a decentralized digital ledger that can be accessed by multiple computers without the need for a central authority to operate. Blockchain technology was pioneered by Bitcoin in 2009, and other industries have since adopted it for various uses. Financial services have been particularly drawn to blockchain due to their difficulty in tracing asset ownership, making them prime candidates for the adoption of this ground-breaking technique. Blockchain works by building a digital ledger from data packages known as "blocks." These blocks can be cryptographically interconnected to form complete digital ledgers when more are added.

Unique hash values are used to detect fraudulent modifications of blocks. This technology safeguards the confidentiality and integrity of blockchain transactions. Blockchain's decentralized structure permits transparent viewing of all transactions. This technology has potential applications in finance and security, as well as IoT and smart contracts.[7]

The following are the primary properties of NFTs:

1. Uniqueness: NFTs can exist as digital or physical entities and possess unique properties.
2. Immutability: This characteristic relies on blockchain security to guarantee that no person has the power to alter, delete or erase recorded data.
3. Non-interchangeability: NFTs cannot be substituted for another item even if there is high degree of similarity between them, as demonstrated by their designation "NFT".

B. NFT Marketplace (Buying and selling NFTs)

NFTs are digital assets created and issued as tokens within seconds. This works similarly to how coins made of metal are struck and then circulated. With NFTs, digital art can be represented as an NFT, traded on the market, and its ownership tracked throughout every step of production. NFT sales experienced a meteoric rise in the second quarter of 2020 when an NFT artwork sold for USD 69 million. Overall, 2020 NFT sales totalled USD 2.5 billion - an indication of rapid expansion - and this number increased substantially during the first six months of 2021 to USD 10 billion. NFT trading volume stands at $4 billion while the entire cryptocurrency market trades at USD 341 billion. Many online platforms allow people to buy or sell NFTs; however, some are more popular than others.[11]

Table I. Top NFT Marketplaces

Rank	NFT Marketplace	Market Share (%)
1	Blur	56.80%
2	OpenSea	36.70%
3	X2Y2	2.60%
4	Magic Eden	2.10%
5	LooksRare	1.00%
6	CryptoPunks	0.80%

NFT Applications

a. Digital Art

Digital art refers to creative content created in digital or virtual mediums such as music and films, paintings, and images, etc. Artists, collectors, and enthusiasts buy and sell it; however, it remains vulnerable to theft and counterfeiting. Digital art utilizes NFTs to generate a unique hash that sets each piece apart from others. Additionally, these digital tokens can be signed by artists in order to validate their authenticity.

b. Licenses And Certifications

NFTs are an efficient way for companies to verify important documentation, ultimately improving administrative operations. NFTs verify authenticity while relieving the institutes issuing licenses and certificates with less effort. Blockchain-based issuance makes these documents more resistant to tampering which reduces the chance of fraudulent documents being discovered.

c. Boosting Gaming Potential

NFTs have many benefits for gamers and game developers, including providing ownership data for in-game objects, facilitating economic systems within games, and more. Players have the choice to purchase items or objects for their inventory but also have the option to sell them once no longer needed. Players may make money if an item's price increases over time. Ultimately, both developers and gamers benefit from this mutually beneficial process. Developers earn a royalty each time an NFT hits the market, creating a win-win business model in which both sides reap benefits from using intermediaries like NFT markets.

d. Sports

NFTs have become a must-have in the sports industry. Within a short time, boxing, basketball and baseball had become three of the top sports with expensive NFTs - released by Golden State Warriors - who became America's first American sports team. NFTs enable complete transparency; for example, an NBA card can now be digitally tracked via ranking system to determine its value. Moreover, NFTs provide fans with new ways to connect with their team while also generating revenue. *[13]*

D. Metaverse

Overview

Metaverse refers to a digital world powered by virtual reality technology. It allows individuals to engage with other users and computer-generated environments. Crypto metaverses offer immense potential and their blockchain architecture makes it possible to trade virtual items for real economic value. Mark Zuckerberg's announcement of Facebook Meta reignited enthusiasm for the metaverse and its value reached high records in November 2021. Although Zuckerberg's announcement may have spurred investors' interest in these virtual world initiatives, Microsoft also contributed by hosting an ignite event that showcased their metaverse technology.[18]

1.Applications of NFTs in the Metaverse

This section of the study investigates how NFTs can be applied to the Metaverse and propose new use cases.

Identity (Related to Virtual Person): Identity is used in the Metaverse for authentication and must be unique and resistant to fraudulence. These aspects are essential if NFTs are going to serve as identities in this space:

- Avatars (visual identification): Profile photos require avatars to stand out among thousands of others in order to be recognized in the Metaverse. NFTs give these objects the uniqueness that makes them so desirable.
- Identity (e.g., name): Every entity in the Metaverse, including users and objects, requires a unique identifier. The Metaverse allows users to link their real identities with their NFT-based identities for identity management, access control, and monitoring purposes.
- Certificate: Metaverse Certificates can be issued to prove ownership and validity. Creating NFT-based certificates for virtual people by Metaverse-based agencies/colleges/academies could make Metaverse-based courses and training more popular.
- Membership: Metaverse-based communities can be formed by connecting NFTs to users' real identities. You have full control over NFTs within these societies, groups, and gatherings in Metaverse instead of having to deal with virtual people.[9]

2. Digital Asset (Related Metaverse-based Assets) –

It is critical to protect and represent digital assets that exist only within the Metaverse, without a physical twin. In order to guarantee security and ownership of these digital assets, they should be linked with NFTs:

- Digital Items: In order to assign any digital item in Metaverse to a virtual group or person, an assignation mechanism must be put in place. This enables the creation of virtual people within a Metaverse while also guaranteeing ownership and security for each digital thing within Metaverse. This requirement can be fulfilled by releasing NFTs (Network Function Tokens) onto each digital thing in Metaverse.
- Metaverse Land: This trend has drawn the attention of many. NFTs are land documents that can be used to prove ownership, transfer property ownership, and more.
- Virtual Certificates: Metaverse-based certificates serve to demonstrate the skillsets and accomplishments of virtual individuals or their completion of virtual courses. NFTs provide the most reliable options for creating these types of certificates.
- Transferring Ownership: Digital assets should be transferable, just like in the real world. NFTs play a vital role in providing proofs of ownership for digital documents.

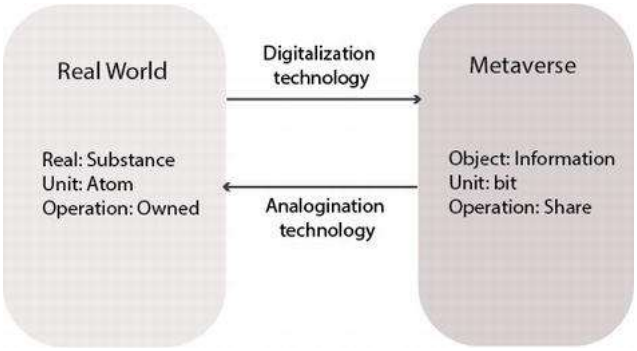

Fig III. Metaverse[9]

A. Blockchain in Healthcare System

Blockchain, a generally unused decentralization instrument, gives vigorous arrangements for security and productivity challenges existing in healthcare frameworks. The thought of applying a blockchain in healthcare spaces could be a result of the need for security and interoperability in healthcare. Points of interest of utilizing Blockchain innovation within the healthcare industry incorporate decentralized and permanent records adjustment of records, secure data, modification, addition, and deletion of data Many organizations are using traditional methods and third party tools in preserving and securing electronics healthcare records, in which they are lacking transparency.

Due to which electronics healthcare records face major trust, privacy and security issues. To overcome these security issues in healthcare businesses, blockchain innovation offers critical prospects. Blockchain may be a decentralized, and

conveyed database which might connect numerous computers through hubs, and it requires no exchanges to construct a modern piece that makes a difference to send secure data from one individual to another, computers, clients, hospitals, etc. Any party or person who uses this technology to secure healthcare records can access the data remotely from anywhere with the help of blockchain secured by cryptography.

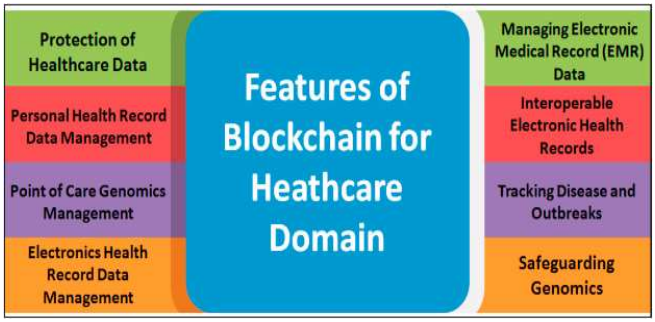

Fig-

a. Key features

Decentralization is a key feature of blockchain technology. The material that is added to the blockchain is not governed by a single entity; rather, each contribution employs a different consensus minimization procedure and accepts the terms of the peer-to-peer network.Blockchain uses the Merkle tree mechanism to maintain the integrity of the transactions. It serves to encode blockchain data more efficiently and securely. Security of information is the most key center of blockchain exchanges. As information is exchanged through blockchain without the association of any third parties, there's essentially no chance of information robbery or change. Blockchain technology in the healthcare sector mainly focuses on creating the safe and secure system to manage the data for the patient, and electronics health records.

b. Different type of blockchin for healthcare

Blockchain is of three types in the healthcare system namely, private, public, and consortium, which decides who can read, write, and access the data on the blockchain. In public blockchain anyone can modify, add, or delete the data from outside if they want, whereas in a consortium only specific group members can access the data and not anyone. With private, data can be access from the central location only and no one from outside this location has access to this data.

Blockchain Type\Properties	Private Blockchain	Consortium Blockchain	Public Blockchain
1 - Efficiency	High	Low	Low
2 - Determination of consensus	An organization	Chosen node set	All miners
3 - Constancy	Could be tampered	Could be tampered	Almost impossible
4 - Centralized	Yes	Partial	No
5 - Reading authorization	Public or restricted	Public or restricted	Public
6 - Process of Consensus	Approved	Approved	Permissionless

Table 1. Blockchain types and their properties.

c. Existing Blockchain and mechanism of Consensus

The foremost prevalent existing blockchains are Hyperledger and Ethereum in which designers can develop unused blockchain applications on top of current ones.. Entries of the data in blockchain is accepted through distributed ledgers with the help of distributed consent protocol. Three consensus methods Proof of work, proof of skate, and Byzantine are being used but they all have some advantages and disadvantages. Table below shows the comparison between these three consensuses methods.

Table 2. Comparison of consensus methods.

Possessions	PBFT	PoS	PoS
Management of nodes	Authorized	Accessible	Accessible
Adversarial tolerance	Faulty replicas less than 33.3%	Stake less than 51%	Computation power less than 25%
Expenditure of energy	Poor	Moderate	High
Instance	Hyperledger Fabric	Peercoin	Bitcoin

d. Blockchain potential in Healthcare

In the figure below, different healthcare operations are divided into sections to prevent form data from being edited and criticized for fiduciary activities. This way, the latest experience, technology and expertise will be provided, depending on the type of care the patient needs.. Additionally, collaboration with the educational organizations, students can also learn and develop necessary skills.

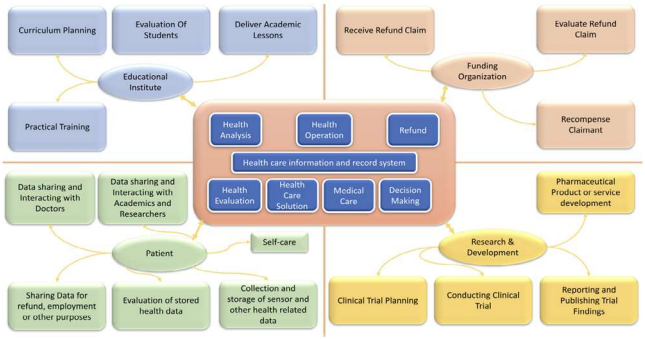

Fig-

e. Major areas of application of blockchain in healthcare system:

1. Health information management: It manages the healthcare data and how blockchain can be used in the pharmaceutical sector.
2. Healthcare Record Sharing: It shares the patient data and other personal information, but for sharing electronics healthcare records, blockchain should have many features.
3. Healthcare Image Sharing: It presents and share the image along with the healthcare records.
4. HealthCare System Log Management: Stores the logs to check any error analysis, intrusion detections and other services.
5. Supply Chain Management: This blockchain technology is very crucial, it is used in prescription and medical fraud as patient can be severely harmed if standard drugs are given and supplied.

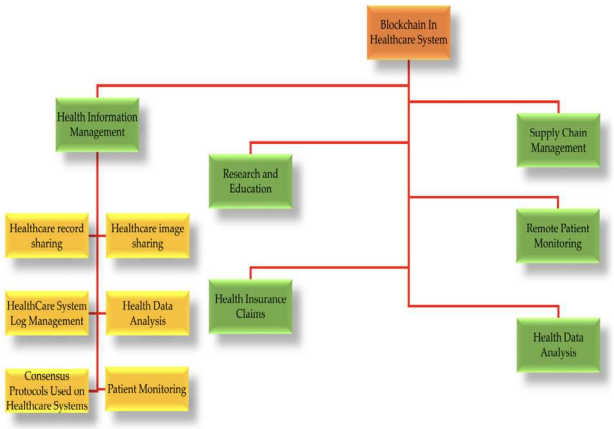

Fig-

E. Follow my vote

Online voting has been a topic of discussion for many years, with proponents citing increased convenience and accessibility as potential benefits. However, concerns about security and reliability have prevented the widespread adoption of online voting systems. Follow My Vote addresses these concerns using blockchain technology to provide a secure and transparent voting platform. Follow My Vote was founded in 2012 with the goal of creating a secure and transparent online voting system. The platform uses blockchain technology to create a tamper-proof record of all votes cast, ensuring that the results cannot be altered or manipulated. The platform also utilizes end-to-end encryption to protect user privacy and prevent unauthorized access to voting data.

a. Benefits of Follow My Vote

One of the main benefits of Follow My Vote is increased transparency in the voting process. Through the use of blockchain technology, all votes are logged and rendered incorruptible, creating a tamper-proof record of the results of the election. This increased transparency can help to increase public trust in the voting process and reduce concerns around election fraud.

Follow My Vote also offers increased accessibility for voters. Voters no longer need to go to a real polling site because they can cast their ballots online from any location with an internet connection. This can help to increase voter turnout, particularly among populations that may have difficulty accessing traditional polling places.

b. Technical Implications of Follow My Vote

There are a number of technical ramifications that should be taken into account when using blockchain technology for online voting. The capacity of blockchain technology to produce a tamper-proof record of every transaction is one of its main benefits. In the context of online voting, this means that all votes are recorded in a secure and transparent manner, with each vote being linked to a unique cryptographic key. This ensures that the results of the election cannot be altered or manipulated, providing greater security and transparency in the voting process.

However, the use of blockchain technology also has some potential technical challenges. For example, the scalability of blockchain networks is a major issue that needs to be addressed. A blockchain network's ability to process votes is constrained by the size of the blocks that make up the blockchain. This means that if there are a large number of votes to be processed, the network may become congested and slow, potentially delaying the announcement of the election results.

Another potential technical challenge is the issue of voter authentication. Ensuring that voters are who they claim to be is a critical aspect of any online voting system. A multi-factor authentication procedure is used by Follow My Vote to make sure that voters are validated before they may cast their ballots. However, there is always the risk that hackers may be able to compromise the authentication process, potentially allowing them to cast fraudulent votes.

F. Decentralized Applications (dApps)

Instead of utilizing a central server or infrastructure, decentralized applications (DApps) are a form of program that are created to run on a decentralized network. These applications can work in a trustless and decentralized manner since blockchain technology is frequently used in their development [29].

The absence of any central authority or middleman control over decentralized applications is one of their main advantages. As a result, they can provide consumers greater security, privacy, and control while also being more resistant to censorship and manipulation. Decentralized applications can also make new types of business models possible that were previously not possible with conventional centralized systems, such as tokenization and micropayments.

Decentralized applications can in a wide variety of forms, from social networks and messaging services to gaming and gambling programs. The Ethereum blockchain is a well-liked platform for developing and executing smart contracts, and it provides the foundation for some of the most well-known decentralized apps. With the programming language Solidity, developers may use Ethereum to build decentralized apps with intricate logic and business rules.

Uniswap, a decentralized exchange for trading bitcoins, is among the most well-known decentralized applications. Users can trade cryptocurrencies with Uniswap, which runs on the Ethereum blockchain, in a decentralized and trustless way without the need for a central exchange or middleman.

The decentralized prediction market platform Augur is another illustration of a decentralized application. Users of Augur can build and trade prediction markets on a variety of topics, and they are rewarded for making successful forecasts with REP, the platform's own cryptocurrency. In the blockchain and cryptocurrency sector, decentralized applications are an area of innovation that is expanding quickly. In the upcoming years, we may anticipate the development of even more ground-breaking and

revolutionary decentralized apps due to the ongoing advancement of technology.

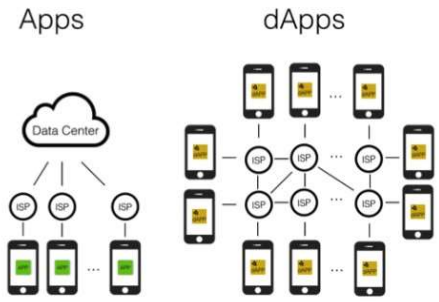

Fig- Decentralized Applications

Blockchain technology is used by decentralized applications (dApps) as a transparent and secure mechanism to store and manage data as well as to execute and validate transactions without the involvement of middlemen. The blockchain acts as a distributed ledger to keep track of all transactions and data changes, creating an unchangeable and impenetrable record of all activity [29, 30].

A decentralized application (dApp) uses the blockchain as the program's underlying architecture to handle and interact with data in a safe and open manner. The execution of business logic or the transfer of payments can both be automated using smart contracts, which are pieces of self-executing code that are recorded on the blockchain [33].

Examples of some dApps using Blockchain as their underlying mechanism-

1. Users of the popular Ethereum blockchain-based game CryptoKitties may collect, breed, and trade virtual cats.
2. On the Ethereum blockchain, a decentralized marketplace called Golem allows individuals to rent out their unused computing resources for jobs like producing 3D graphics.
3. MakerDAO is a decentralized platform for stablecoins built on the Ethereum blockchain, allowing users to borrow a stablecoin (DAI) by pledging Ethereum tokens as security.
4. The Ethereum blockchain-based Basic Attention Token (BAT) digital advertising platform pays users in cryptocurrency for watching advertisements and other content.
5. Built on the Bitcoin blockchain, OpenBazaar is a decentralized marketplace for buying and selling commodities and services.
6. Storj is a decentralized cloud storage system built on the Bitcoin blockchain that enables users to charge others for extra storage space.
7. In order to facilitate transparent charitable giving and social impact projects, BitGive is a non-profit company.
8. Blockstream Satellite is a satellite-based blockchain broadcast technology that transmits data globally via the Bitcoin blockchain.

A. Lightning Network

The Lightning Network enables the connection of various payment channels, resulting in a network of payment channels between parties. This makes it possible to send money to a party indirectly through a network of linked payment channels.

On top of the Bitcoin blockchain, there is a second layer payment mechanism called the Lightning Network. Its main goal is to make transactions on the Bitcoin network faster, less expensive, and more scalable. By establishing a network of payment channels between two parties, the Lightning Network functions. As they do not need to be recorded on the Bitcoin blockchain for every transaction, these payment channels enable rapid and inexpensive transactions.

Two parties must construct a multi-signature address on the Bitcoin blockchain in order to establish a payment channel, which necessitates that both parties approve of all transactions. Following that, they trade a number of off-chain transactions that update the payment channel's balance. When the channel is closed, the channel's final balance is recorded on the Bitcoin blockchain.

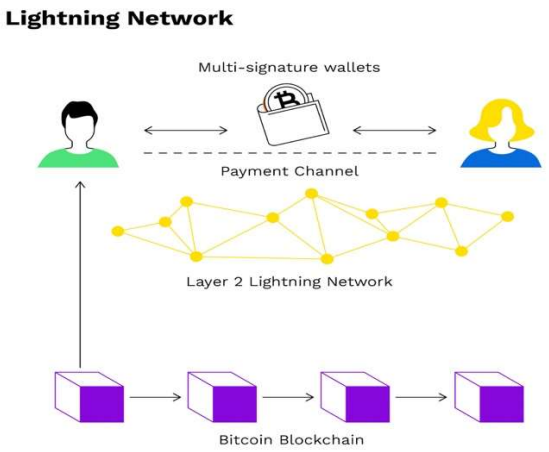

Fig- Lightning Network

Scalability is one of the Lightning Network's main advantages. Compared to using the Bitcoin blockchain directly, transactions can be completed more quickly and cheaply because the majority of transactions take place off-chain. For Bitcoin to become a more useful payment method, especially for micropayments, this scalability is crucial.

Increased anonymity is another benefit of the Lightning Network, as transactions are carried out off-chain and are not accessible to everyone on the Bitcoin blockchain. Moreover, it supports quick transactions, a crucial feature for use cases like point-of-sale transactions [31,35].

B. OpenBazaar

A decentralized market using blockchain technology is called OpenBazaar. Instead of using middlemen like in conventional marketplaces, the platform enables users to transact directly with one another for the purchase and sale of goods and services. Peer-to-peer (P2P) networks enable private and secure transactions.

There is no central authority or control over OpenBazaar because it runs on a decentralized network. The InterPlanetary File System (IPFS), a protocol for storing and distributing files in a distributed network, is used to establish direct connections between users. This means that transactions are carried out directly between buyers and sellers and that there are no fees or limitations on what can be offered on the platform. Users must download and install OpenBazaar on their computer or mobile device in order to utilize it. Users can then register on the platform, establish a profile, and start buying and selling. On OpenBazaar, transactions are made using digital currencies like Bitcoin, Ethereum, and Litecoin.

OpenBazaar's emphasis on privacy and security is one of its standout characteristics. The platform employs encryption to guarantee the privacy and security of every transaction. Additionally, because all data is housed in a decentralised network, there is no central database or server that outsiders can break into or access [36].

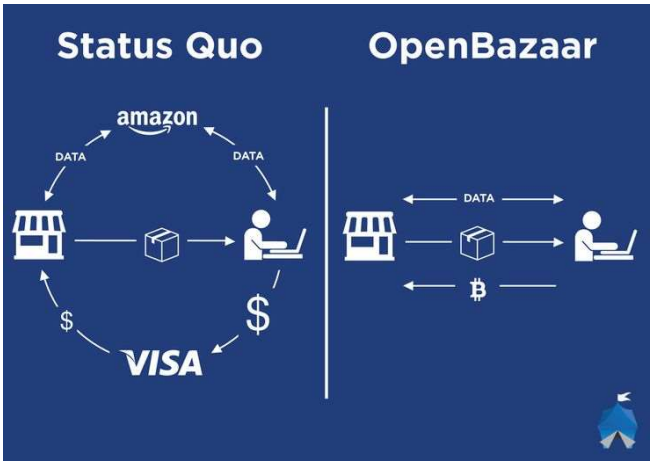

Fig- OpenBazaar vs Status Quo

The capability of OpenBazaar to facilitate international trading is another crucial characteristic. It is a genuinely global marketplace since users can deal with anyone anywhere in the globe and there are no middlemen or limitations on what can be sold. Moreover, OpenBazaar offers a special rating system that lets buyers and merchants assess their interactions with one another. Users may then decide who to transact with greater knowledge thanks to the increased trust and confidence in the market.

Ultimately, OpenBazaar is a ground-breaking platform that offers consumers and sellers a decentralised, private, and secure marketplace. It is a promising alternative to conventional marketplaces and is anticipated to continue growing in popularity due to its emphasis on peer-to-peer transactions, privacy, and security [37].

C. Counterparty

Using the Bitcoin blockchain, users may generate and trade digital assets using Counterparty, a decentralised platform. The development of unique tokens, smart contracts, and decentralised apps (dApps) on the Bitcoin network is made possible by this peer-to-peer protocol.

Using the security and dependability of the Bitcoin blockchain as a layer, Counterparty functions as a platform for asset creation and administration. Custom tokens that represent anything from company shares to in-game items or other digital assets can be created and issued by users. The immutability and traceability of these tokens are guaranteed by their storage on the Bitcoin network.

Counterparty facilitates the creation and execution of smart contracts in addition to the creation of tokens. These contracts have their conditions directly put into lines of code, making them self-executing. Smart contracts can be used to manage supply chains, automate intricate transactions, and more. Decentralized apps (dApps) can be created using Counterparty on the Bitcoin network. These programs, which can be configured to run independently and securely on the blockchain, can range from online games to financial applications.

Fig- Counterparty Bitcoin Blockchain

Allowing for decentralised asset trading is one of Counterparty's primary features. On the platform, users can directly buy and sell assets without the aid of middlemen or centralized exchanges. As all transactions are tracked on the Bitcoin blockchain, it is a safer and more open way to transfer digital assets. The community-driven development of Counterparty is another key component. Anyone can contribute to the platform's growth and improvement because it is open source. This guarantees that the platform is always using the most recent technology and industry standards.

The creation and maintenance of digital assets on the Bitcoin blockchain are made possible by Counterparty, a strong and adaptable platform. It is a promising platform for a variety of applications in the digital asset market because of its support for customized tokens, smart contracts, and decentralised apps (dApps), as well as its emphasis on decentralised trading and community-driven development [33,34].

V. HOW BLOCKCHAIN IMPROVED

a. BEvote

The design outlined is vulnerable to two potential threats in real-world scenarios. First, a Sybil attack where an attacker creates several Bitcoin addresses to fake the identities of voters and gain more voting rights. Second, the premature leakage of ballots by a misbehaving insider of the Supervisor who could reveal the ballots before the voting has ended.

1. *E-Voting Protocol for BEvote for enhanced security*

A safeguard E-voting protocol is designed to address the potential risks outlined earlier in BEvote. The protocol includes a validation mechanism based on public key based cryptography to avert Sybil attacks and an encryption policy using collaborative Shamir random secret sharing to thwart untimely leakage of ballots by Supervisors. The protocol involves several steps, including registration, anonymous address generation, secret sharing, ballot creation, and voting transaction broadcasting. Each candidate collects secret shares from the voting transactions and constructs a winning transaction if enough shares are obtained, while the Voter constructs a refund transaction otherwise.

Furthermore, the security of the protocol may also depend on the implementation of the Supervisor's verification process, which is crucial in ensuring that only legitimate voters, candidates, and mixers participate in the election. If the verification process is not robust enough, it could result in fraudulent or invalid votes, compromising the integrity of the election.

However, while the proposed protocol for anonymous voting using Bitcoin addresses and secret sharing seems promising, implementing it in practice will require careful consideration of the potential challenges and limitations. It may also require a high level of technical expertise and resources to ensure that the protocol is implemented securely.

2. *Security Analysis*

A series of theorems to are provided to prove the efficiency and robustnesss of the BEvote e-voting protocol. The first theorem focuses on the validity of the protocol, which ensures that only valid bodies examined can chip into the voting process, and the second theorem discusses the robustness of the system, which can resist attacks and avoid errors. The third theorem confirms that the protocol guarantees anonymity to shield the concealment of voters, and the fourth theorem guarantees fairness in the choice of voters that cannot be induced by the protocol's fairness.

The fifth theorem confirms the verifiability of the voting procedure and the results, even when the protocol run has terminated. Finally, the sixth theorem confirms the receipt-free nature of the protocol, which ensures that ballots that could not be attested in advance are sent by precise voters. The provided theorems prove that the BEvote e-voting protocol is an effective and robust solution that can ensure the anonymity, validity, fairness, verifiability, robustness, and receipt-free nature of the voting process.

3. *Performance Evaluation*

a. *Theoretical Analysis*

Based on the theoretical analysis, the computational and communication overhead of BEvote has been evaluated. The efficiency of BEvote is mainly affected by three key stages, including confusing voters' identities, generating ballots, and constructing voting transactions. The third stage's efficiency is determined by the output of the Bitcoin platform used as the storage infrastructure, which is not evaluated as the Bitcoin network has substantially improved its speed of transaction. Therefore, the focus is on investigating the efficiencies of the first two stages.

The confusion strategy for voter's identity comprises identity confusion, confusion audit and Mixer registration, with most of the calculative overhead focused in the confusion phase due to the time-consuming modular multiplication and modular exponentiation operations. The confusion phase requires both mixers and voters to compute RSA signatures and group blind signatures.

b. *Experimental Analysis*.

The simulation involves using the JPBC library and java programming to perform procedures in the elliptic curve group, while also utilizing numerous threads for simulation of numerous voters simultaneously. The simulation was conducted on a 64-bit Windows 10 operating system, equipped with 16 GB RAM and CPU with i7-8750H (@2.2 GHz). To execute the program, the user generates a polynomial by selecting arbitrary numbers and then switches n numbers to gauge it, sending it to further users. Each user receives their secret share by adding up all the received values.

The investigational values presented were averaged after continuing the simulation 100 times using Eclipse IDE. The simulation results showed that the implementation time of the confusion strategy for voter's identity profoundly depends on the modular exponentiation operation, which is much more time-consuming than the modular multiplication operation. As a result, the total finishing time of the confusion phase is larger than ten times that of the confusion audit and Mixer registration phases.

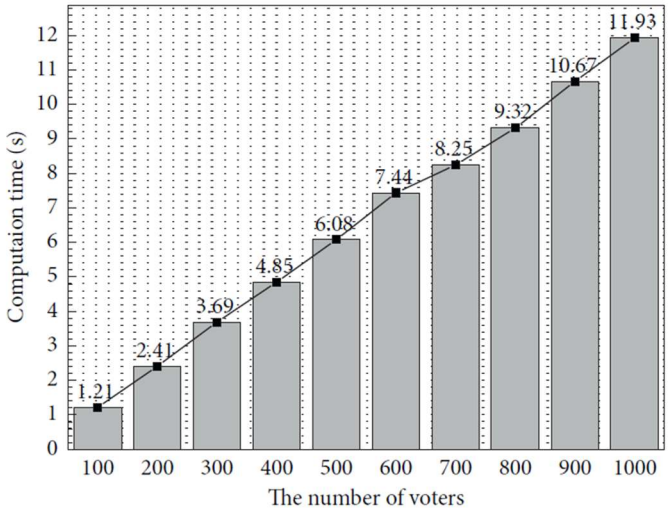

Fig- Simulation Results

Regarding the ballot collection stage, the simulation results demonstrated that the time overhead intensified approximately linearly with the amount of voters. However, even for thousands of voters, the computation time was lower than one minute, which suggests that the time overhead for extensive-scale systems is within an adequate range. Overall, the simulation results showed that BEvote has reasonable computational and communication overhead, which makes it feasible for practical use in large-scale voting systems.

4. Future Scope

The Bitcoin-based electronic voting with robustness and anonymity is designed to abstract a Bitcoin transaction as the voting procedure achieves strong anonymity through a coin-mixing-based model. The protocol keeps the voting numbers private using E-voting protocol based upon secret sharing. Security probes and investigational evaluations have been conducted to demonstrate the robustness and efficiency of the proposed scheme. There are various paths in which this work can be widened. Firstly, the high network lags and low throughput of the Bitcoin could cause scalability issues in local joint medical systems. A probable solution is to employ Mobile Edge Computing (MEC) nodes to construct a private blockchain concerning E-voting, rather than relying on a public blockchain. In this case, the blockchain can be made more voting friendly, with both robustness and scalability.

Another path is to discover additional applications of E-voting, such as recommendation systems/decision support. E-voting can be used to facilitate the decision-making process in various fields, such as corporate governance or public policy. Additionally, recommendation systems can use E-voting to obtain user feedback and improve their recommendations.

Overall, the scheme provides a promising approach for secure and anonymous E-voting, and there is ample scope for further research in this area.

b. NFT's

a. Intellectual Property Right

NFTs pose a significant challenge and risk due to the issue of intellectual property rights. Before purchasing anything made from an NFT seller, it is essential to confirm their ownership rights. Sometimes, people have taken photos or made reproductions of NFTs which could lead to disputes about ownership. When an NFT is sold, the buyer only gains access to its assets and not its intellectual property rights. The smart contract metadata clearly outlines these terms for ownership. NFTs provide a great source of revenue but come with numerous risks due to a lack of regulations surrounding trading in them and excessive hype around them.[7]

b. Cyber Security

With the exponential growth of NFT transactions and digital world, cyber security has become more of a priority. Malicious actors may create fake NFTs under famous artists.

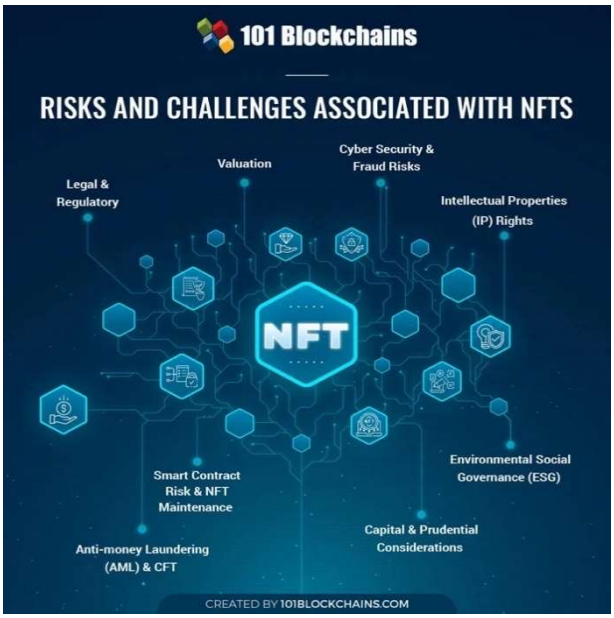

Fig. Risks and Challenges in NFTs[18]

names or sell copies of popular NFTs; this could lead to copyright theft, false giveaways, and airdrops via NFT airdrops. Technology has made it easier to trade digital assets but also presents significant security risks.

c. Security and Privacy

NFTs face a number of challenges but Data integrity and security must always remain at the top of any system's priority list, making privacy and security for NFTs an especially major challenge. Many NFT transactions rely on Ethereum platform which offers pseudo-anonymity but not total anonymity. As their activity is visible to everyone else, users can only hide their identities to an extent. With increased risk of data misappropriation or loss of linkage to unauthorized parties possible, enhanced security measures need to be put in place in order to safeguard sensitive data against potential breaches.

d. Environment

NFTs are becoming more widely adopted, which makes investing in crypto technology easier. Unfortunately, the environmental consequences are significant: Ethereum alone is estimated to consume 44.94 Terawatt-hours annually of electricity. Bitcoin mining consumes energy on par with countries such as Qatar or Hungary, while using resources comparable to those employed in Sweden and Malaysia. Recent studies have suggested that blockchain-based technologies could cause Earth's temperature to rise two degrees Celsius higher than historical levels if they become widely adopted. Power shortages in Iran have been attributed to crypto miners. China's energy consumption using this type of technology is higher than countries such as Qatar or Czech Republic's annual greenhouse gas emissions.[18]

e. Discussion

This discussion examines the pros and cons of NFTs. NFTs offer a secure and convenient method to generate revenue on the blockchain, linking unique information to one account for authentication purposes. However, this technology also comes with its own risks and issues to contend with. Online

transactions are usually vulnerable to misuse as well as unauthorized access. New technologies like zero-knowledge proofs can be employed as a safeguard against these risks.

Users with large amounts of NFTs should utilize non-browser wallets with advanced security teams and physical wallets for long-term safekeeping. Developers can encourage developers to utilize more sustainable alternatives like Bit Green and Solar Coin in order to reduce the environmental impact of NFTs. This may even be applied in virtual environments like the Metaverse to boost their reliability and utility, thus encouraging more people to invest in NFTs.

c. Follow My Vote

Legal Implications of Follow My Vote

The use of blockchain technology for online voting also has several legal implications that need to be considered. In many jurisdictions, the legal framework surrounding online voting is still evolving, and there may be legal challenges to the use of blockchain technology for voting.

One potential legal issue is the issue of voter privacy. While Follow Although My Vote uses end-to-end encryption to protect voter privacy, there may be questions about how voter data is gathered and used. It is crucial to confirm that the gathering and use of voter data complies with all applicable privacy regulations.

Another potential legal issue is the issue of election integrity. In many jurisdictions, there are strict rules around the conduct of elections, including rules around campaign financing, voter registration, and ballot counting. It is crucial to make sure that using blockchain technology for online voting complies with all of these guidelines and that the election's results are recognised by all pertinent authorities.

Impact of Follow My Vote on Voter Turnout and Election Results

One of the key potential benefits of Follow My Vote is its potential impact on voter turnout. By providing a more convenient and accessible way to vote, Follow My Vote could help to increase voter turnout, particularly among populations that may have difficulty accessing traditional polling places, such as the elderly, disabled, or those living in rural areas.

However, the impact of Follow My Vote on voter turnout is not clear. While online voting may increase convenience and accessibility, there may also be concerns around the security and reliability of the voting process, which could potentially discourage some voters from participating.

Follow My Vote could also have an impact on election results. By providing a more transparent and secure voting process, Follow My Vote could help to reduce concerns around election fraud and increase public trust in the electoral process. This could help to ensure that the election results are accepted by all relevant authorities and reduce the risk of political unrest or violence following an election.

However, there are also potential risks to using Follow My Vote for election results. If there are technical issues or security breaches during the voting process, this could potentially compromise the integrity of the election results, leading to accusations of election fraud or other irregularities.

Overall, Follow My Vote's effect on voter participation and election outcomes is unclear and will rely on a number of variables, including the particular environment in which the system is used and the degree of public confidence in it.

Follow My Vote is an innovative platform that has the potential to improve the voting process by increasing transparency and security. However, there are also potential drawbacks and technical and legal implications that need to be considered. Further research is needed to fully understand the potential impact of Follow My Vote on voter turnout and election results, and to determine whether the platform is a viable solution for improving the voting process. Overall, Follow My Vote represents an important step towards creating a more secure and transparent online voting system.

d. dApps

1) Lightning network

The Lightning Network has the power to completely alter how Bitcoin transactions are carried out. Lightning Network can facilitate new use cases for Bitcoin, including immediate payments, micropayments, and machine-to-machine payments, by enabling quick and affordable micropayments. As a result, more people may be able to use Bitcoin as a form of payment, bringing it into the mainstream and increasing its accessibility.

Blockchain offers security in Lightning Network by enforcing the finality of transactions. The closing of a channel broadcasts the channel's final state to the Bitcoin blockchain, ensuring that the transaction is legitimate and irreversible. While transactions must be approved by both parties, using multisignature addresses in Lightning Network channels adds an additional layer of security.

Future plans for Lightning Network include making it possible for quick, inexpensive, and secure Bitcoin transactions to be processed off-chain, which could help to address some of the scalability problems the Bitcoin network is now experiencing. The capacity and capabilities of the Lightning Network are anticipated to increase as more users use it, enabling it to develop into a more reliable and effective payment system.

2) OpenBazaar

E-commerce may be significantly impacted by OpenBazaar. OpenBazaar, a decentralised marketplace, provides a safer and more private substitute for established e-commerce sites like Amazon or eBay. With the help of OpenBazaar, businesses could sell their wares without having to pay expensive commissions to middlemen, while customers could make purchases without disclosing any personal information. A more decentralised and democratic e-

commerce environment may result from this, giving smaller retailers a greater chance to compete with bigger ones.

Blockchain offers security by producing a tamper-proof record of every transaction. Because all OpenBazaar transactions are stored on the Bitcoin blockchain, they cannot be changed or reversed. This makes sure that there is no chance of fraud and that all transactions are transparent.

Future plans for OpenBazaar include developing a more decentralised and open marketplace where users can trade goods and services directly with one another without the use of middlemen. It is anticipated that the platform will keep improving, introducing new features and capabilities that will increase its user appeal and transaction processing effectiveness.

3) Counterparty

The financial sector may be impacted by Counterparty. Counterparty can enable new use cases by issuing assets on the Bitcoin blockchain, including the development of digital securities, smart contracts, and decentralised exchanges. By lowering the entry barriers for carrying out financial transactions and issuing securities, this may increase the number of people who can access the financial sector. Additionally, Counterparty can improve the security and openness of financial transactions by using the Bitcoin blockchain as a safe and decentralised ledger.

Blockchain contributes to security in Counterparty by offering a safe and decentralised ledger for tracking asset ownership and transactions. Counterparty makes guarantee that all transactions are impenetrable to tampering and cannot be undone by utilizing the Bitcoin blockchain. Additionally, Counterparty's implementation of smart contracts enables the development of sophisticated financial instruments that could boost transaction security [38].

Future plans for Counterparty include offering a safe and decentralised marketplace for the creation and exchange of assets and financial instruments. By facilitating the creation and trading of complex financial instruments, the platform has the potential to upend established financial markets.

Since they are all cutting-edge and revolutionary uses of blockchain technology that have the ability to change how we conduct transactions and connect with one another, the future potential of Lightning Network, OpenBazaar, and Counterparty appears bright.

In general, the future of Lightning Network, OpenBazaar, and Counterparty is promising because they are all blockchain-based apps with the potential to improve security, efficiency, and transparency across a range of sectors and use cases. These programs may become more significant in determining the direction of commerce and finance as they develop and mature.

CONCLUSION

An extensive range of industries, including art and collectibles as well as e-commerce, finance, and voting, have been dramatically impacted by blockchain technology. The invention of NFTs, which have transformed how we think about ownership and value in the digital world, is one of the most exciting advancements in blockchain technology. BEvote and MyVote have shown how blockchain-based voting systems can improve democratic process accessibility, security, and transparency.

From art and collectibles to e-commerce, economics, and voting, blockchain technology has had a profound impact on a variety of industries. The invention of NFTs, which has completely changed how we think about ownership and value in the digital world, is one of the most exciting advancements in blockchain technology. The promise of blockchain-based voting systems to improve accessibility, security, and transparency in the political process has been shown by BEvote and MyVote.

Overall, across a variety of industries and application cases, blockchain technology has aided in enhancing security, effectiveness, and transparency. It has also opened up more access to markets that were previously closed off to innovation and disruption. These blockchain-based solutions are likely to play an even bigger role in determining how business, finance, and society as a whole develop throughout time.

REFERENCES

[1] Pilkington, Marc. "11 Blockchain Technol-Ogy: Principles and Applications." Re-Search Handbook On Digital Transfor-Mations (2016)

[2] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Tech-Nology: Beyond Bitcoin. Applied Innova-Tion.

[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2009. [Online] Available: https://bitcoin.org/bitcoin.pdf.

[4] J. Kishigami et. al., “The Blockchain-based Digital Content Distribution System” in 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, 2015.

[5] G. Hurlburt and I. Bojanova, “Bitcoin: Benefit or Curse?” in IT Pro, vol. 16, no. 3, 2014

[6] Ning Lu, Xin Xu, Chang Choi, Tianlong Fei, Wenbo Shi, "BEvote: Bitcoin-Enabled E-Voting Scheme with Anonymity and Robustness", Security and Communication Networks, vol. 2021, Article ID 9988646, 14 pages, 2021

[7] Rehman, Wajiha & Zainab, Hijab & Imran, Jaweria & Bawany, Narmeen. (2021). NFTs: Applications and Challenges. 10.1109/ACIT53391.2021.9677260.

[8] Saeed Banaeian Far, Seyed Mojtaba Hosseini Bamakan, Qiang Qu, Qingshan Jiang”A Review of Non-fungible Tokens Applications in the Real-world and Metaverse”

[9] Redman, J. (2020, September 13). *NFT economy grows exponential: $1m in non-fungible token sales last week*. Bitcoin News. Retrieved April 2, 2023, from https://news.bitcoin.com/nft-economy-grows-exponential-1m-in-non-fungible-token-sales-last-week/

[10] Julia ng. (2023, March 7). *Most popular NFT marketplaces by market share*. CoinGecko. Retrieved April 2, 2023, from https://www.coingecko.com/research/publications/market-share-nft-marketplaces

[11] Murray, P. (2021, April 27). *Golden State Warriors launch NFT collection, becoming first U.S. sports team to release own nfts*. Forbes. Retrieved April 2, 2023, from https://www.forbes.com/sites/patrickmurray/2021/04/27/golden-state-warriors-launch-nft-collection-become-1st-sports-team-to-create-own-nfts/?sh=709ce71d1d94

[12] Priya Pedamkar. (2023, March 4). *Applications of blockchain: 10 most popular application of Blockchain*. EDUCBA. Retrieved April 2, 2023, from https://www.educba.com/applications-of-blockchain

[13] Etal. (2022, May 20). *From bitcoin to the metaverse: The current evolution is a revolution*. Check Point Software. Retrieved April 2, 2023, from https://blog.checkpoint.com/2022/05/20/from-bitcoin-to-the-metaverse-the-current-evolution-is-a-revolution/

[14] Jeon, H.-joo, Youn, H.-chang, Ko, S.-mi, & Kim, T.-heon. (2021, August 3). *Blockchain and AI meet in the metaverse*. IntechOpen. Retrieved April 2, 2023, from https://www.intechopen.com/chapters/77823

[15] Metaverse in Blockchain. (n.d.). Retrieved April 2, 2023, from https://www.alibabacloud.com/knowledge/tech/metaverse-in-blockchain

[16] 101 Blockchains. (2022, August 15). *Non-fungible tokens - risks and challenges*. 101 Blockchains. Retrieved April 2, 2023, from https://101blockchains.com/nft-risks-and-challenges/

[17] *Ethereum Energy Consumption index*. Digiconomist. (2022, December 6). Retrieved April 2, 2023, from https://digiconomist.net/ethereum-energy-consumption

[18] Scribani, J. (2018, September 7). *Infographic: How the Blockchain is powering our future*. Visual Capitalist. Retrieved April 2, 2023, from https://www.visualcapitalist.com/blockchain-powering-future/

[19] Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain Application in Healthcare Systems: A Review. Systems. 2023; 11(1):38

[20] Bitpanda. (n.d.). *How does a blockchain work?* - Bitpanda Academy. Retrieved April 2, 2023, from https://www.bitpanda.com/academy/en/lessons/how-does-a-blockchain-work/

[21] Abid Haleem, Mohd Javaid, Ravi Pratap Singh, Rajiv Suman, Shanay Rab,"Blockchain technology applications in healthcare: An overview,International Journal of Intelligent Networks"

[22] L. Soltanisehat, R. Alizadeh, H. Hao and K. -K. R. Choo, "Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review," in IEEE Transactions on Engineering Management,

[23] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul and S. Ghouzali, "Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues

[24] M. H. Chinaei, H. Habibi Gharakheili and V. Sivaraman, "Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract," in IEEE Internet of Things Journal,

[25] Anand, A. (n.d.). *6 applications of blockchain in the healthcare sector*. Analytics Steps. Retrieved April 2, 2023, from https://www.analyticssteps.com/blogs/6-applications-blockchain-healthcare-sector

[26] Osgood, R., 2016. The future of democracy: Blockchain voting. COMP116: Information security, pp.1-21.

[27] 2. Abuidris, Y., Kumar, R. and Wenyong, W., 2019, December. A survey of blockchain based on e-voting systems. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications

[28] 3. Agbesi, S. and Asante, G., 2019, November. Electronic voting recording system based on blockchain technology. In 2019 12th CMI Conference on Cybersecurity and Privacy (CMI)

[29] Raval, S., 2016. *Decentralized applications: harnessing Bitcoin's blockchain technology*. " O'Reilly Media, Inc.".

[30] Verma, S., Dash, S. and Joshi, A., 2022, October. A Detailed Study of Blockchain and dapps. In *2022 International Conference on Cyber Resilience (ICCR)* (pp. 1-5). IEEE.

[31] Miraz, M.H. and Donald, D.C., 2019, April. LApps: technological, legal and market potentials of blockchain lightning network applications. In *Proceedings of the 2019 3rd International Conference on Information System and Data Mining* (pp. 185-189).

[32] Chauhan, A., Malviya, O.P., Verma, M. and Mor, T.S., 2018, July. Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 122-128). IEEE.

[33] Wu, K., Ma, Y., Huang, G. and Liu, X., 2021. A first look at blockchain-based decentralized applications. *Software: Practice and Experience*, *51*(10), pp.2033-2050.

[34] Wu, K., 2019. An empirical study of blockchain-based decentralized applications. *arXiv preprint arXiv:1902.04969*.

[35] Holzer, P., 2020. *Payment Channel Network Analysis with Focus on Lightning Network* (Doctoral dissertation, Wien).

[36] Arps, J.E. and Christin, N., 2020. Open market or ghost town? The curious case of OpenBazaar. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24* (pp. 561-577). Springer International Publishing.

[37] Dennis, R. and Owen, G., Breaking open the Bazaar: identifying and exploiting key weaknesses in the OpenBazaar network.

[38] Baliga, A., 2016. The blockchain landscape. *Persistent Systems*, *3*(5), p.4.