



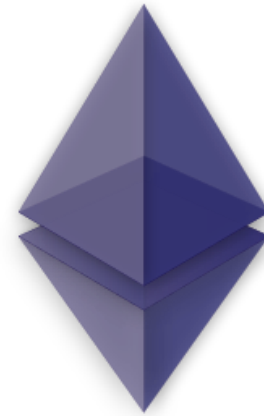
CryptoVote

Idee

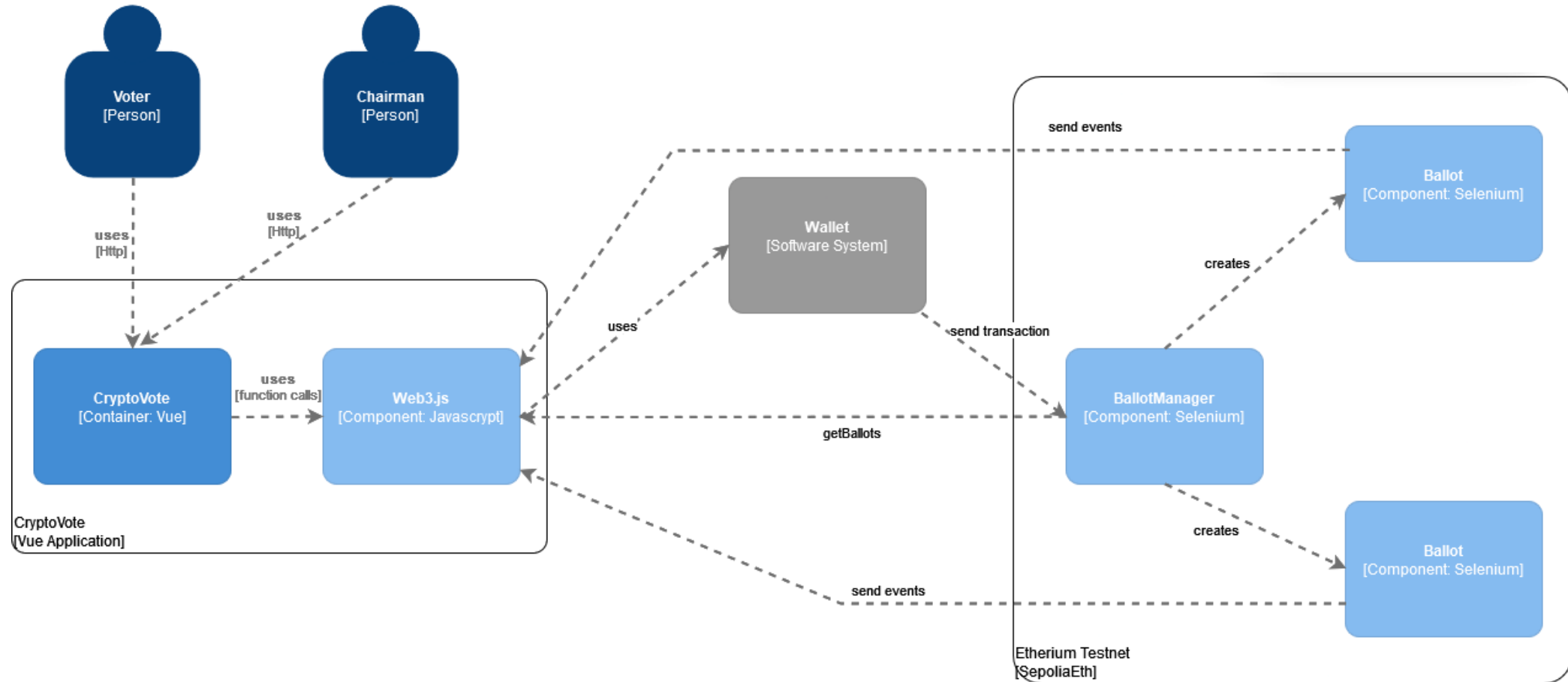
- Abstimmungen auf der Ethereum Blockchain durchführen
- Vorteile
 - Transparenz
 - Integrität
- Nachteile
 - Hohe Kosten
 - Off-Chain Probleme

Architektur Gesamt

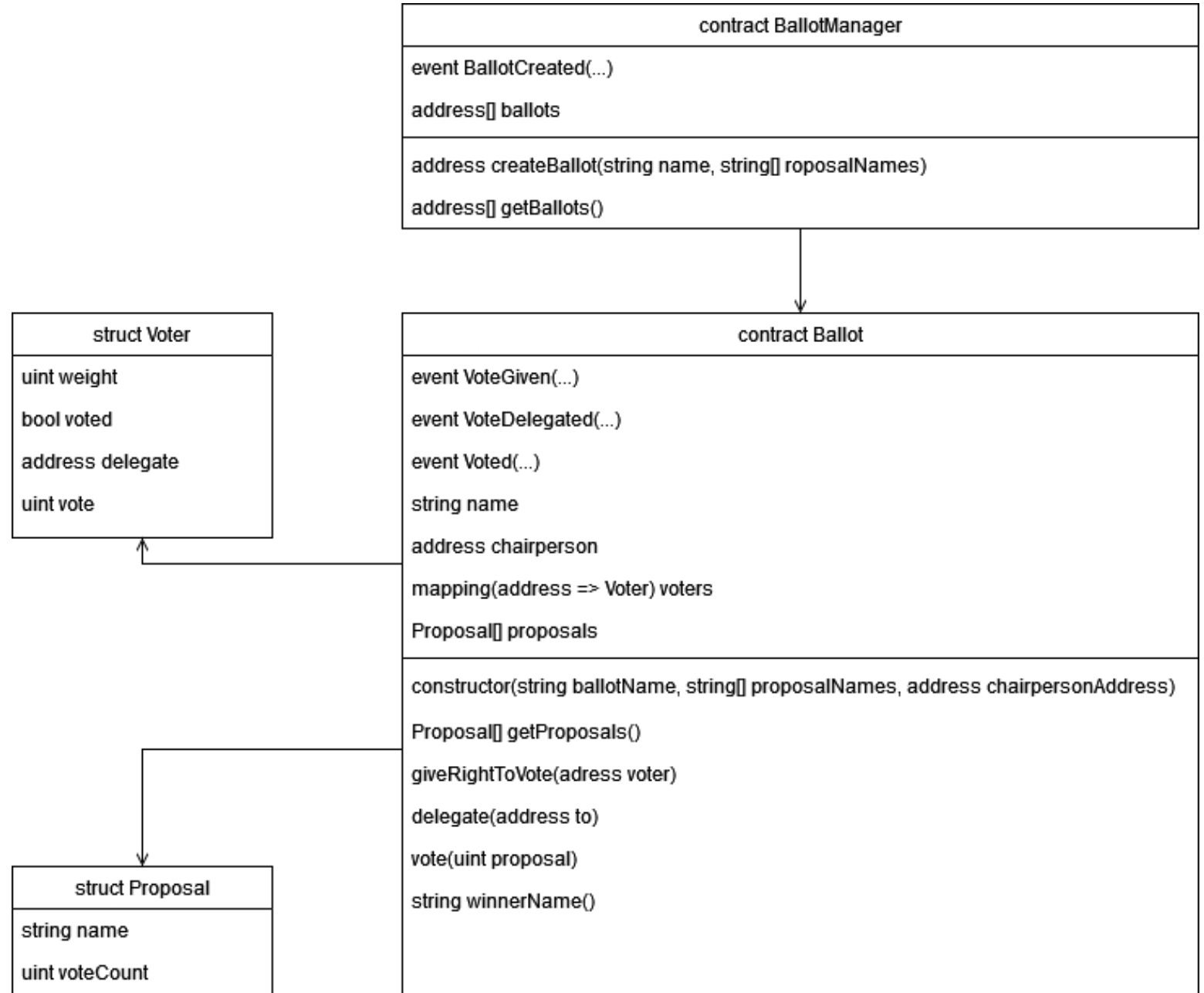
- Frontend: Vue
- Backend: Ethereum
- Contract: Solidity



Diagramm



Architektur Smart Contract



Architektur Vue

- Web3.js für Blockchain Interaktionen
- Events für Audit Funktionalität
- Klassischer Vue Aufbau



Security


- Kern des Smart Contracts aus Beispielcode
- Sender.voted gesetzt, bevor voteCount verändert

```
function vote(uint proposal) public {  ⌨ infinite gas
    Voter storage sender = voters[msg.sender];
    require(sender.weight != 0, "Has no right to vote");
    require(!sender.voted, "Already voted.");
    sender.voted = true;
    sender.vote = proposal;

    // If 'proposal' is out of the range of the array,
    // this will throw automatically and revert all
    // changes.
    proposals[proposal].voteCount += sender.weight;
    emit Voted(msg.sender, address(this), proposal);
}
```

Security

- Delegate: voted true zuerst setzen.

```
function delegate(address to) public {   infinite gas
    Voter storage sender = voters[msg.sender];
    require(!sender.voted, "You already voted.");
    require(to != msg.sender, "Self-delegation is disallowed.");

    while (voters[to].delegate != address(0)) {
        to = voters[to].delegate;

        // We found a loop in the delegation, not allowed.
        require(to != msg.sender, "Found loop in delegation.");
    }
    sender.voted = true;
    sender.delegate = to;
    Voter storage delegate_ = voters[to];
    if (delegate_.voted) {
        // If the delegate already voted,
        // directly add to the number of votes
        proposals[delegate_.vote].voteCount += sender.weight;
    } else {
        // If the delegate did not vote yet,
        // add to her weight.
        delegate_.weight += sender.weight;
    }
    emit VoteDelegated(msg.sender, address(this), to);
}
```


Demo

