# BLOCKCHAIN TECHNOLOGY: A CRITICAL REVIEW AND ITS PROPOSED USE IN E-VOTING IN INDIA

Mehtab Alam[a], Dr. Ihtiram Raza Khan[b], Dr. Safdar Tanweer[b]
[a] Jamia Hamdard, New Delhi-110062, India
[b] Assistant Professor, Jamia Hamdard. New Delhi-110062, India

**Abstract:** In 2009, the evolution of the blockchain technology was the foundation of the first ever cryptocurrency, bitcoin. It not just changed the financial industry but also proved to be a major break-through for peer-to-peer data transfer, information exchange having high security, efficiency, and transparency. Blockchain is a database of records which is distributed on the network, or we can say, its a public ledger of all transactions that have executed and are shared between every user on that blockchain network. Some of its characteristics include anonymity, irreversibility, immutability, decentralization and persistence. It has found applications and use in almost all fields which require data sharing but with secure authentication, anonymity and permanence. Some of the areas of its application are finance, real-estate and IoT. In this paper we discuss the blockchain technology and its fundamentals, its working, types of blockchain, applications, advantages, disadvantages and some other aspects in details.

In this research paper, we introduce a model of e-voting as a CASE study which is developed in decentralised environment on the Ethereum blockchain.

Using the concept of Blockchain, e-voting will assist to strengthen security and integrity of the election system reducing the cost while increasing the privacy. The use of encryption helps to provide security to the system. No intruder can gain access to the voting system and tamper it and in this way, EVMs can't be accused of being fixed.

**Keywords: Blockchain, cryptography, hash, transaction, digital information, digital signature, peer-to-peer, e-voting, Ethereum, EVM**

## I. INTRODUCTION

Blockchain is truly one of the many emerging technologies. A blockchain, is a list of records which keeps on growing as new data is added, called blocks, which are linked using cryptographic algorithms. Each block contains a cryptographic hash value of the previous block, a timestamp, and transaction data, and a hash for its own complete block, making it like a linked chain. This paper presents in-depth knowledge of blockchain technology, its advantages, disadvantages, uses and future prospects.

## II. BLOCKCHAIN

Blockchain, at its most key level, is literally just a chain of interconnected blocks [1][2]. Block resembles digital information and chain resembles the block stored in a database which is public. Blockchain does not do anything unless it is paired with a solid use case where it works as a sort of Trust-as-a-Service (TaaS) [3] to all the participants.

Blocks on the blockchain contain digital pieces of information [4]. Specifically, they have three parts:

- Blocks of a blockchain store information about the transactions, for example, the date, time, and the cost of the most recent purchase made online.
- Blocks also store the information about who are the participants of the transactions. A blockchain block for an

online shopping environment would record buyers name along with the online website, the cost of the item purchased etc. the purchase is recorded and saved using a unique "digital signature" [5].

- Blocks also store information that would distinguish them from other blocks on any given network. Each block stores a "hash value" [6] which is a unique code for every block. For example, if someone purchases a particular item twice, but, in different orders, even though the details of both the transactions would look nearly identical to each other, they can still be identified and recognized as different blocks because of their unique hash values.

A single block on the blockchain can store up to 1 MB of data [4][7]. Depending on the size of the transactions taking place on the blockchain, a single block can store up-to a few thousand transactions.

## III. WORKING OF BLOCKCHAIN

Whenever a block has some new data to store, it is added to the end of the blockchain. Blockchain, as we know, consists of multiple blocks put together in form of a chain. To add a new block to the blockchain, four things must take place [4]:

i. **A transaction must occur**. To simplify the understanding, let's take for example an online purchase is made.

ii. After a purchase (transaction) is made, **the transaction must be verified**. For example, the public records of information, such as, Wikipedia, there's someone in charge of vetting new data entries. But in blockchain network, this job is left up to a network of computers. These networks often consist of thousands or more computers spread across the globe. When a purchase is made, that network of computers rushes to check whether the transaction happened in the way it was supposed to be done. In other words, they confirm the details of the purchase, including the transaction's time, amount, and the participants.

iii. That **transaction must be stored in a block**: After the transaction has been verified as accurate, and complete, it goes to the next step. The transaction's amount, digital signature of both the parties (seller and buyer in our example), are stored in a block. Here, the transaction is likely to be joining hundreds, or thousands, of other transaction like itself.

iv. That **block must be given a hash**. Once all the transactions of a block have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the previous block that was the most recent block added to the blockchain. Once the hash value is generated, the block can be added to the blockchain.

The block becomes publicly available for anyone to view, as soon as, it is added to the blockchain.

## IV. BLOCKCHAIN CAN BE PUBLIC/PRIVATE BUT VERY SECURE

Anyone can view the contents of the blockchain. Users can opt to connect their computers to the blockchain network. If they do so, their computer system receives a copy of the blockchain that is updated automatically whenever a new block is added to the blockchain, it is kind of like a Facebook News Feed that updates whenever a new status or post is posted [4].

Each computer in the blockchain network has its own copy of the blockchain, which means that there are thousands or millions of copies of the same blockchain [8]. Each copy of the blockchain is identical, spreading new information across a network of computers makes the

information more difficult to manipulate. With blockchain, there is not a single, definitive account of events that can be manipulated. Rather, the hacker would need to manipulate/edit every copy of the blockchain present on the network.

Blockchain technology elucidate the issues of security and trust in several ways. First, new blocks are stored linearly and chronologically always. That means, they are added to the end of the blockchain. It is very difficult to go back and alter the contents of the block once a block has been added to the end of the blockchain, that is so since each block contains its own unique hash, along with the hash of the block situated before it. Hash codes are created by a mathematics function that converts digital information into a string of numbers and/or letters. If the hashed information is edited in any way, the hash code changes as well.

Hash is very important for the security of blockchain. If a hacker or an intruder attempts to edit the transaction. As soon as they edit information of the transaction, the block's hash will change. The next block in the chain will still contain the old hash, so to cover their tracks, the hacker would need to update that block also. Doing so would change that block's hash. And the next, and so on [4].

In order to change a single block, the hacker would need to change every single block after it on the blockchain. Recalculating all the altered hashes would take an enormous, huge and improbable amount of computing power. In short, once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.

## V. TYPES OF BLOCKCHAIN

At present there are roughly three types of blockchain networks [9]

i. **Public blockchains**

A public blockchain has no access restrictions. Anyone with an internet access can send transactions to a public blockchain as well as become a validator [10]. These networks offer economic incentives to the users. Bitcoin and Ethereum are most known public blockchain networks.

ii. **Private blockchains**

A private blockchain is a one that is permissioned.[11] Unless invited by the administrators, one cannot join it. Participant and validator access are restricted.

Private blockchains can be used as a middle-ground for companies and industries that are interested in the blockchain technology but are not very comfortable with the level of control offered by public networks. They might wish to incorporate blockchain into their record-keeping and accounting systems without removing autonomy and having the risk of exposing their sensitive and private data to the internet that is public.

iii. **Consortium blockchains**

A consortium blockchain is also referred as semi-decentralized. It is permissioned, but instead of a single organization/industry controlling it, a number of companies operate a particular node on consortium network. The administrators restrict users' reading rights as required and allow only a limited number of trusted nodes to execute and run a consensus protocol.

Table 1: Comparisons between public, consortium and private blockchain [9].

| Property | Public Blockchain | Consortium Blockchain | Private Blockchain |
|---|---|---|---|
| Consensus Determination | All connected Miners | Select number of Nodes | Single Organisation |
| Read Permission | Public | Could be public as well as Restricted | Could be public as well as Restricted |
| Immutability | Almost impossible to tamper | Could be Tampered with | Could be Tampered with |
| Efficiency | Low | High | High |
| Centralized | No | Partial | Yes |
| Consensus Process | Permission less | Permissioned | Permissioned |

## VI. APPLICATIONS OF BLOCKCHAIN

There are currently a number of uses of blockchain technology. Some of them are discussed below [4][12][13]

### i. Banks

Banking sector is set to gain the most benefits by integrating blockchain into its business operations, as of now. Financial offices operate during business hours, five days a week. That is if someone deposits a cheque on Friday at 6 p.m., or any other day that is a bank holiday, ie. the bank sleeps, he/she will have to wait until Monday or the next working day to see the amount in his/her account. Even if the deposit Is made during the normal business hours, the transaction takes 1-3 days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, in contrast, never sleeps. By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes, ie. the time it takes to add a block to the blockchain, regardless of the time or day of the week, be it a bank holiday or non-working hours. In the stock trading business also, with the use of blockchain the settlement and clearing process can be done quickly.

### ii. Cryptocurrency

Blockchain forms the bedrock for cryptocurrencies like Bitcoin. Currencies like the Indian Rupee are regulated and verified by a central authority, ie. a bank or government. Under a bank or government, a user's data and currency are technically controlled and governed by them. If a bank shuts down or collapses or the people reside in a country with an unstable government, the expected value of their currency may be at risk at all times. These were the worries out of which Bitcoin was crafted. Blockchain allows Bitcoin and other numerous cryptocurrencies to operate without the need for a central authority, by spreading its operations across a network of computers. Apart from reducing the risk, it also, eliminates the processing fees, transaction fees and delays that takes place in fund transfers. It also helps the people get a more stable currency in countries with unstable currencies. It also provides with more applications and a wider network of groups and individuals and institutions they can conduct business with, in both domestic and international market.

### iii. Healthcare

Health care providers can use blockchain to securely store their patients' medical records. Once a medical record is created and signed, it can be added to the blockchain, it would provide patients with proof and assurance that their record and reports are fixed and cannot be changed or altered with. The personal health records will get encoded and stored on the blockchain using a private key, so that they will be accessible by only select individuals, ensuring privacy of the records.

**iv. Property Records**

Blockchain for record keeping has the potential to eliminate the need for submitting and scanning documents and tracking down physical files and signatures in a local recording office. If property ownership is stored and verified on the blockchain, owners can rest assured that their data is accurate and permanent.

**v. Supply Chains**

Blockchain can be used by the suppliers to record the origins of materials and items that they purchase. This would allow companies to track their products while in transit. It will help them verify the authenticity of their products, along with health and ethics labels like "Organic," "Local," and "Fair Trade."

**vi. Voting**

Blockchain in voting carries the potential to eradicate election fraud and thereby increasing voter turnout. Each vote casted would be stored as a block on the blockchain with a unique hash, making them nearly impossible to tamper or alter with. The blockchain software and the protocol would maintain transparency, and at the same time keeping personal identity of the voter undisclosed. It might also provide officials with instant results, if required.

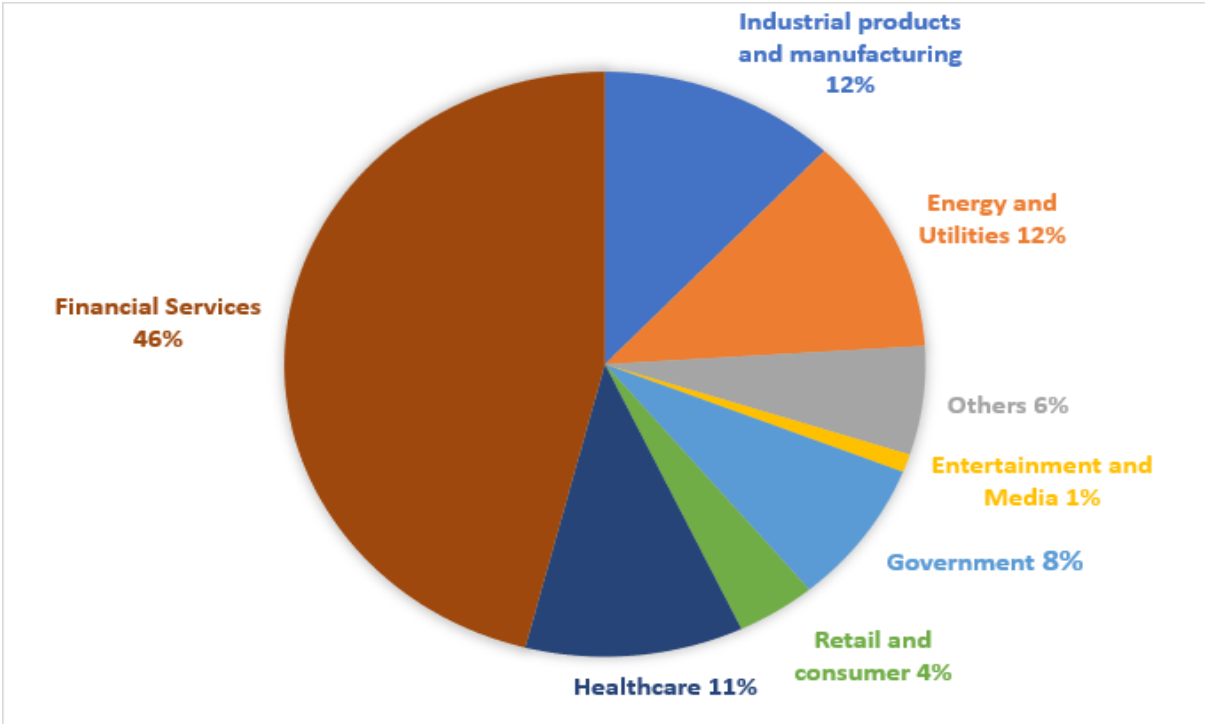


Figure 1: Blockchain in various industries [14]

## VII. ADVANTAGES OF BLOCKCHAIN

Blockchain's offers a decentralized form of record-keeping without limit. From increased user privacy and stronger security, to decreased processing fees and fewer to non-errors, blockchain technology may very well see applications beyond those mentioned above. In this section we discuss some of the advantages of blockchain technology [4][15][16].

i. **Accuracy**

Transactions on the blockchain network are always approved by thousands or millions of computers on the network. This simplifies verification process and removes all human involvement, resulting in a more accurate record of information and less to none human error.

ii. **Cost**

In general, consumers pay a bank to verify a transaction, a notary to sign a document

and for using other services. Blockchain eliminates the need for third-party verification and their associated costs. Companies charge a small fee whenever they accept payments using credit cards, because banks have to process those transactions. Bitcoin, on the other hand which uses blockchain technology, does not have a central authority and has virtually no transaction fees.

iii. **Decentralization**

Blockchain does not store any of its information in any central location. The blockchain is copied and distributed across a number of computers on the network. As soon as a new block is added to the blockchain, all the computers on the network update their blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes more difficult to tamper with or lose due to hardware failure. If a hacker gets a copy of the blockchain, only a single copy of information is compromised instead of the entire network.

iv. **Efficiency**

Transactions placed through a central authority can take up to a few days to settle due to the huge load on the central authority. As discussed above about a cheque deposit on a Friday evening, one may not actually see funds in the account until Monday morning. Financial institutions operate during the normal business hours, only five days a week, blockchain, on the other hand, is working 24 hours a day, seven days in a week. Transactions get completed in about ten minutes or less and within a few hours, can be considered secured.

v. **Privacy**

Most of the blockchain networks transactions operate as public databases that anyone with an active internet connection can view as a list of the network's transaction history. Every user can access details about the transactions, but they cannot access identifying information about the users making those transactions. It is a common misconception that blockchain networks are anonymous. They are not anonymous but only confidential. That is, when a user makes a transaction, their unique code called a public key, is recorded on the blockchain, instead of their personal information. Even though a person's identity is still linked to their blockchain address, hacker cannot obtain a user's personal information.

vi. **Security**

As soon as a transaction is recorded, the authenticity of the record must be verified by all the computers on the blockchain network. Thousands or millions of computers on the blockchain rush to confirm that the details of the transaction are correct. Once a computer has validated the transaction, a block with all the relevant information is added to the blockchain. A unique hash is present in every block on the blockchain, along with the unique hash of the block before it. When the information on a block is edited in any way, that block's hash code changes, but, the hash code on the block after it would not. This inconsistency makes it very difficult for information on the blockchain to be changed or altered without notice.

vii. **Transparency**

The blockchain technology is almost always open source. In this, the users on the blockchain network can modify the code as they see fit, as long as they have a majority of the network's computational power. Keeping data on the blockchain open source, makes tampering with data much more difficult. With more than millions of computers on the blockchain network at any given time, it is very unlikely that anyone could make a change without it being noticed.

## VIII. PROPOSED SYSTEM

This section introduces the e-voting solution we are suggesting, explains the chosen decentralised blockchain platform.

We highlight the architecture of the proposed voting system and explain the smart contracts that were deployed on the Ethereum blockchain. the interface, API and functionalities that are implemented; and lastly, it describes the encryption server, explaining how it can ensure the privacy of the vote.

**Blockchain Platform**

The chosen blockchain platform was Ethereum. The advantages of this blockchain platform include a suitable protocol for developing decentralized applications, by building a blockchain with a built-in turing-complete programming language (Solidity), allowing users to write smart contracts with their own rules for transactions formats, rules for ownership and state transitions functions. Moreover, Ethereum is a public blockchain which philosophy is based on principles that are considered ideal to electronic voting systems.

**Decentralized Application**

This implementation consists of an HTML interface for the application users, a cryptographic server that will encrypt/decrypt the votes, three contracts deployed on the Ethereum blockchain that are coded in the Solidity language and an API to act as a bridge between all the components mentioned before. The architecture of the system is represented in Figure 2.

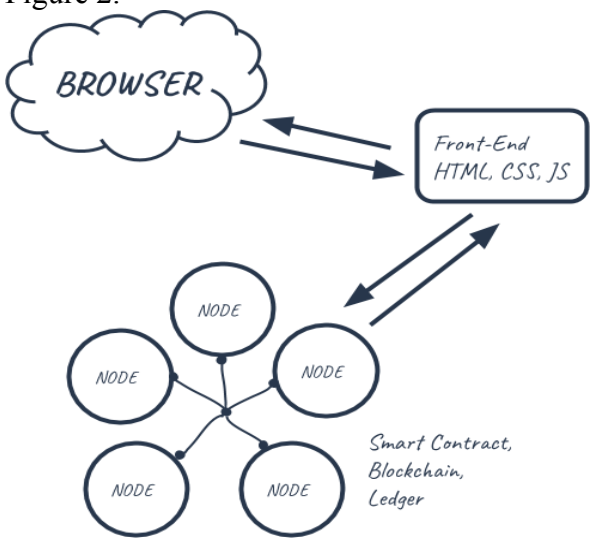


Fig 2: Proposed system Architecture [18]

The user interface is a simple HTML page that allows users to access the functionalities of the application. The API is responsible to react to actions made on the interface and interact with the encryption server and the blockchain. For each request made in the interface, it will interact with the encryption server by server calls to encrypt, decrypt or add votes. To interact with the blockchain, transactions or web3.eth.calls are used, in order to store or retrieve information, respectively.

## IX. CONCLUSION

Businesses around the world are speculating about the technology and its capabilities and where it's headed in the years to come. As being a hot topic nowadays, blockchain promises to make business, government operations and organizational work more accurate, efficient, and secure. Blockchains has the potential to transform traditional industry and organizations with its key characteristics: persistency, anonymity, decentralization and auditability.

In this paper, we presented a complete overview on blockchain. We first presented an overview of blockchain technologies including working of blockchain and its security aspect. We then discussed the types of blockchain. We tried to eliminate the myth about blockchain and bitcoins are the same thing. We included a few global surveys presenting the integration of blockchain in businesses and organizations. Further we listed some of its applications, advantages and disadvantages.

Nowadays applications based on blockchain are coming up and we are determined to conduct an in-depth investigation on blockchain based applications in the near future.

This paper uses e-voting as a model and CASE study which involves the use of Ethereum blockchain in a decentralized

environment. We finally conclude that the blockchain is a good technology for improvements in voting systems in our country. Due to distributed peer to peer framework, it guarantees the security and avoids the risk of hacking.

## REFERENCES

[1] https://en.wikipedia.org/wiki/Blockchain

[2] D. Yaga, P. Mell, N. Roby, K. Scarfone, "Blockchain Technology Overview" in Draft NISTIR 8202 NIST, January 2018.

[3] Talal H. Noor , Quan Z. Sheng, Trust as a service: a framework for trust management in cloud environments, Proceedings of the 12th international conference on Web information system engineering, October 13-14, 2011, Sydney, Australia

[4] https://www.investopedia.com/terms/b/blockchain.asp

[5] T. Huynh, T. Tru Huynh, D. Pham and A. Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain", 2018 International Conference on Advanced Technologies for Communications (ATC), 2018. Available: 10.1109/atc.2018.8587428 [Accessed 18 March 2019].

[6] https://blockgeeks.com/guides/what-is-hashing/

[7] https://www.blockchain.com/charts/avg-block-size?

[8] D. Puthal, N. Malik, S. Mohanty, E. Kougianos and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems", IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6-14, 2018. Available: 10.1109/mce.2018.2816299.

[9] V. Buterin, “On public and private blockchains,”2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[10] "How Companies Can Leverage Private Blockchains to Improve Efficiency and Streamline Business Processes". Perfectial.

[11] Bob Marvin (30 August 2017). "Blockchain: The Invisible Technology That's Changing the World". PC MAG Australia. ZiffDavis, LLC. Archived from the original on 25 September 2017. Retrieved 25 September 2017.

[12] https://blockgeeks.com/guides/blockchain-applications/

[13] https://www.blockchaintechnologies.com/applications/

[14] https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html

[15] https://www.entrepreneur.com/article/306420

[16] https://www.fool.com/investing/2017/12/11/5-big-advantages-of-blockchain-and-1-reason-to-be.aspx

[17] https://www.coindesk.com/information/blockchains-issues-limitations

[18] Architecture of Blockchain http://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial