SmartVote
– A Distributed E-voting System Deploying Blockchain and Smart Contracts

Problem Statement : Deficits of Current E-Voting System

Receipt-based Voting process
- Could cause **vote purchase** – receipt could be bought by someone
- Could cause **receipt lost** – peeked and then used by someone OR lost it
- Could cause **voting under duress** – someone knows you have the "passport" to vote

Centralized Data-storing Architecture
- Is easy to be **tampered**
- Is easy to be **attacked**
- Is **not fault-tolerant**

Third Party Supervision
- Could cause **illegal counting process**
- Could cause **result changing**
- Could cause any kind of **threat to voters** – third parties have access to both receipts, voters' personal information and the result of all votes

Key Characteristics of Current E-Voting Systems

Receipt-based Voting process
- Voters use the receipts given by a third-party authority as "passport" to participate in an election.

Centralized Data-storing Architecture
- Using a centralized Database to store all Data of an election.

Third Party Supervision
- Election must be held and supervised by trusted third parties.
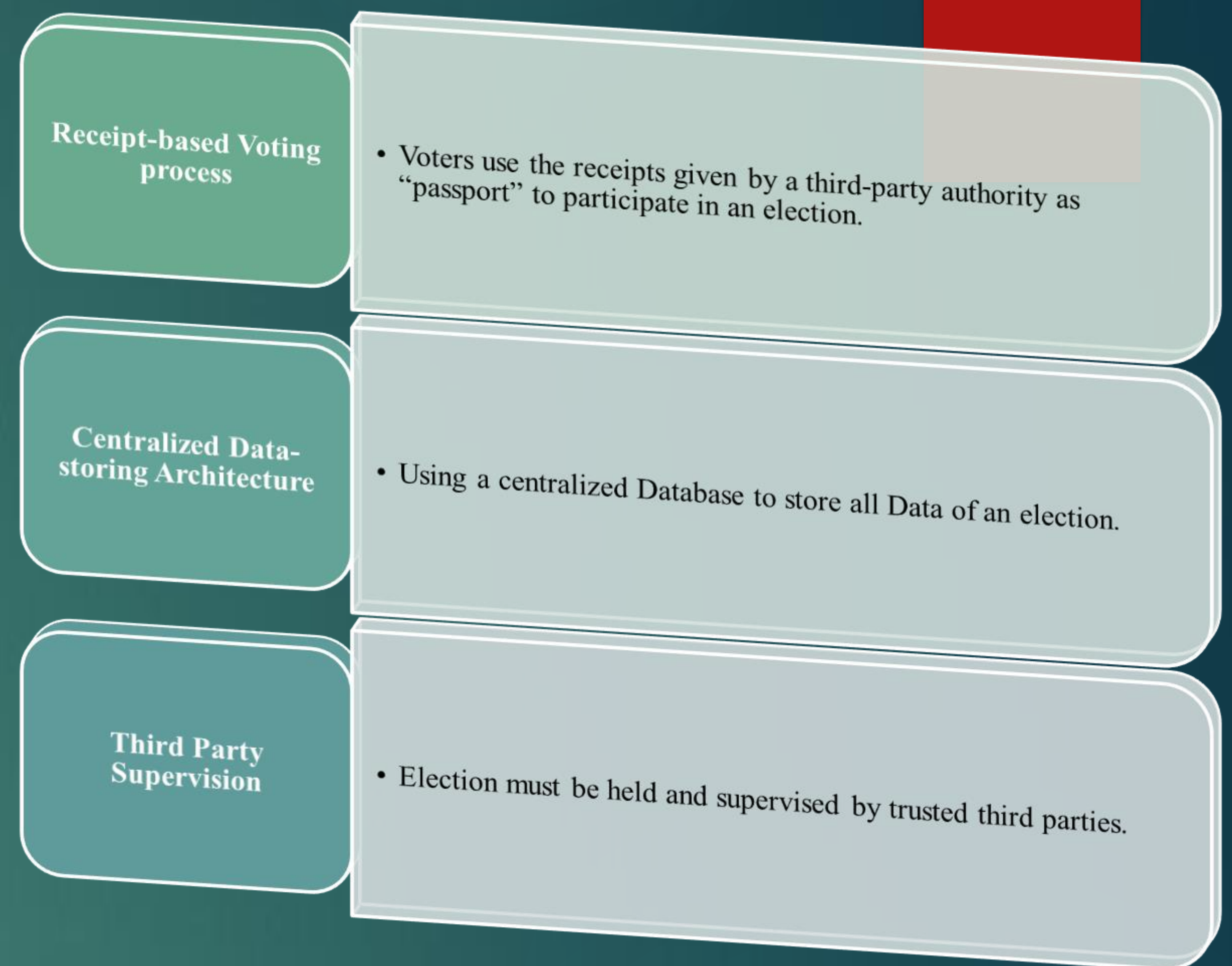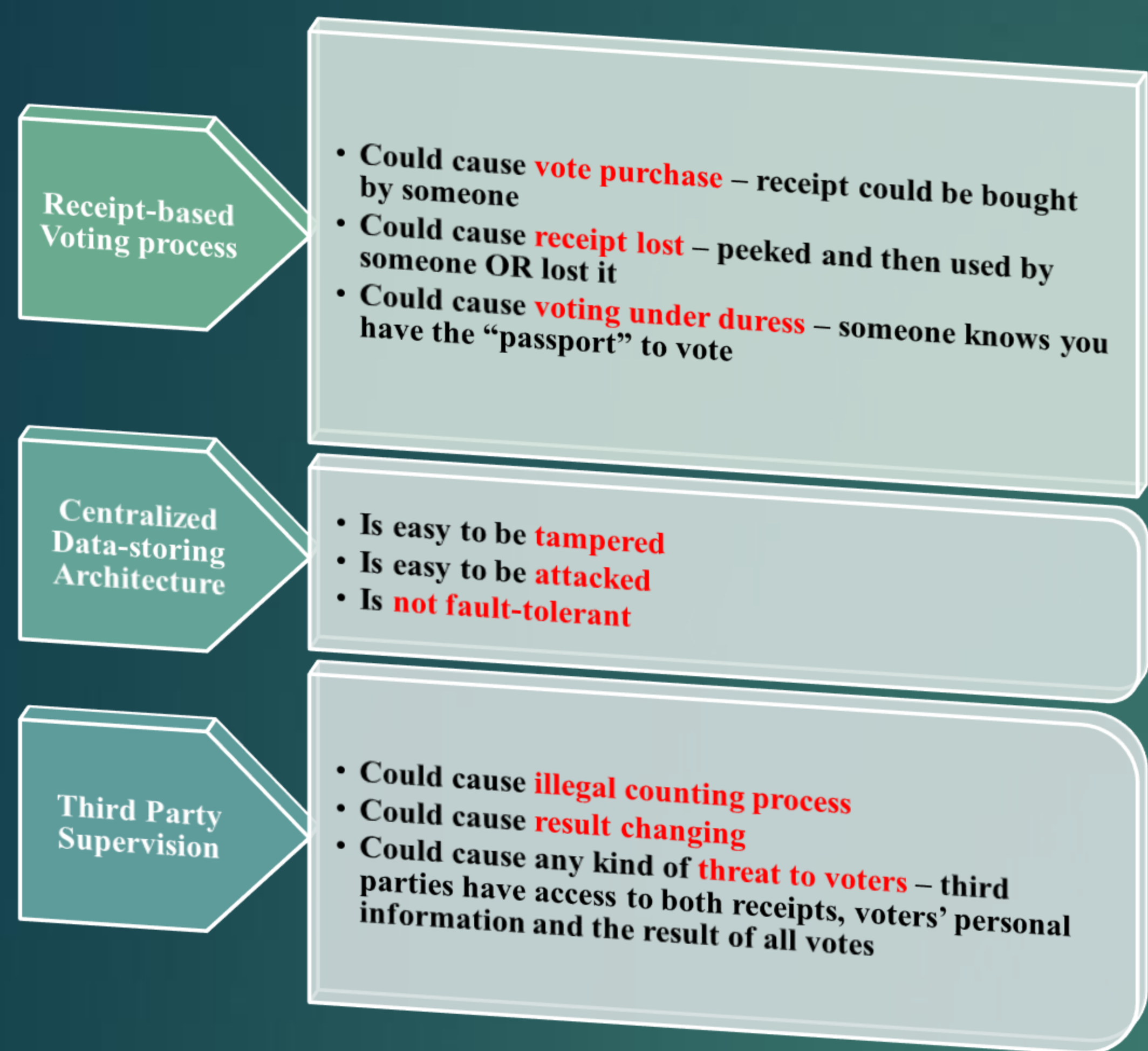
Why SmartVote?

Better voter Authentication
- Non-receipt-based user authentication

Security:
- No one can falsify votes without getting caught

Anonymity:
- Other people couldn't find out how a voter voted

Non-expert Verifiability:
- Non-expert voters can easily verify their votes has been counted properly.

Free from Coercion:
- Avoid 'gun-to-the-head' situations (impossible) & There is no way that a voter can show to another person how he/she voted
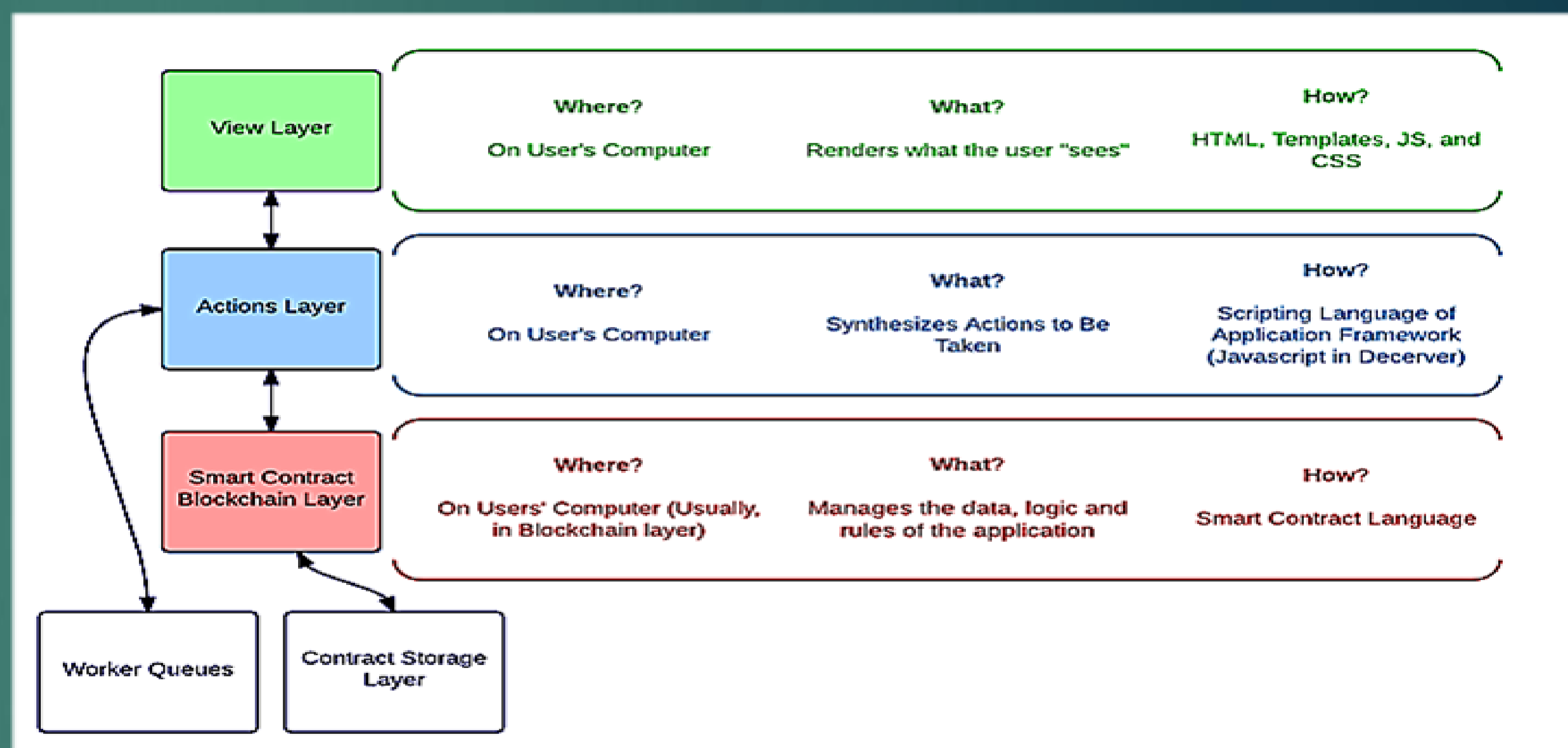
Customizable Voting Rules:
- More than voting to whom OR "agree or disagree" etc.

Who Needs It?

- Non-Governmental Organizations (NGOs)
- Large Companies, education institutions and other for-profit organizations
- Large Communities
- Governments

The Architecture of SmartVote

What is Blockchain?

- A blockchain is a **distributed database** serving as a public ledger of data transactions – each participating network node keeps a copy of this ledger and offers its computing power to repeatedly collect, verify and broadcast newly performed transactions, trying to record them as a new block to the end of the blockchain ("mining").
- A blockchain is extremely hard for an attacker to fraudulently modify, unless the attacker has more computing power than the rest of the network combined.
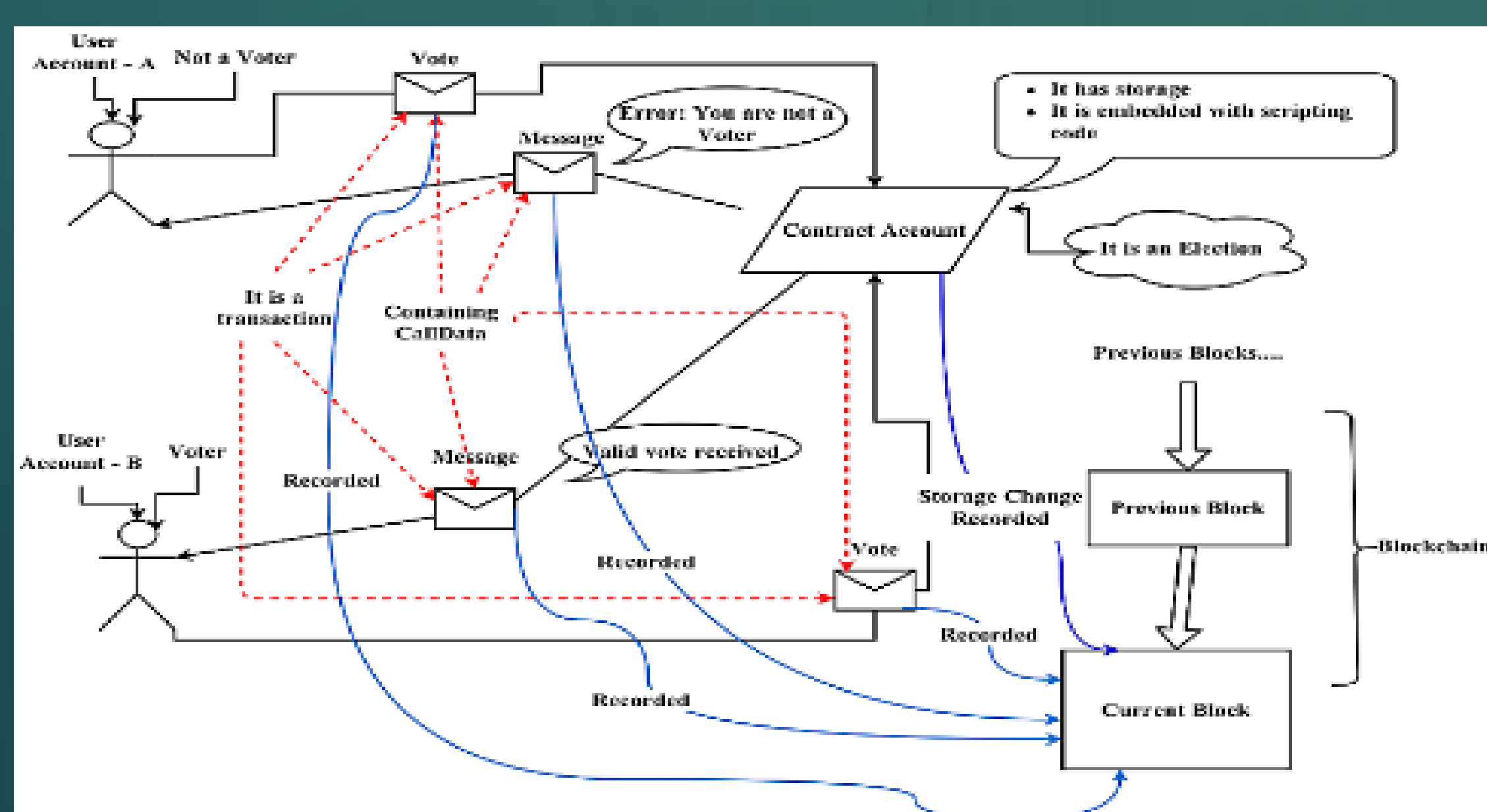
The Structure of A Blockchain - A Sequential Distributed Database.

Data Structure of Blockchain: Merkle Tree

Situation: When someone is trying to tamper the transaction record, it will be detected
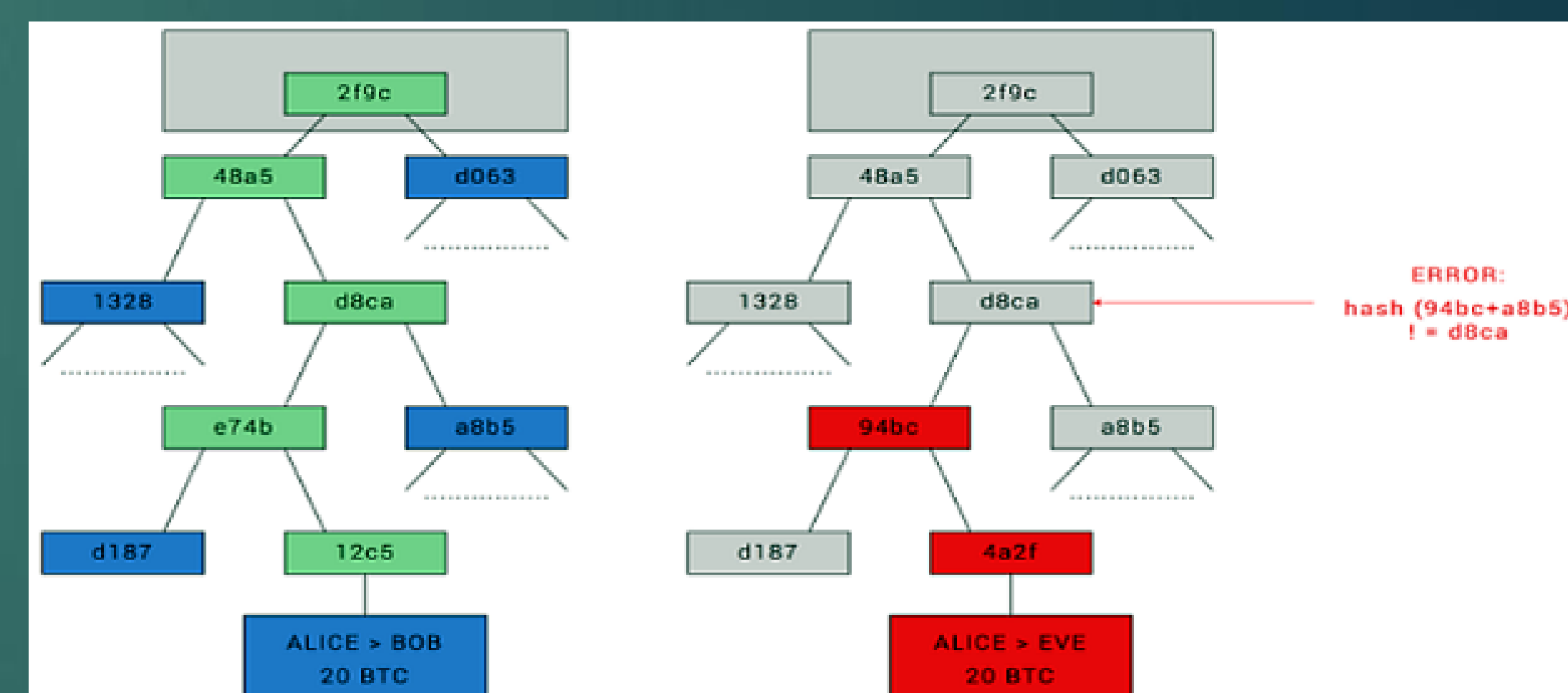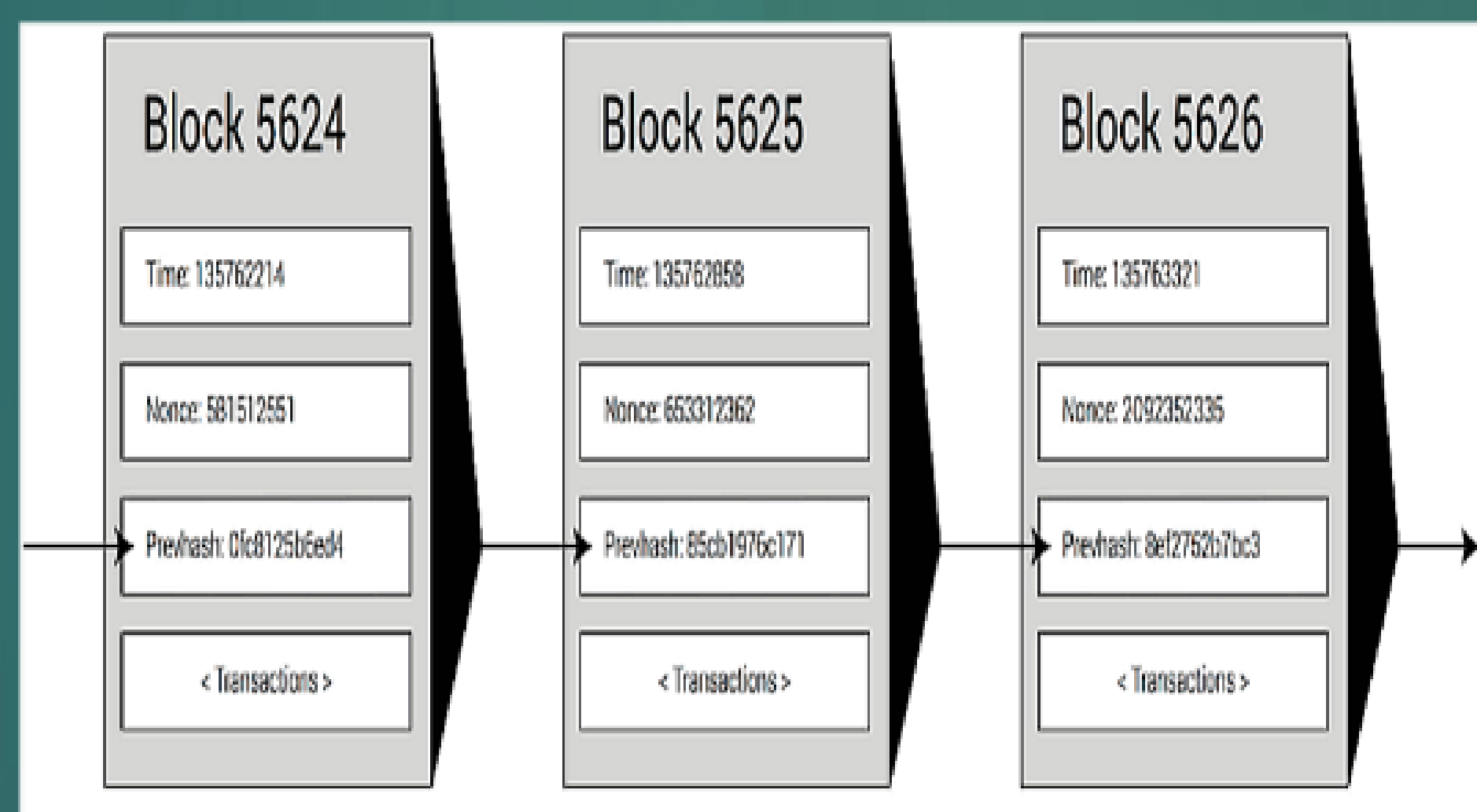
A Simple Voting Process in SmartVote

Smart Contracts are blockchain housed scripts which are compiled into very low level operation codes and stored in the Blockchain's data store at a particular. When a transaction is sent to that address the distributed virtual machine executes the script's operation codes and is able to use the data which is sent with the transaction.

Benefits of Using Blockchain and Smart Contracts

Decentralized software – low cost, trustless, fault-tolerance

Security – strong tamper resistance (which could lead to receipt-less)

More complicated use cases – customizable rules for ownership, transaction formats and state transition functions, etc.

Expectation

The ultimate goal of SmartVote is to build a distributed E-voting system that can provide an anonymity-supporting, verifiable , secure, customizable voting environment integrating with user management and communication modules.