Decentralized Web Application for Online Voting

Author: Ing. Dávid Košičiar
Supervisor: Ing. Tomaš Majer, PhD.

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Motivation

Traditional voting methods, while established, often lack the security and trust required in modern online environments. By integrating blockchain technology, the system ensures that each vote is not only securely cast but also immutable, meaning it cannot be altered. The transparency of blockchain further guarantees that the entire voting process can be verified and audited by anyone with access to the system, enhancing public trust in the results.

Additionally, the decentralized nature of the system removes the reliance on a single authority to oversee and validate the election, making it resilient to attacks and manipulation. This innovation is set to transform both public elections and internal voting within organizations by making the voting process easier, lowering administrative costs, and encouraging more people to vote by offering the convenience of online participation.

Methodology

The methodology outlines the approach taken to design and implement a decentralized online voting system. It focuses on developinga secure, transparent, and efficient solution using innovative technologies to enhance the voting process.

1 System Design

The project started with an analysis of existing voting systems, focusing on using blockchain to enhance security and transparency. Key challenges like fraud and transparency were addressed through blockchain features like smart contracts.

2 Blockchain Selection

Ethereum was chosen for its support of decentralized applications (DApps) and smart contracts. Solidity was used to implement voting logic, including voter registration and result calculation.

3 Smart Contract Development

Core voting processes were managed via smart contracts deployed on the Ethereum blockchain, ensuring tamper-proof and transparent elections.

4 Frontend and Backend

The frontend was developed using React, while the backend leveraged the Nethereum library to enable communication with the Ethereum blockchain. Metadata storage was handled via IPFS.

5 Testing and Deployment

The system was tested on Ethereum testnets and deployed using CI/CD pipelines through Azure DevOps.

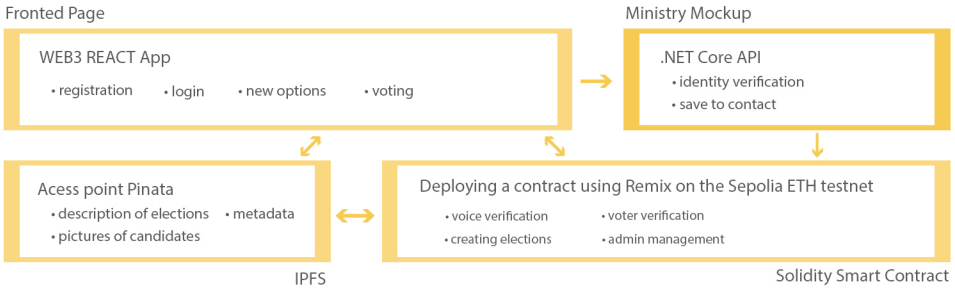
6 Security

The project explored balancing transparency with voter privacy, focusing on maintaining data integrity while protecting voter anonymity.

Results

The cost comparison between traditional and blockchain-based voting systems shows that, under current conditions, traditional elections are more financially viable. In the 2024 Slovak presidential elections, the cost per vote was 3.77 euros, based on a total expense of 18.6 million euros for organizing the election and voter participation numbers.
In contrast, testing of blockchain voting revealed that each vote consumed 76,000 gas, translating to a cost of approximately 6.36 euros per vote at the current Ethereum price of 3,220 euros. While blockchain voting offers enhanced transparency and security, its current high costs make it less competitive than traditional methods.
However, the use of Layer 2 (L2) solutions such as Arbitrum One could significantly reduce these costs, lowering the price per vote to 0.0245 euros. The trade-off for these lower costs is a slight reduction in the overall security of the voting system, but this approach holds promise for future scalability and cost-effectiveness.

Design



Conclusion

This thesis presents a fully functional decentralized web application for online voting, built using Ethereum smart contracts and a React-based interface. The project demonstrates how blockchain can modernize voting by offering transparency, security, and immutability. The work highlights the potential of blockchain beyond financial uses, ensuring secure, verifiable voting. It also shows the advantages of decentralized applications (DApps), like resistance to censorship, though they are still in early adoption stages.

A major challenge identified is maintaining both decentralization and voter anonymity. While blockchain ensures transparency, achieving complete anonymity is challenging due to the public nature of blockchain records. One proposed solution involves using a centralized server to manage encryption keys, but this compromises the decentralized nature of the system. This highlights the difficult balance between ensuring privacy and maintaining transparency in the voting process.