# Blockchain, a Distributed Ledger Technology and in Depth Study of its Applications in Various Domains

**Gayatri Bangar[1], Nahush Kulkarni[2], Sameer Mahajan[3]**

*[2,3]Student, Department of Computer Engineering, TEC, University of Mumbai, Mumbai, India*
*[1]Student, Department of Information Technology, TEC, University of Mumbai, Mumbai, India*

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract:** *Blockchain, a distributed ledger technology, is a structure that comprises a list of records, known as blocks, that are stored in a public database. These blocks are cryptographically linked together. Due to some of the properties like decentralization, transparency, irreversibility etc, blockchain is not only of great interest to itself as a fundamental technology, but also has huge potential when incorporated into several other areas. The most popular application of blockchain is cryptocurrency, however there are several other applications that are yet to be explored. This paper discusses some of the enthralling applications of blockchain technology.*

***Index terms: Blockchain, Decentralization, Internet of Things, Voting Mechanism, Supply Chain, Identity Management, Applications***

## 1. INTRODUCTION

With the use of decentralization and cryptographic hashing, Blockchain, also referred to as Distributed Ledger Technology (DLT), renders the history of any digital asset irrevocable and clear. [19]

A Google Doc is a basic analogy for understanding blockchain technology. The data is shared instead of copying or transferring as we create a document and exchange it with a group of individuals. This provides a decentralized chain of delivery that simultaneously allows everybody access to the data. No one is held out waiting for updates from some other user, while in actual all modifications to the document are registered, making changes fully clear. [19]

Blockchain is indeed a platform that is highly exciting and innovative as it helps minimize risk, rules out theft and offers clarity for various uses in a scalable manner. [19]
Three major terms are used in Blockchain: blocks, nodes and miners. [19]

### Blocks

Every chain is made up of several chains and has three key aspects for every block:

1. The data within that block.
2. An entire 32-bit integer, termed as nonce. Whenever a block is produced, the nonce is. Chosen at random, which further creates a hash of block header.
3. The hash is a number of 256 bits wedded to the nonce. This should begin with an immense number of (i.e. incredibly small) zeroes.

A nonce produces the hash code just as the first block of a chain is produced. Unless it's been mined, the information in the block is deemed signed and forever bound to the nonce and hash. [19]

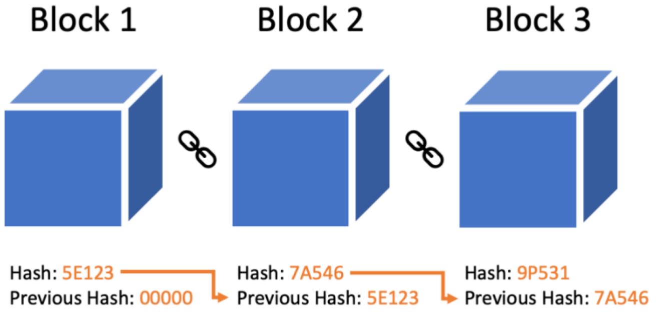

**Fig-1:** A diagrammatic representation of blocks in a blockchain

### Miners

Via a method called mining, miners develop new blocks upon the chain.
Every block has its own distinct nonce and hash in a blockchain, but also refers to the preceding hash chain of blocks, so mining a block is not simple, particularly on large chains. [19]

To resolve the unbelievably complicated mathematical problem of seeking a nonce which produces an agreed hash, miners utilize special tools. Since the nonce is only 32 bits and the hash is 256, there exist nearly four billion different variations of nonce-hash that must be mined prior to finding the correct one. If it occurs, the "golden nonce" is seen to be discovered by miners and their block is attached to the chain. [19]

Producing a modification to any block sooner in the chain needs not just certain blocks with the tweak to be remined, but also the blocks that follow. That's why exploiting blockchain technologies is incredibly challenging. Assume of it as "safety in math" because it takes a tremendous amount of time and computational resources to discover golden nonce. [19]

Whenever a block is adequately mined, every one of the nodes on the network support the shift and financially compensate the miner. [19]

**Nodes**

Decentralization is among the most crucial principles of blockchain computing. The chain cannot be owned by any single machine or entity. Instead, through the nodes attached to the chain, it is a distributed ledger. Nodes can be seen as an electronic system that holds blockchain clones and keeps the network running. [19]

Each node has its very own copy of the blockchain and each newly mined block for the chain to be modified, trusted and validated it must be accepted by the network computationally. Since blockchains are transparent, it is possible to quickly verify and display any activity in the ledger. A unique alphanumeric identifier that indicates their purchases is issued to each user. [19]

Integrating public records with a checks-and-balances framework helps preserve integrity throughout the blockchain and builds trust among users. Fundamentally, it is possible to visualize blockchains as the scalability of trust through technology. [19]

Following are the properties exhibited by blockchain technologies:

1. Data transparency
2. Decentralized control
3. Data auditability
4. Decentralized consensus
5. Security
6. Distribute information [4]

Some of the common implementations of blockchain are:

1. Bitcoin
2. Ethereum: It is a programming platform with a scripting language called Solidity.
3. Rootstock
4. Hyperledger [4]

We have discussed the most common applications in the upcoming section.

## 2. APPLICATIONS OF BLOCKCHAIN

### 2.1 Voting Mechanism

Voting, traditional or electronic, is a vital act that builds the democracies. The traditional method of voting requires a person to physically visit the voting booth, wait in long queues and cast their vote. Many people don't cast their votes as they might be out of the station, they might think that their votes do not count or they don't have faith in voting systems. These problems can be resolved by electronic voting (e-voting). There will be no need of visiting the voting booth and waiting in a queue, a person can cast their vote by being anywhere across the world, this can be made possible with the help of e-voting. Remote electronic voting comes with many challenges. It requires stringent security measures because there is a risk of hacking activities and there is a risk of large scale manipulation, coerced and influenced voting can also be a major problem. These challenges can be resolved by blockchain technology as it is immutable, transparent and it cannot be hacked into to manipulate the results.

Zhang et. al. [1] proposed a protocol, for peer voting, that safeguards the voter's identity and allows to discover and rectify cheating without the need of a third party. The main concepts behind the protocol is 1) Distributed Voting: Peer's voting intention are tested by assigning multiple ballots instead of just one and by the mode of their ballots. Privacy of vote is maintained due to this design. 2) Distributed Tally: The counting of ballots is distributed to each peer using the homomorphic encryption application. Doing so results in elimination of the need for a third party and no peer has complete knowledge of the final results. And 3) Cryptography-based verification: In order to eliminate the dishonest votes, verification of votes and tallying the results is carried out. There is no need for a third party as the verification of votes can be done publicly without violating privacy. The voting protocol is carried out in five stages and needs off-chain and on-chain computations.

Stage 1: Voting: - In this stage, the voters, within the given time frame, use client applications to create and submit their ballots on blockchain.

Stage 2: Two-Phase verification of every ballot :- In this stage, every ballot is decrypted and verified by the peers whose Homographic Encryption Public Key (HEPK) is used to encrypt the ballot.

Stage 3: Re-voting of ballots encrypted by dishonest peers' public key :- A peer has two choices, either to give up replacement so that the ballot with "to be replaced" status can be excluded from voting process or they can revote with a new ballot and the by using other peer's HEPK, encrypt the ballot. Stage 3 is carried out if there is a need to replace the ballot.

Stage 4: Distributed Tally :- In this stage each individual honest peer tallies the ballots and publishes the result on blockchain. By using homographic encryption property the tallies of each peer are verified by smart contract. If a dishonest tally is detected then the corresponding peer is claimed to be dishonest and Stage 3 will be repeated until there are no dishonest tallies found.

Stage 5: Final Aggregation: - In this step, all of the individual results of tally from peers are aggregated using a smart contract and the final voting result is published on the blockchain.

They implemented this protocol on Hyperledger Fabric and concluded that, for small to medium scale voting problems, the protocol is convenient and viable.

Blockchain is categorized into three categories, public, private, consortium blockchain. Public blockchains are weighted under fully decentralized categories, the consensus algorithm depends on competition of computing power and public awareness, and is not controllable by rules and regulations. Although the consensus algorithm cannot be applied to the business community due to two major limitations, (1) a vast amount of energy is wasted and the efficiency of validation of a transaction is also diminished due to the competition of computing power. (2) The unmanageable network-wide decentralized verification is the basis for its block generation and transaction verification, which does not comply with commercial social law and is difficult to comply with the rules of business society [3].

Li et. al. [3] proposed, Proof of Vote (POV), a voting-based consensus algorithm. Their main goal was to build a high-performance consensus algorithm that can be of use for consortium blockchain and prove that, with ultra-low latency in verification of transaction, POV can achieve outstanding performance. There are several organizations in a consortium hence a syndicate committee is formed in order to share information and data efficiently and a commissioner, a member of the syndicate committee, on behalf of every company is chosen. But complete power of controlling the blockchain cannot be given to a particular company and hence a team of butlers is elected to maintain and create blocks. These butlers are elected by the commissioners as recommending, voting and evaluating the butlers are the rights of a commissioner. The two important steps for becoming a butler are,

1. Being a butler candidate
2. Winning a butler's election.

The butler candidates are voted by the commissioners. The commissioners, butlers, butler candidates, users, to authenticate their identities, use cryptography. In this consensus algorithm, the butlers are responsible for creating blocks in a given timeframe. A genesis block is created at the initial step in which commissioners write the initial information and a special block is generated at the end of the round of consensus that includes the result of the elections and server details of newly elected butler nodes. The round of consensus is the process of generating valid blocks and each block is generated in 8 steps. The generated block is then sent for verification to all commissioners. For a block to be valid, minimum 51% votes should be received by a block. The voting processes are mainly for block production and butler candidates. They concluded that the decentralized consensus algorithm, POV, can assure the low power consumption, transaction finality, security and ensures that there will be no bifurcation in blockchain at any point.

Hardwick et. al. [2] proposed a e-voting protocol that uses blockchain transparent ballot boxes. The protocol upholds fundamental e-voting properties like,

1. Fairness: Results of the voting procedure will be disclosed at the end and the results will not be obtainable at any stage, this provides guarantee that the voters will remain uninfluenced by the result.
2. Eligibility: Only eligible voters should be allowed to cast their votes and only once.
3. Privacy: The voters identity should not be revealed at any point.
4. Verifiability: The ability of all the concerned parties to verify that their votes are counted or not, is guaranteed by this property.
5. Coercion-resistance: The vote casted by a coerced voter should not be detectable by the coarser.

Along with these properties, a degree of decentralization is also provided and voters are allowed to change or cancel their votes within a given time frame. The implementation of this proposed protocol was carried out on a private network using Ethereum blockchain API. In order to achieve the primary objective, it was decided that some degree of centralization was necessary. This is due to the inability of storing confidential information on the public blockchain without a trusted third party, hence a Central Authority is introduced in order to maintain the voter's identity and allow only eligible voters to cast their votes. There are four voting phases in this protocol, namely

1. Initialization phase: The rules that govern the elections are established and a CA is chosen in this stage, and the blockchain and all other systems are also initialized. A list of eligible voters and a way to authenticate those users is provided to the CA. For the public signature scheme, a pair of signing and verifying keys will be generated among which the verifying key will be published as a parameter across the system. The initialization block of the blockchain will function as the genesis block. The initialization block contains information regarding the election set of valid nominations, it also includes the CA's signature validating key.
2. Preparation phase: In this phase, the voter is called upon to authenticate itself, using the e-voting platform's client application, to the CA. The CA checks the eligibility of a voter using the list of eligible voters and authentication information obtained from the initialization phase. Once the voter is considered eligible, a public key pair is generated by the voter's client, and its public counterpart is used as voter's pseudonymous identity, which also acts as verifying key.
3. Voting Phase: Every voter creates and delivers their vote to the network in this phase. A vote is considered as valid and is added in the block if and only if the voter has not previously casted his vote. For a vote to be valid, one must ensure that the ballot is validated by CA's signature and the predefined structure is adhered to by the vote. By using the alteration ballot, the voters can change or cancel their votes even after they have casted those votes. A ballot can be cancelled several times and the final ballot is considered in the count.
4. Counting Phase: In this phase, by broadcasting a ballot opening message consisting of their voter ID of the final vote to the network, the opening value of their vote commitment and a signature on both values, the voters are asked to reveal their final choice. The voters then broadcast the messages to their adjoining peers if the verification of signature is done and move ahead with inclusion of vote in their count. It is expected that, as all peers operate on the same blockchain, they should achieve the same result.

Protocol analysis was done to check whether the properties held true or not. It was seen that the protocol holds properties such as Eligibility, Privacy, Fairness, Verifiability both Individual and Universal.

## 2.2 IOT

IoT has officially defined as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies” [8].

Oscar et. al. [4], have demonstrated an approach with betterments in,

1. Mobility
2. Accessibility
3. Concurrency
4. Weight
5. Scalability
6. Transparency

When compared to other centralized system approaches. They have used Ethereum for the implementation. Their system consists of 6 main components:

1. Wireless Sensor Networks: A communication network used to get a constrained connectivity in limited power applications.
2. Managers: An entity that manages permissions to access IoT devices.
3. Agent Nodes: A node that looks after the deployment of smart contracts.
4. Smart Contracts: It is an integral part of the system that governs the access management system.
5. Blockchain Network: A private blockchain network.
6. Management Hubs: It is an interface that converts CoAP messages into JSON-RPC messages.

They have successfully addressed the scalability problems related to management access of billions of devices in IoT.

In order to validate and analyze it, they have created a proof of concept (PoC) implementation of the decentralized access control system.

Their program was built under a standardized genesis block in their very own private Ethereum network. As all the components of the prototype are more dimensioned to have more detailed outcomes than a public blockchain when testing the method, they preferred a private blockchain. The purpose of this implementation, though, was to deploy it in actual situations in public blockchains.

All administrators are externally managed accounts in this architecture, while the smart contract is deployed under a contract account.

In the smart contract, the restricted system data, manager data, and access control policy information are contained in two separate data structures.

The data structure that is used to hold the data is called Mapping. Mapping structures are identical to hash-tables where several possible keys are initialized from the beginning with the values. Mapping allows the combination of multiple forms of data to form a single type of data.

In order to interact with the Ethereum nodes using RPC calls, the interface utilizes the web3 JavaScript API and a CoAP JavaScript library called node-coap5 to bind to the IoT devices.

To automatically create a public/private key per computer, the LibCoAP was updated. The key is 20 bytes long and used to individually mark the machines in the managing scheme. A CoAP client and a CoAP server are being introduced by the library.

The studies in this analysis were conducted with an i7-950 processor clocked at 3.07GHz on an Ubuntu-16.04 laptop. They used Docker11 and an image named vertigo/ethereum12, which is derived from the client-go image of the Ethereum protocol ethereum/client-go golang implementation image. To render operating a private Ethereum network easier, Vertigo was also slightly updated. The IoT devices were running an updated LibCoAP library version on the same computer.

A benchmark instrument called CoAPBench13 that uses Californium14 as the reference for the execution of CoAP has been used. CoAPBench seems to be the only benchmark method usable for CoAP, to the best of the cited author's understanding.

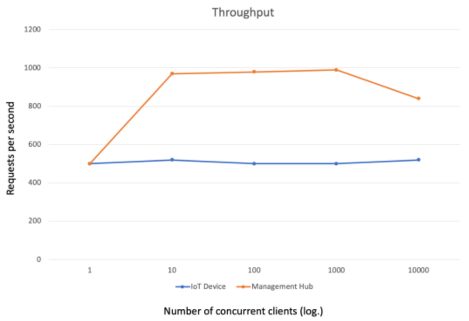

**Fig-2:** In a management hub and in an IoT system demanding the information from a management hub, throughput performed separately.

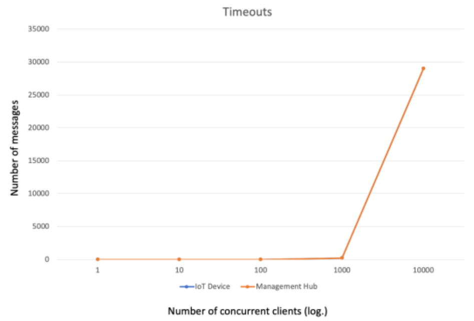

**Fig -3:** The total test timeout query messages conducted in Fig. 2.

*Fig -2 and Fig -3 display rough estimation based on the original work.*

Francesco et. al. [5], have discussed a Tweet-Chain model with the same level of anonymity degree as Blockchain. Their method is an alternative way for the implementation of public ledger. Their idea is to reinvent a consensus protocol with the use of tweets, wherein PoW and fees of miners has been substituted. This method overcomes the drawbacks of low computational power and storage capabilities and hence making it suitable for IoT purposes.

They have three performers: the Twitter social network, which gives registered users the ability to publish, check for and alert tweets; a welcoming profile W used it to introduce a kind of yellow page assistance; the Tweetchain group, including C, of users entering the Tweetchain protocol. By beginning from a password, a user constructs a SHA-256 hash chain [6] of length k to engage in the Tweetchain community. This chain would be used to keep all his timeline operations connected and unforgeable together.

They also found the system in a stable condition, which means that within the Tweetchain group there are indeed at least s = (2t)/(1-m) participants, where t and m are system parameters.

Registration: This move is carried out by a member x who wants to join the C group of Tweetchain. Obviously, the regular subscription to Twitter to construct a profile on it is a precursor.

Therefore, in a join- first chronology, W includes at least one tweet per member. At this stage, x randomly produces the Fx set of follow-ups chosen for future confirmation of its transactions.

The Fx set is compiled as follows:

- x seeks the identifier for his Twitter. (Each Twitter handle has a 64-bit identifier.)
- The identifier is used to produce random numbers as a seed for a public PRNG. Say n, n mod w is determined for each generated number, where w is the total amount of tweets posted by W (corresponding to the Tweetchain community's size).
- The numbers thus acquired are utilized as indices to pick W's different profiles.
- At this stage x sends each of the accounts a private message telling them to join him.
- Each of the approached accounts adds the following link to x by checking the validity of the message arriving from x by using the group PRNG, and copies the welcome tweet of W by modifying #HCWi with its current hash chain feature.

Generation of transactions: This is the procedure carried out to establish a new transaction. Similar to Blockchain, numerous data are used in each transaction:

- A transaction timestamp,
- A payload, i.e. the essence of the transaction,
- A transaction with input.
- A collector of sales, which is a goal profile.

The production in this procedure of a new transaction relates to the uploading of a user's latest tweet. This tweet is called t- tweet.

Verification: This procedure has been used to validate a transaction's legitimacy. The checking of a transaction material is not recognized by this procedure. It is indeed solely connected to the intent of the contract, which is entirely reliant on the application and orthogonal to the proposal.

They designed a Java prototype incorporating this method, and all the tests were carried out on a 4.0 GHz Intel I7 Processor personal computer with 8 GB of RAM. As far as the applications adopted, Ubuntu 16.10 operating system was fitted with JDK, Apache and Tomcat servers.

In brief, the time needed for a t-tweet to be checked was 13.5. Thus, success of this approach is greater than the state of the art. Perhaps in Blockchain, the corresponding period is around 10 minutes (it relies on the fee paid), while in Ethereum, in the best scenario, it is around 15 seconds (i.e. just when the evidence of involvement is deemed critical).

Ali et. al. [7], have exhibited an approach aimed at security of IoT devices in a smart home scenario with the use of blockchain. Their approach consists of the following tiers:

1. Cloud Storage,
2. Overlays,
3. Smart Home.

Each smart home consists of a miner that is responsible for handling communications within and outside the home. Each miner is always online and high resourced. These miners are responsible for the preservation of privacy and security of a blockchain. They have effectively shown a secure framework through a thorough analysis of confidentiality, availability and integrity.

### 2.3 Supply Chain Management

A supply chain is a nexus between companies and its suppliers to manufacture and distribute to the final customer a particular product. Diverse individuals, organisations, activities, resources and information are included in this nexus. Product development, distribution, marketing, finance, operations and customer service are the main functions that are carried out in a supply chain. The management of flow of goods and services can be defined as Supply chain management, and it involves different processes right from production of a product from raw materials to the finished product. For a quicker production cycle and lower costs of an advanced supply chain, supply chain management is an important process. Supply chain management generally operates centrally, it helps the businesses to cut excess production costs and ensure faster delivery [9]. Blockchain, when introduced in the supply chain, can help bring transparency, traceability, reduce risk and administrative costs, and help businesses to flourish. Some other benefits of implementing supply chain on blockchain are decrement in losses due to counterfeit market trading, reduction in paper work, improvement in credibility and trust, stakeholders engagement, etc. [10].

According to [11], the three use cases of blockchain in supply chain management are, 1)Traceability: By mapping and visualising business supply chains, traceability enhances operational efficiency. Blockchain can ensure the engagement between companies and consumers with immutable, verifiable data; 2)Tradeability: Tradeability is a special offering of blockchain that redefines the idea of the traditional marketplace. An asset can be tokenized by separating an object into shares that digitally delineate ownership using blockchain. These tokens can be transferred from one person to another and thus the ownership; 3)Transparency: By recording important data points like claims and certifications transparency establishes trust and then this data is made publicly accessible.

Some supply chain startups like Provenance use blockchain for tracking responsible tuna sourcing in

Indonesia [12], and Monegraph uses blockchain to protect the use and distribution of digital media rights and allow revenue sharing among distributors, publishers, and media creators. Skuchain develops a trade and supply chain finance products, based on blockchain, that aims towards the 18 trillion USD finance market that includes various individuals like sellers, buyers, customs, banks, logistic providers and third parties [13]. Guido et. al. [14], have integrated current literature while filling the lacking concerns of the digital strategy. They have created a standard methodology to design blockchain technology that aren't related to financial applications. They have also presented the resulting use case in fresh food delivery. Their paper has been aimed at reduction of logistical costs and operation optimizations. Sara et. al. [15], have examined the significance of smart contracts and their applications in supply chains. They have identified the importance of blockchain for sustainability of supply chains. They have discussed the common problems faced by organizations in implementation of blockchain and have stated possible solutions to those. They have acknowledged a scope of future work in blockchain technology in supply chain management.

### 2.4 Identity Management

We are often asked to provide the proof of our identity to prove that we are who we say we are but often we tend to share personal information that is not asked. For example, providing a driver's license as identity proof may provide the other party with sensitive information like address, eye colour, height, hair colour. This information can be used to steal one's identity. Identity theft i.e. uncertified access to one's personal information is a serious crime and it has impacted many people's lives in this digital era. The identity verification systems used nowadays lack the ability to secure data till some extent. The online identity authentication mainly depends on password and in rare cases dual-factor authentication is used. The huge drawback of password based authentication is that the passwords are extremely insecure while dual-factor authentication generally uses one time password or a third party for authentication. Blockchain can be used to overcome the drawbacks of the traditional authentication system because of its decentralized nature. The data can be stored in a distributed ledger that makes the data more secure and hard to breach. As the ledger is shared it becomes nearly impossible for an attacker to breach the data as he would have to breach every member's machine and alter the data [16].

Cresitello-Dittmar [16] reviewed the techniques used by companies such as Blockstack and Tierion for identity verification and management. Blockstack uses handshake based on blockchain, this handshake tests the authenticating app and user and the third party. The first step of this handshake is an authentication request which is generated when the user tries to login to the protected app. In this step, the user, instead of being prompted to enter password, will see a form for the username on the protected app then a QR code for authentication will be displayed or any alternate method for authentication will be deployed. The verification of the request and sending a response is the next step of the handshake. In order to ensure authentication, this step includes several steps. With the help of public key cryptography, the user can validate the legitimacy of the request. This will permit the protected application to sign the request, which is then publicly validated by either the blockchain or the certificate authority. The verify login button will be prompted to the user after the verification of request. The request is then generated and signed by the user and then it is sent back to a predefined path on the protected app. The user will be logged in after the protected app validates this request using public key cryptography. Tierion uses cryptographic hashing for sharing only the required information. The user sends a data packet which consists of relevant information to the website that asks for identity proof, this packet is hashed and signed by the user. This website then searches for the hashed and signed type of the data on the blockchain. The website will know that the data is actually affiliated with the individual and the data is totally non-tampered, assuring that the information is provided by the legit user, if the hashes match the signatures. An exhaustive, secure and distributed system can be established for the authentication and verification of identity by applying the concepts employed by Blockstack and Tierion.

Jamal et. al. [17] proposed a Identity system based on blockchain that stores the personal information of a person on the blockchain. The security attributes of blockchain are employed in this system so that the people know who has access to their data. There are three user categories under this new system, such as: user, authority and a third party. Each of these entities have specific functionality, a user can permit the third party to access its data and also see the list of requesters; the personal details of a user can be uploaded by the authority on the blockchain; and the request to access the user's data is sent by the third party. They designed their system using Agile Unified Process for development purposes. The implementation was carried out in four phases. In the Initial phase, determination of key elements, security risks and inefficiencies of the existing model were scrutinized, the constraints and scope of the system were determined. In the second phase, the system design, on the basis of six Unified Modelling Language diagrams, was drafted. In the third phase, Android 3 and Microsoft Visual Studio Code were used to build the system as it is both mobile and web application. In the final phase, the system testing as well as acceptance testing was carried out, in order to verify the functionality of the proposed system; total 18 case scenarios were tested. The acceptance testing was carried out on three main basis namely, 1) Prefer online verification, 2) Ease of verification, and 3) Availability to all. Out of 141 respondents 65 preferred online verification, 116 corroborated that the system provides ease of verification, and 109 respondents had a positive response on making the system available to everyone. They concluded that the system, when implemented on real blockchain, would provide an efficient way of handling identity.

Liu et. al. [18] proposed a Ethereum blockchain based identity management system. They combined identity authentication and reputation management together and stored the personal information in the blocks. As blockchain is completely decentralized in nature the data stored is secure. They have used solidity programming, Truffle which is a smart contract framework, and Testrpc which is a blockchain development environment. They have deployed this system on a small scale blockchain, consisting of 10 users, for demonstration purposes. The system proposed is quite unique as it has identity authentication and reputation management modules. The assurance that real world entities can only create virtual identity on the system, by enabling the identity to correlate with the Ethereum public key, is the main aim of the identity authentication module. Whereas, the aim of the reputation management module is to monitor the behavior of an individual on the system. The authentication model consists of two parts: 1) Identity creation and 2) Identity modification. As one can create many Ethereum public key addresses and if the system identity is considered to be this public key address then the attacker can manipulate the reputation results. Hence Identity creation module is essential as only a real world entity can have a virtual identity. In this module, the user has to upload their personal information, after this an unique public key and an unique ID is assigned to the user. The identity of the user in the system consists of Ethereum public key, user ID and RpCoin; the RpCoin is the token that cannot be transacted or transferred among users in any way. In the Identity modification module, if the user updates his personal information the system implements the transformation of RpCoin so that the user's reputation remains unaffected; it is taken into account that multiple identities are not formed. Hence, when a user updates his personal information a new ID is created and an old ID is still maintained in the blockchain. Another type of identity modification can happen when the user requests to change the Ethereum public key address, in this case, a new Identity is generated and the old address is stored in the blockchain. The identity information and RpCoin are transferred from old identity to the new. In the Reputation model, the representation of one's behaviour on the system is it's reputation. RpCoin is used in the reputation task and incentive task. The reputation task aims at defining a user's reputation, and it consists of crowdsourcing tasks that have binary options. The publishing stage and consensus stage are the two stages of the reputation task. The publisher generates a task and publishes it to the users of the network. The consensus stage begins after the number of participants satisfies the minimum number requirement defined by the network. In the consensus stage, the participating user votes the tasks they agree to do and the tasks that have no votes are abandoned. The incentive task is a special type of task used to avoid the undesirable behaviour of participants, it can be created by any user. The Undesirable behaviour of participants are of two types 1) Negative worker i.e. users who provide fallacious votes, and 2) Repetitive task i.e. the publisher publishes the same task multiple times. They introduced a new concept named RpCoinDay using RpCoin. It is a criterion that determines the number of days the user holds a RpCoin. They also proposed a new concept named reputation fluctuation factor that is used to record user's RpCoinDay collection process. They concluded after demonstrating viability of the proposed system by performing experiments and proving that the experiments validate the proposed system.

## 3. CONCLUSION

Hereby we have successfully reviewed a few applications of Blockchain like Voting mechanism, IOT, Supply chain and Identity management and we conclude that, even if blockchain technology provides a solution to the drawbacks of above applications, it cannot be considered completely reliable. As the implementation of many applications requires third party authority, to some extent, it contradicts the decentralized nature of blockchain. However, blockchain possesses certain properties like transparency, security, traceability, tradeability, privacy and data auditability, and when harnessed in the proper direction it can bring about major change in the technical world.

## 4. FUTURE SCOPE

Blockchain being in its early stages and having a very few applications explored, that too with no proper implementations as of the date of writing, we see a large scope for the rise of new innovations and ideas in the future.

## REFERENCES

1. W. Zhang et al., "A Privacy-Preserving Voting Protocol on Blockchain," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 401-408, doi: 10.1109/CLOUD.2018.00057.
2. F. Sheer Hardwick, A. Gioulis, R. Naeem Akram and K. Markantonakis, "E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1561-1567, doi: 10.1109/Cybermatics_2018.2018.00262.
3. K. Li, H. Li, H. Hou, K. Li and Y. Chen, "Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain," 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Bangkok, 2017, pp. 466-473, doi: 10.1109/HPCC-SmartCity-DSS.2017.61.
4. O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, April 2018, doi: 10.1109/JIOT.2018.2812239.
5. Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. 2017. Overcoming Limits of Blockchain for IoT Applications. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 26, 1–6. doi:https://doi.org/10.1145/3098954.3098983
6. Faye, Y., Niang, I. and Noel, T., 2011. A Survey of Access Control Schemes in Wireless Sensor Networks. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 5, pp.1254-1263.
7. A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 618-623, doi: 10.1109/PERCOMW.2017.7917634.
8. Atlam, H., Alenezi, A., Alassafi, M. and Wills, G., 2018. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. I.J. Intelligent Systems and Applications, 6, pp.40-48.
9. Investopedia. 2020. Supply Chain Management (SCM): What You Need To Know. [online] Available at: <https://www.investopedia.com/terms/s/scm.asp>.
10. Using Blockchain to Drive Supply Chain Transparency and Innovation", Deloitte United States, 2020. [Online]. Available: https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html#:~:text=Blockchain%20can%20enable%20more%20transparent,or%20use%20by%20end%20user.
11. Blockchain in Supply Chain Management | ConsenSys", ConsenSys, 2020. [Online]. Available: https://consensys.net/blockchain-use-cases/supply-chain-management/.
12. From shore to plate: Tracking tuna on the blockchain", Provenance, 2020. [Online]. Available: https://www.provenance.org/tracking_tuna_on_the_blockchain.
13. Skuchain Developing Blockchain Solutions for $18 Trillion Trade Finance Market With Funding From Amino, DCG, and FBS Capital", Prnewswire.com, 2020. [Online]. Available: http://www.prnewswire.com/news-releases/skuchain-developing-blockchain-solutions-for-18-trillion-trade-finance-market-with-funding-from-amino-dcg-and-fbs-capital-300214205.html.
14. G. Perboli, S. Musso and M. Rosano, "Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases," in IEEE Access, vol. 6, pp. 62018-62028, 2018, doi: 10.1109/ACCESS.2018.2875782.
15. S. Saberi, M. Kouhizadeh, J. Sarkis and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management", International Journal of Production Research, vol. 57, no. 7, pp. 2117-2135, 2019. Available: 10.1080/00207543.2018.1533261.
16. B. Cresitello-Dittmar, "Application of the Blockchain for Authentication and Verification of Identity", 2016.
17. A. Jamal, R. A. A. Helmi, A. S. N. Syahirah and M. -A. Fatima, "Blockchain-Based Identity Verification System," 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 2019, pp. 253-257, doi: 10.1109/ICSEngT.2019.8906403.
18. Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan and S. Wang, "An Identity Management System Based on Blockchain," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, 2017, pp. 44-4409, doi: 10.1109/PST.2017.00016.
19. What Is Blockchain Technology? How Does It Work? | Built In", Builtin.com, 2020. [Online]. Available: https://builtin.com/blockchain.