**MICRO PROJECT**

**FOUNDATION OF BLOCKCHAIN**

**(4361603)**

: Do a feasibility analysis on Vote chain – Electronic Voting System based on Blockchain and prepare a detailed plan to create the system.



R.C. TECHNICAL INSTITUTE,SOLA,AHMEDABAD

SUBMITTED BY:

SHAH CHAITYA .T.(216400316018)

UNHAVNE MARUT .C.(216400316016)

**INTRODUCTION:-**

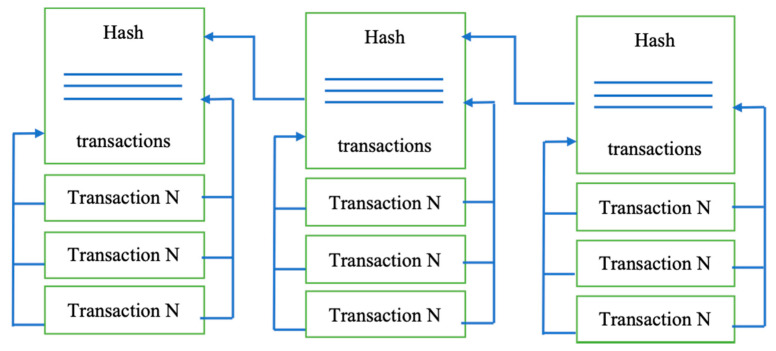
* Electoral integrity is essential not just for democratic nations but also for state voter’s trust and liability. Political voting methods are crucial in this respect. From a government standpoint, electronic voting technologies can boost voter participation and confidence and rekindle interest in the voting system. As an effective means of making democratic decisions, elections have long been a social concern. As the number of votes cast in real life increases, citizens are becoming more aware of the significance of the electoral system [[1](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B1-sensors-21-05874),[2](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B2-sensors-21-05874)]. The voting system is the method through which judges judge who will represent in political and corporate governance. Democracy is a system of voters to elect representatives by voting [[3](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B3-sensors-21-05874),[4](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B4-sensors-21-05874)]. The efficacy of such a procedure is determined mainly by the level of faith that people have in the election process. The creation of legislative institutions to represent the desire of the people is a well-known tendency. Such political bodies differ from student unions to constituencies. Over the years, the vote has become the primary resource to express the will of the citizens by selecting from the choices they made [[2](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B2-sensors-21-05874)].
* The traditional or paper-based polling method served to increase people’s confidence in the selection by majority voting. It has helped make the democratic process and the electoral system worthwhile for electing constituencies and governments more democratized. There are 167 nations with democracy in 2018, out of approximately 200, which are either wholly flawed or hybrid [[5](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B5-sensors-21-05874),[6](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B6-sensors-21-05874)]. The secret voting model has been used to enhance trust in democratic systems since the beginning of the voting system.
* It is essential to ensure that assurance in voting does not diminish. A recent study revealed that the traditional voting process was not wholly hygienic, posing several questions, including fairness, equality, and people’s will, was not adequately [[7](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B7-sensors-21-05874)] quantified and understood in the form of government [[2](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B2-sensors-21-05874),[8](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B8-sensors-21-05874)].
* Engineers across the globe have created new voting techniques that offer some anti-corruption protection while still ensuring that the voting process should be correct. Technology introduced the new electronic voting techniques and methods [[9](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B9-sensors-21-05874)], which are essential and have posed significant challenges to the democratic system. Electronic voting increases election reliability when compared to manual polling. In contrast to the conventional voting method, it has enhanced both the efficiency and the integrity of the process [[10](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B10-sensors-21-05874)]. Because of its flexibility, simplicity of use, and cheap cost compared to general elections, electronic voting is widely utilized in various decisions [[11](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B11-sensors-21-05874)]. Despite this, existing electronic voting methods run the danger of over-authority and manipulated details, limiting fundamental fairness, privacy, secrecy, anonymity, and transparency in the voting process. Most procedures are now centralized, licensed by the critical authority, controlled, measured, and monitored in an electronic voting system, which is a problem for a transparent voting process in and of itself.
* On the other hand, the electronic voting protocols have a single controller that oversees the whole voting process [[12](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B12-sensors-21-05874)]. This technique leads to erroneous selections due to the central authority’s dishonesty (election commission), which is difficult to rectify using existing methods. The decentralized network may be used as a modern electronic voting technique to circumvent the central authority.
* Blockchain technology offers a decentralized node for online voting or electronic voting. Recently distributed ledger technologies such blockchain were used to produce electronic voting systems mainly because of their end-to-end verification advantages [[13](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B13-sensors-21-05874)]. Blockchain is an appealing alternative to conventional electronic voting systems with features such as decentralization, non-repudiation, and security protection. It is used to hold both boardroom and public voting [[8](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B8-sensors-21-05874)]. A blockchain, initially a chain of blocks, is a growing list of blocks combined with cryptographic connections. Each block contains a hash, timestamp, and transaction data from the previous block. The blockchain was created to be data-resistant. Voting is a new phase of blockchain technology; in this area, the researchers are trying to leverage benefits such as transparency, secrecy, and non-repudiation that are essential for voting applications [[14](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B14-sensors-21-05874)]. With the usage of blockchain for electronic voting applications, efforts such as utilizing blockchain technology to secure and rectify elections have recently received much attention [[15](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B15-sensors-21-05874)].
* The remainder of the paper is organized as follows. [Section 2](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec2-sensors-21-05874) explains how blockchain technology works, and a complete background of this technology is discussed. How blockchain technology can transfer the electronic voting system is covered in [Section 3](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec3-sensors-21-05874). In [Section 4](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec4-sensors-21-05874), the problems and their solutions of developing online voting systems are identified. The security requirements for the electronic voting system are discussed in [Section 5](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec5-sensors-21-05874), and the possibility of electronic voting on blockchain is detailed in [Section 6](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec6-sensors-21-05874). [Section 7](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec7-sensors-21-05874) discusses the available blockchain-based electronic voting systems and analyzes them thoroughly. In [Section 8](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec8-sensors-21-05874), all information related to the latest literature review is discussed and analyzed deeply. [Section 9](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec9-sensors-21-05874) addresses the study, open issues, and future trends. Furthermore, in the end, [Section 10](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#sec10-sensors-21-05874) concludes this survey.

BACKGROUND:-

The first things that come to mind about the blockchain are cryptocurrencies and smart contracts because of the well-known initiatives in Bitcoin and Ethereum. Bitcoin was the first crypto-currency solution that used a blockchain data structure. Ethereum introduced smart contracts that leverage the power of blockchain immutability and distributed consensus while offering a crypto-currency solution comparable to Bitcoin. The concept of smart contracts was introduced much earlier by Nick Szabo in the 1990s and is described as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises” [[16](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B16-sensors-21-05874)]. In Ethereum, a smart contract is a piece of code deployed to the network so that everyone has access to it. The result of executing this code is verified by a consensus mechanism and by every member of the network as a whole [[17](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B17-sensors-21-05874)].

Today, we call a blockchain a set of technologies combining the blockchain data structure itself, distributed consensus algorithm, public key cryptography, and smart contracts [[18](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B18-sensors-21-05874)]. Below we describe these technologies in more detail.

Blockchain creates a series of blocks replicated on a peer-to-peer network. Any block in blockchain has a cryptographic hash and timestamp added to the previous block, as shown in [Figure 1](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/figure/sensors-21-05874-f001/). A block contains the Merkle tree block header and several transactions [[19](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B19-sensors-21-05874)]. It is a secure networking method that combines computer science and mathematics to hide data and information from others that is called cryptography. It allows the data to be transmitted securely across the insecure network, in encrypted and decrypted forms [[20](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B20-sensors-21-05874),[21](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B21-sensors-21-05874)].

[[](https://www.ncbi.nlm.nih.gov/core/lw/2.0/html/tileshop_pmc/tileshop_pmc_inline.html?title=Click%20on%20image%20to%20zoom&p=PMC3&id=8434614_sensors-21-05874-g001.jpg)](https://www.ncbi.nlm.nih.gov/core/lw/2.0/html/tileshop_pmc/tileshop_pmc_inline.html?title=Click%20on%20image%20to%20zoom&p=PMC3&id=8434614_sensors-21-05874-g001.jpg" \t "tileshopwindow)

[Figure 1](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/figure/sensors-21-05874-f001/)

The blockchain structure.

As was already mentioned, the blockchain itself is the name for the data structure. All the written data are divided into blocks, and each block contains a hash of all the data from the previous block as part of its data [[22](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B22-sensors-21-05874)]. The aim of using such a data structure is to achieve provable immutability. If a piece of data is changed, the block’s hash containing this piece needs to be recalculated, and the hashes of all subsequent blocks also need to be recalculated [[23](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B23-sensors-21-05874)]. It means only the hash of the latest block has to be used to guarantee that all the data remains unchanged. In blockchain solutions, data stored in blocks are formed from all the validated transactions during their creation, which means no one can insert, delete or alter transactions in an already validated block without it being noticed [[24](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B24-sensors-21-05874)]. The initial zero-block, called the “genesis block,” usually contains some network settings, for example, the initial set of validators (those who issue blocks).

Blockchain solutions are developed to be used in a distributed environment. It is assumed that nodes contain identical data and form a peer-to-peer network without a central authority. A consensus algorithm is used to reach an agreement on blockchain data that is fault-tolerant in the presence of malicious actors. Such consensus is called Byzantine fault tolerance, named after the Byzantine Generals’ Problem [[25](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B25-sensors-21-05874)]. Blockchain solutions use different Byzantine fault tolerance (BFT) consensus algorithms: Those that are intended to be used in fully decentralized self-organizing networks, such as cryptocurrency platforms, use algorithms such as proof-of-work or proof-of-stake, where validators are chosen by an algorithm so that it is economically profitable for them to act honestly [[26](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B26-sensors-21-05874)]. When the network does not need to be self-organized, validators can be chosen at the network setup stage [[27](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B27-sensors-21-05874)]. The point is that all validators execute all incoming transactions and agree on achieving results so that more than two-thirds of honest validators need to decide on the outcome.

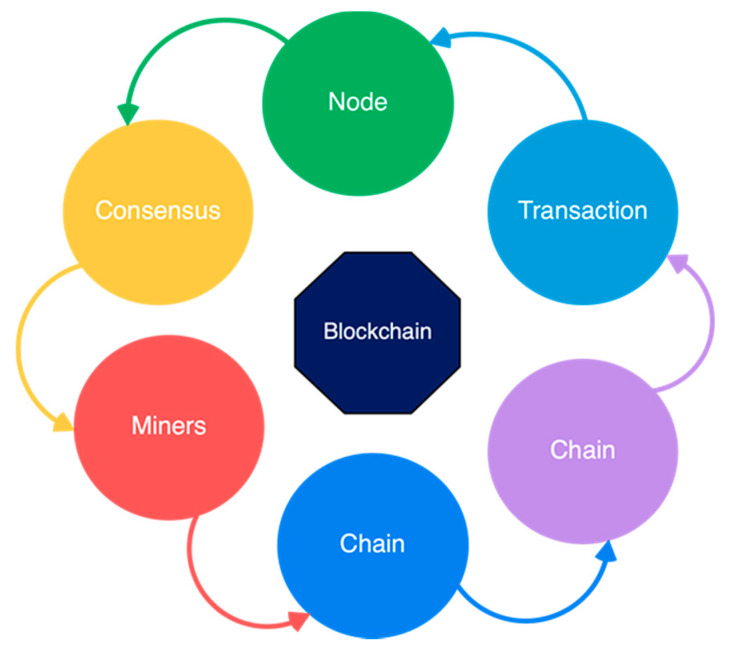
Public key cryptography is used mainly for two purposes: Firstly, all validators own their keypairs used to sign consensus messages, and, secondly, all incoming transactions (requests to modify blockchain data) have to be signed to determine the requester. Anonymity in a blockchain context relates to the fact that anyone wanting to use cryptocurrencies just needs to generate a random keypair and use it to control a wallet linked to a public key [[28](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B28-sensors-21-05874)]. The blockchain solution guarantees that only the keypair owner can manage the funds in the wallet, and this property is verifiable [[29](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B29-sensors-21-05874),[30](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B30-sensors-21-05874)]. As for online voting, ballots need to be accepted anonymously but only from eligible voters, so a blockchain by itself definitely cannot solve the issue of voter privacy.

Smart contracts breathed new life into blockchain solutions. They stimulated the application of blockchain technology in efforts to improve numerous spheres. A smart contract itself is nothing more than a piece of logic written in code. Still, it can act as an unconditionally trusted third party in conjunction with the immutability provided by a blockchain data structure and distributed consensus [[31](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B31-sensors-21-05874)]. Once written, it cannot be altered, and all the network participants verify all steps. The great thing about smart contracts is that anybody who can set up a blockchain node can verify its outcome.

As is the case with any other technology, blockchain technology has its drawbacks. Unlike other distributed solutions, a blockchain is hard to scale: An increasing number of nodes does not improve network performance because, by definition, every node needs to execute all transactions, and this process is not shared among the nodes [[32](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B32-sensors-21-05874)]. Moreover, increasing the number of validators impacts performance because it implies a more intensive exchange of messages during consensus. For the same reason, blockchain solutions are vulnerable to various denial-of-service attacks. If a blockchain allows anyone to publish smart contracts in a network, then the operation of the entire network can be disabled by simply putting an infinite loop in a smart contract. A network can also be attacked by merely sending a considerable number of transactions: At some point, the system will refuse to receive anything else. In cryptocurrency solutions, all transactions have an execution cost: the more resources a transaction utilizes, the more expensive it will be, and there is a cost threshold, with transactions exceeding the threshold being discarded. In private blockchain networks [[33](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B33-sensors-21-05874),[34](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B34-sensors-21-05874)], this problem is solved depending on how the network is implemented via the exact mechanism of transaction cost, access control, or something more suited to the specific context.

2.1. Core Components of Blockchain Architecture

These are the main architectural components of Blockchain as shown in [Figure 2](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/figure/sensors-21-05874-f002/).

[[](https://www.ncbi.nlm.nih.gov/core/lw/2.0/html/tileshop_pmc/tileshop_pmc_inline.html?title=Click%20on%20image%20to%20zoom&p=PMC3&id=8434614_sensors-21-05874-g002.jpg)](https://www.ncbi.nlm.nih.gov/core/lw/2.0/html/tileshop_pmc/tileshop_pmc_inline.html?title=Click%20on%20image%20to%20zoom&p=PMC3&id=8434614_sensors-21-05874-g002.jpg" \t "tileshopwindow)

[Figure 2](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/figure/sensors-21-05874-f002/)

Core components of blockchain architecture.

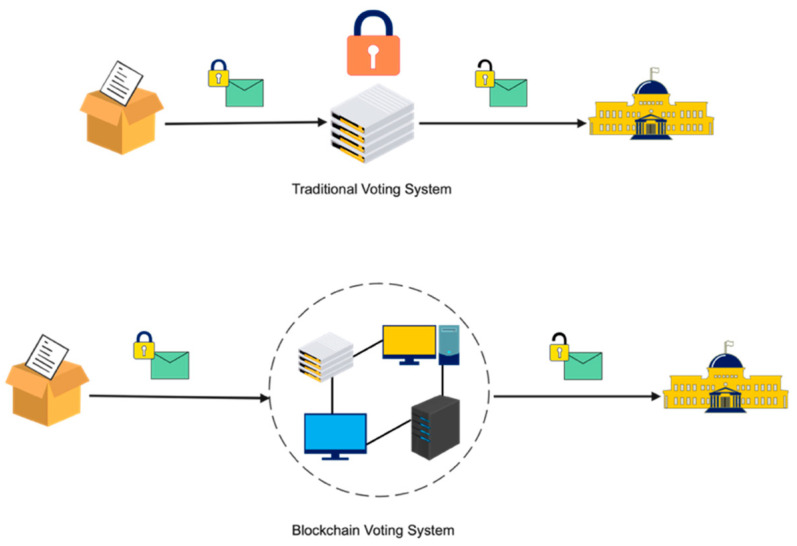
* Node: Users or computers in blockchain layout (every device has a different copy of a complete ledger from the blockchain);
* Transaction: It is the blockchain system’s smallest building block (records and details), which blockchain uses;
* Block: A block is a collection of data structures used to process transactions over the network distributed to all nodes.
* Chain: A series of blocks in a particular order;
* Miners: Correspondent nodes to validate the transaction and add that block into the blockchain system;
* Consensus: A collection of commands and organizations to carry out blockchain processes.

2.2. Critical Characteristics of Blockchain Architecture

Blockchain architecture has many benefits for all sectors that incorporate blockchain. Here are a variety of embedded characteristics as described [Figure 3](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/figure/sensors-21-05874-f003/):

* Cryptography: Blockchain transactions are authenticated and accurate because of computations and cryptographic evidence between the parties involved;
* Immutability: Any blockchain documents cannot be changed or deleted;
* Provenance: It refers to the fact that every transaction can be tracked in the blockchain ledger;
* Decentralization: The entire distributed database may be accessible by all members of the blockchain network. A consensus algorithm allows control of the system, as shown in the core process;
* Anonymity: A blockchain network participant has generated an address rather than a user identification. It maintains anonymity, especially in a blockchain public system;
* Transparency: It means being unable to manipulate the blockchain network. It does not happen as it takes immense computational resources to erase the blockchain network.

Blockchain technology fixed shortcomings in today’s method in elections made the polling mechanism clear and accessible, stopped illegal voting, strengthened the data protection, and checked the outcome of the polling. The implementation of the electronic voting method in blockchain is very significant [[35](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B35-sensors-21-05874)]. However, electronic voting carries significant risks such as if an electronic voting system is compromised, all cast votes can probably be manipulated and misused. Electronic voting has thus not yet been adopted on a national scale, considering all its possible advantages. Today, there is a viable solution to overcome the risks and electronic voting, which is blockchain technology. In [Figure 4](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/figure/sensors-21-05874-f004/), one can see the main difference between both of the systems. In traditional voting systems, we have a central authority to cast a vote. If someone wants to modify or change the record, they can do it quickly; no one knows how to verify that record. One does not have the central authority; the data are stored in multiple nodes. It is not possible to hack all nodes and change the data. Thus, in this way, one cannot destroy the votes and efficiently verify the votes by tally with other nodes.

[[](https://www.ncbi.nlm.nih.gov/core/lw/2.0/html/tileshop_pmc/tileshop_pmc_inline.html?title=Click%20on%20image%20to%20zoom&p=PMC3&id=8434614_sensors-21-05874-g004.jpg)](https://www.ncbi.nlm.nih.gov/core/lw/2.0/html/tileshop_pmc/tileshop_pmc_inline.html?title=Click%20on%20image%20to%20zoom&p=PMC3&id=8434614_sensors-21-05874-g004.jpg" \t "tileshopwindow)

[Figure 4](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/figure/sensors-21-05874-f004/)

Traditional vs. blockchain voting system.

If the technology is used correctly, the blockchain is a digital, decentralized, encrypted, transparent ledger that can withstand manipulation and fraud. Because of the distributed structure of the blockchain, a Bitcoin electronic voting system reduces the risks involved with electronic voting and allows for a tamper-proof for the voting system. A blockchain-based electronic voting system requires a wholly distributed voting infrastructure. Electronic voting based on blockchain will only work where the online voting system is fully controlled by no single body, not even the government [[36](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B36-sensors-21-05874)]. To sum-up, elections can only be free and fair when there is a broad belief in the legitimacy of the power held by those in positions of authority. The literature review for this field of study and other related experiments may be seen as a good path for making voting more efficient in terms of administration and participation. However, the idea of using blockchain offered a new model for electronic voting.

## **4. Problems and Solutions of Developing Online Voting Systems**

Whether talking about traditional paper-based voting, voting via digital voting machines, or an online voting system, several conditions need to be satisfied:

* Eligibility: Only legitimate voters should be able to take part in voting;
* Unreusability: Each voter can vote only once;
* Privacy: No one except the voter can obtain information about the voter’s choice;
* Fairness: No one can obtain intermediate voting results;
* Soundness: Invalid ballots should be detected and not taken into account during tallying;
* Completeness: All valid ballots should be tallied correctly.

Below is a brief overview of the solutions for satisfying these properties in online voting systems.

### 4.1. Eligibility

The solution to the issue of eligibility is rather apparent. To take part in online voting, voters need to identify themselves using a recognized identification system. The identifiers of all legitimate voters need to be added to the list of participants. But there are threats: Firstly, all modifications made to the participation list need to be checked so that no illegitimate voters can be added, and secondly, the identification system should be both trusted and secure so that a voter’s account cannot be stolen or used by an intruder. Building such an identification system is a complex task in itself [[37](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B37-sensors-21-05874)]. However, because this sort of system is necessary for a wide range of other contexts, especially related to digital government services, researchers believe it is best to use an existing identification system, and the question of creating one is beyond the scope of work.

### 4.2. Unreusability

At first, glance, implementing unreusability may seem straightforward—when a voter casts their vote, all that needs to be done is to place a mark in the participation list and not allow them to vote a second time. But privacy needs to be taken into consideration; thus, providing both unreusability and voter anonymity is tricky. Moreover, it may be necessary to allow the voter to re-vote, making the task even more complex [[38](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B38-sensors-21-05874)]. A brief overview of unreusability techniques will be provided below in conjunction with the outline on implementing privacy.

### 4.3. Privacy

Privacy in the context of online voting means that no one except the voter knows how a participant has voted. Achieving this property mainly relies on one (or more) of the following techniques: blind signatures, homomorphic encryption, and mix-networks [[39](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B39-sensors-21-05874)]. Blind signature is a method of signing data when the signer does not know what they are signing. It is achieved by using a blinding function so that blinding and signing functions are commutative–Blind(Sign(message)) = Sign(Blind(message)). The requester blinds (applies blinding function to) their message and sends it for signing. After obtaining a signature for a blinded message, they use their knowledge of blinding parameters to derive a signature for an unblinded message. Blind signatures mathematically prevent anyone except the requester from linking a blinded message and a corresponding signature pair with an unblinded one [[40](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B40-sensors-21-05874)].

The voting scheme proposed by Fujioka, Okamoto, and Ohta in 1992 [[41](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B41-sensors-21-05874)] uses a blind signature: An eligible voter blinds his ballot and sends it to the validator. The validator verifies that the voter is allowed to participate, signs the blinded ballot, and returns it to the voter. The voter then derives a signature for the unblinded vote and sends it to the tallier, and the tallier verifies the validator’s signature before accepting the ballot.

Many online voting protocols have evolved from this scheme, improving usability (in the original method, the voter had to wait till the end of the election and send a ballot decryption key), allowing re-voting, or implementing coercion resistance. The main threat here is the power of the signer: There must be a verifiable log of all emitted signatures; this information logically corresponds to the receiving of a ballot by the voter, so it should be verified that only eligible voters receive signatures from the signer [[42](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B42-sensors-21-05874)]. It should also be verifiable that accounts of voters who are permitted to vote but have not taken part in voting are not utilized by an intruder. To truly break the link between voter and ballot, the ballot and the signature need to be sent through an anonymous channel [[43](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B43-sensors-21-05874)].

Homomorphic encryption is a form of encryption that allows mathematical operations to be performed on encrypted data without decryption, for example, the addition

Enc(a) + Enc(b) = Enc(a + b); or multiplication Enc(a) × Enc(b) = Enc(a × b). In the context of online voting, additive homomorphic encryption allows us to calculate the sum of all the voters’ choices before decryption.

It is worth mentioning here that multiplicative homomorphic encryption can generally be used as an additive. For example, if we have choices x and y and multiplicative homomorphic encryption, we can select a value g and encrypt exponentiation: Enc(gx) × Enc(gy) = Enc(g(x + y)).

Homomorphic encryption can be used to obtain various properties necessary in an online voting system; with regards to privacy, it is used so that only the sum of all the choices is decrypted, and never each voter’s choice by itself. Using homomorphic encryption for privacy implies that decryption is performed by several authorities so that no one can obtain the decryption key; otherwise, privacy will be violated [[44](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/#B44-sensors-21-05874)].

