E-VOTING

Security

An online voting system may have multiple weak spots.

- Cybersecurity risks can come from the system itself
- the authentication mechanisms it deploys
- the mobile devices used by voters
- the mechanisms responsible for protecting stored and transferred data.

Possible example of security risks are:

- compromise of personal data
- manipulation of voting platform by compromising a voter's mobile device or a third-party data storage service.

Voter authentication

Voter authentication is an essential part of any voting system and is necessary to prevent double voting, voter impersonation, and other election manipulations.

When authenticating a voter, a voting system must ensure the person:

- Is exactly who they claim to be
- Has the right to vote
- Hasn't voted already

Online voting systems rely on digital identity verification mechanisms. A person's identity can be verified based on their:

- Digital IDs(government ID card)
- Personal security keys
- Verified mobile devices(personal smartphone)
- Biometrics(fingerprints, face recognition systems)

Possible challenges to face:

- Flawed encryption algorithms threaten the security of voting data.
- And if a person's biometrics aren't processed correctly, an eligible voter might not get a chance to vote.

Accessibility

Pros:

- Online voting could increase the participation rate among voters with physical disabilities and voters living in rural areas.
- Online translation of ballots and voter instructions could be useful for overcoming language barriers.

Cons:

- online voting system requires a stable internet connection, which might not be available in some regions.
- Mobile devices used for authentication purposes are usually smartphones that have to meet certain technical requirements. Thus, a person possessing a less technologically advanced device won't be able to use it as an identity verification tool.
- modern face recognition systems have higher error rates when processing images of minority faces. In case of a recognition error, a misrecognized voter might be prevented from participating in an election.

Voter anonymity

When it comes to any sort elections, voter anonymity is an essential requirement. Anonymity is supposed to prevent possible attempts to influence a voter's decision.

Possible challenges:

- meeting this requirement is more challenging for digital voting systems than for traditional offline vote casting approaches.
- In a digital voting system, it's difficult to ensure that no one can link a particular vote to a specific person while also providing end-to-end (e2e) verifiability and guaranteeing that all votes are properly registered and counted.

Possible solutions:

- voter non-repudiation
- ring signature-based (used for blockchain voting systems)
  Detailed explanation on Ring-based approach: ***http://ceur-ws.org/Vol-2588/paper2.pdf***

Blockchain-based online voting systems

Blockchains can be used to enhance different e-voting systems with the strictest requirements for systems used in national elections, where voter anonymity is a must.

A blockchain can help you achieve several goals when building an e-voting solution:

- Securely store data
- Reliably verify identities
- Cast votes
-

Below are the few Blockchain-based voting systems used in different regions:

- Zcoin blockchain is used as a database to store encrypted data containing voter identification documents and vote tallies.
- Voatz app relies on the Hyperledger Fabric blockchain to create an immutable trail of cast ballots.
- Ethereum-based uPort solution which is used as an e-government authorization service. Citizens registered in uPort can use this service as a third-party authorization tool for accessing various online government services, including e-voting.
- Votem is a blockchain-based mobile voting system. The platform can verify a voter's identity, facilitate an absentee ballot request, and securely cast votes.

Pros of blockchain-based e-voting

As a distributed ledger, a blockchain offers several crucial advantages for e-voting systems:

- Resistance to cyberattacks
- Immutable data records which eliminates the risk of tampering with voting results.
- Transparent transaction history which make it easier to audit and verify election results.
- Voter anonymity: Standard methods like multi-factor authentication (MFA) can be used for voters authentication, and ring signature method can be applied to ensure voter anonymity,
- Blockchain-based solutions can increase the speed of vote counting and mitigate the risk of human errors and fraud by reducing human intervention in the balloting process.

Cons of blockchain-based e-voting

Key concerns regarding voting systems with blockchain capabilities include:

- **Dependence on software and devices:** Hackers may use software or device flaws to steal a voter's data or alter their vote before it is recorded on the blockchain.
- **Voter disqualification risks:** A voter can be disqualified by mistake and thus prevented from participating in an election. For instance, most current concepts of blockchain-based voting systems rely on private keys as a vote authenticity validation measure. However, private keys are unrestorable, so if a voter loses their private key, they won't be able to cast their ballot.
- **Lack of clear regulations and public trust:** The lack of clear state-level regulations for blockchain-based solutions creates additional concerns and insecurities for both the developers and users of such systems. Establishing unified guidelines and standards would make it easier to build secure, unbiased, and well-performing blockchain-based voting platforms that could gain public trust.

Building a blockchain-based e-voting solution: key aspects

- **Purpose:** First, you need to determine what purpose the blockchain will serve as part of your voting solution.

Depending on the task at hand, your focus may range from securely recording votes on the blockchain to casting actual votes using smart contracts. When working on a general blockchain-based e-voting system, there will be several crucial choices you need to make:

1. What type of blockchain network to use?

There are three common types of blockchain network architectures:

- Public Networks with Permissionless access: Operate with untrusted members
- Public Networks with Permissioned access: Operate with trusted members
- Private Networks with Permissioned access: Operate with trusted members of defined community

There are several aspects that may influence your choice when it comes to the architecture of a blockchain network

- Level of decentralization
- Information publicity
- Transaction fees

Permissioned networks:

- preferable for cases when only partial decentralization is desired.

Public permissionless:

- to achieve the maximum possible decentralization.

Public networks:

- all transaction information is available to everyone, so you can monitor election progress in real time.
- require a transaction fee (mostly as a security measure against denial of service attacks).

Private blockchain network :

- you can manage what data can be seen by the general public
- it's much easier to configure free transactions

2. What consensus algorithm to implement?

Consensus algorithms are responsible for reaching a single source of truth within a blockchain and can be competitive or non-competitive.

Competitive consensus algorithms

- they may be prone to double payment. For example, As an Ethereum-based solution, uPort relies on the proof of stake consensus algorithm.

Non-competitive consensus algorithms,

- allow for processing only one agreement at a time in a trusted network. However, they can be more vulnerable to attacks as such networks usually consist of a small number of nodes. For instance, Voatz is a blockchain-based voting solution that relies on the non-competitive Practical Byzantine Fault Tolerance (PBFT) consensus algorithm.

3.What integration opportunities to enable?

Digital voting solutions can be used in conjunction with traditional offline vote casting instead of replacing other voting approaches completely

Blockchain-based solution can be integrated with multiple systems. Depending on the extent to which blockchain technology is used in your application, you need to plan different integration scenarios for each of these options :

- Third-party identity verification services
- Online voting systems
- Databases storing votes cast by other systems

4. How to maintain the required level of anonymity?

By default, blockchain transactions are public so that any user might get access to transaction details. However, online elections usually require ensuring complete ballot secrecy. So when building a blockchain-based e-voting system, it's necessary to eliminate the possibility of linking a particular vote to a particular user.

Many of the current blockchain-based voting systems rely on non-interactive zero-knowledge (NIZK) arguments as a measure for achieving the right balance between ballot secrecy and voting result verifiability.

- For instance, Zcash, a blockchain that some researchers see as a fitting solution for online voting, uses a zero-knowledge Succinct Non-interactive Argument of Knowledge.

Conclusion

- You can build a blockchain-based e-voting system to securely store voting data, authenticate legitimate voters, and cast actual ballots.
- In contrast to other solutions for online voting, solutions that leverage blockchain technology offer improved data security, contain convenient identity verification mechanisms, and make it easier to maintain the right balance between ballot secrecy and voting results verification.