HACK THE FUTURE

Team of Absolutes

Multiparty Electronic Voting System

Objective and Solution Overview

The aim is to design a secure, multiparty electronic voting system that ensures voter anonymity, prevents result tampering, and provides public verifiability, utilizing cryptographic techniques such as Shamir's secret sharing and homomorphic encryption.

1. Each voter’s vote is encrypted to ensure privacy and anonymity.
2. The encrypted votes are stored securely on a blockchain, preventing tampering.
3. The voting system uses a method to calculate the results without revealing individual votes.
4. Blockchain technology ensures the immutability of the stored votes, making them tamper-proof.
5. The final election result can only be decrypted by a majority of the election team, ensuring no single entity controls the outcome.
6. The system guarantees transparency and accountability by allowing public verification of the final result.

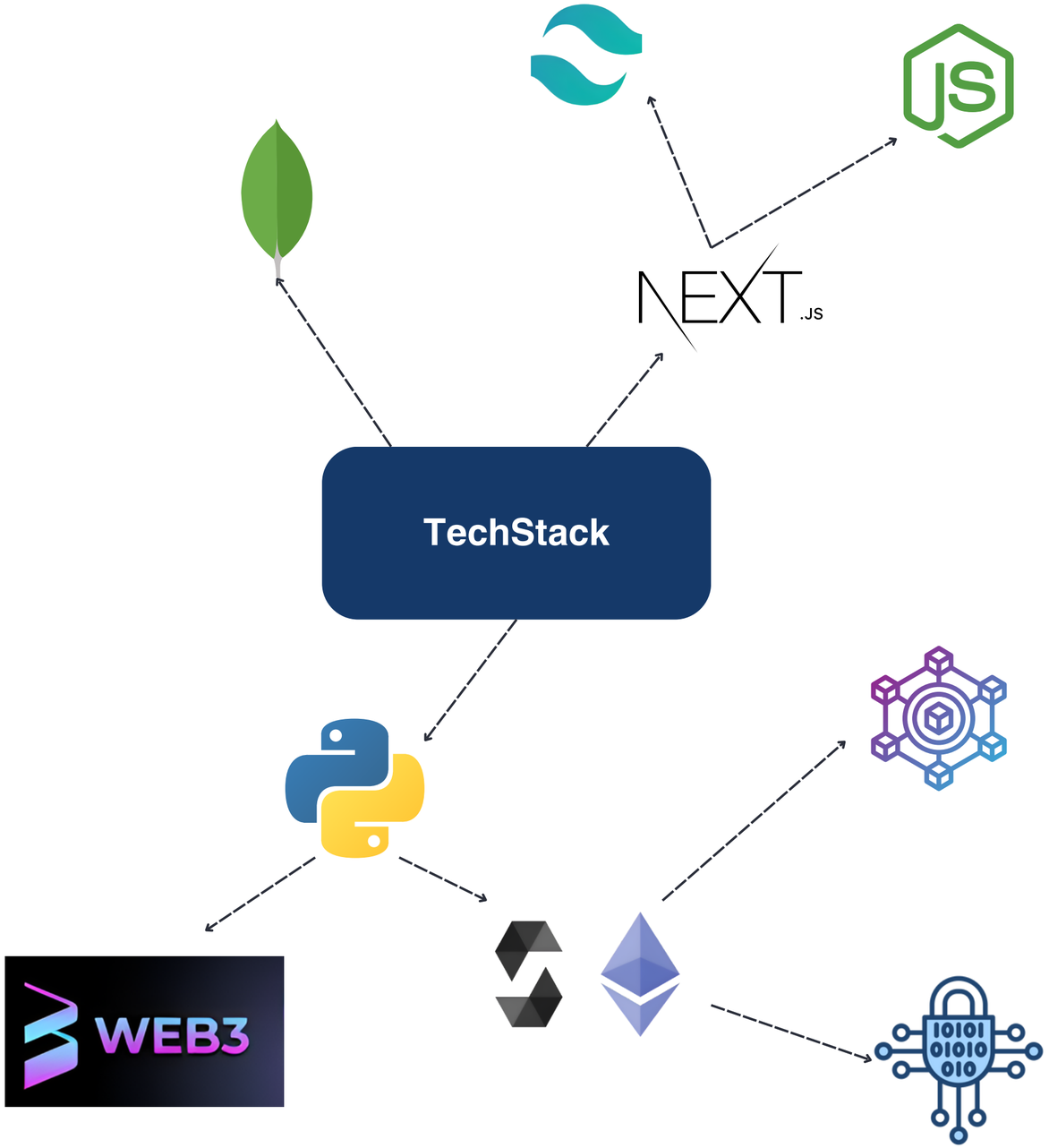
Key Features

Key Generation and Encryption: Generate public and private keys for each voter. Each vote is encrypted using the voter's public key and stored securely on the blockchain, ensuring that the vote cannot be tampered with once cast.

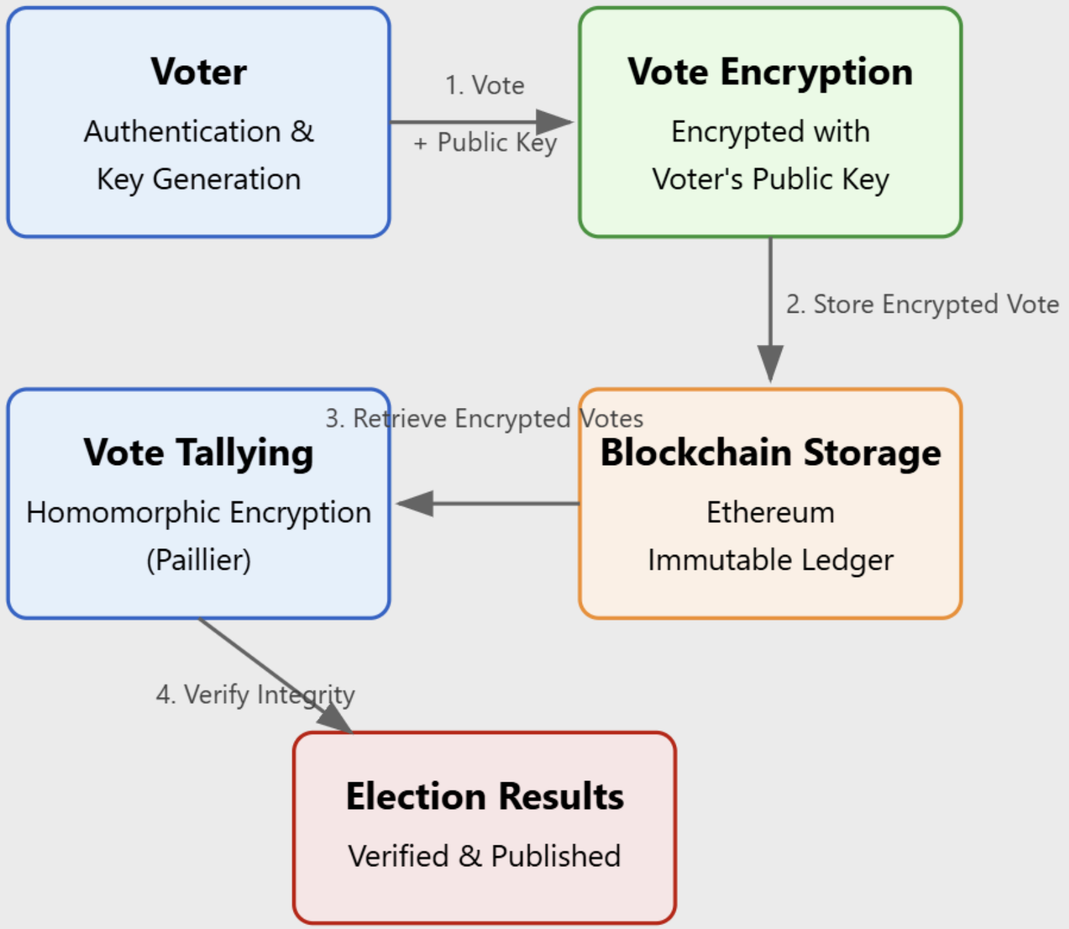
Blockchain Storage: Store the encrypted votes on a blockchain, guaranteeing immutability and transparency. This prevents unauthorized alterations and ensures that the votes remain secure throughout the election process.

Homomorphic Encryption: Use homomorphic encryption to allow encrypted votes to be processed without decryption. Homomorphic addition is applied to aggregate votes, ensuring the election result can be computed directly from the encrypted votes.

Shamir's Secret Sharing for Decryption: Implement Shamir's Secret Sharing to split the decryption key among the election team. More than half of the team members must agree and combine their private keys to decrypt the final election result, ensuring no single entity has control over the outcome.



Implemented Solution



Challenges

- Ensuring Voter Anonymity: Maintaining complete privacy for voters while allowing for accurate result tallying is a critical challenge. Balancing anonymity with the need for transparent verification without compromising security is complex.

- Key Management and Distribution: Securely distributing and managing encryption keys, particularly in systems using Shamir's Secret Sharing, introduces logistical challenges. Ensuring that keys are not lost or tampered with and that only authorized parties can access them is crucial.

- Homomorphic Encryption Complexity: While homomorphic encryption allows for privacy-preserving vote tallying, it is computationally intensive. Ensuring that the system can handle large-scale voting operations without slowing down is a significant challenge.

- Blockchain Storage and Integrity: Storing votes securely on a blockchain is beneficial, but ensuring the blockchain can scale and remain efficient for large datasets without compromising security or transparency can be difficult.