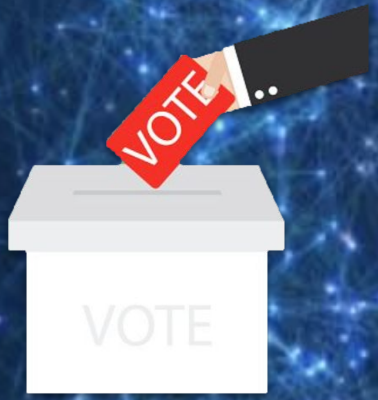


BioVote

Next Generation Ballot Machine
using Blockchain as a Service

Existing Solution

- Electronic Voting Machines are being used to implement electronic voting from 1999 elections.
- Costs approximately ₹12,000 per unit.
- Voting is offline and centralized, with each ballot unit manually transported to voters commision.
- Voter-verified paper audit trail system produces a printed paper ballot to counter record tampering.
- An EVM can record a maximum of 3840 votes and can cater to a maximum of 16 candidates.

The Problem

- Counting votes is very labour intensive and is subject to human error.
- Votes can be manipulated during the transport and tallying procedure.
- The centralized structure of the system makes it insecure at scale.
- Cannot be easily verified since counting is done in secret.
- The EVM also had allegations of getting rigged by the different political parties.
- As EVM maintenance and development is restricted to the Electoral Commision of India, it gives a central body immense power to affect the entire future of a country.

Proposed Solution

BioVote is a next generation ballot machine based on the revolutionary blockchain technology to make the voting process **tamper-proof.**

A frugal device using recent networking breakthroughs, votes are stored on a local blockchain that is synchronized across all voting centers as soon as a vote is cast.

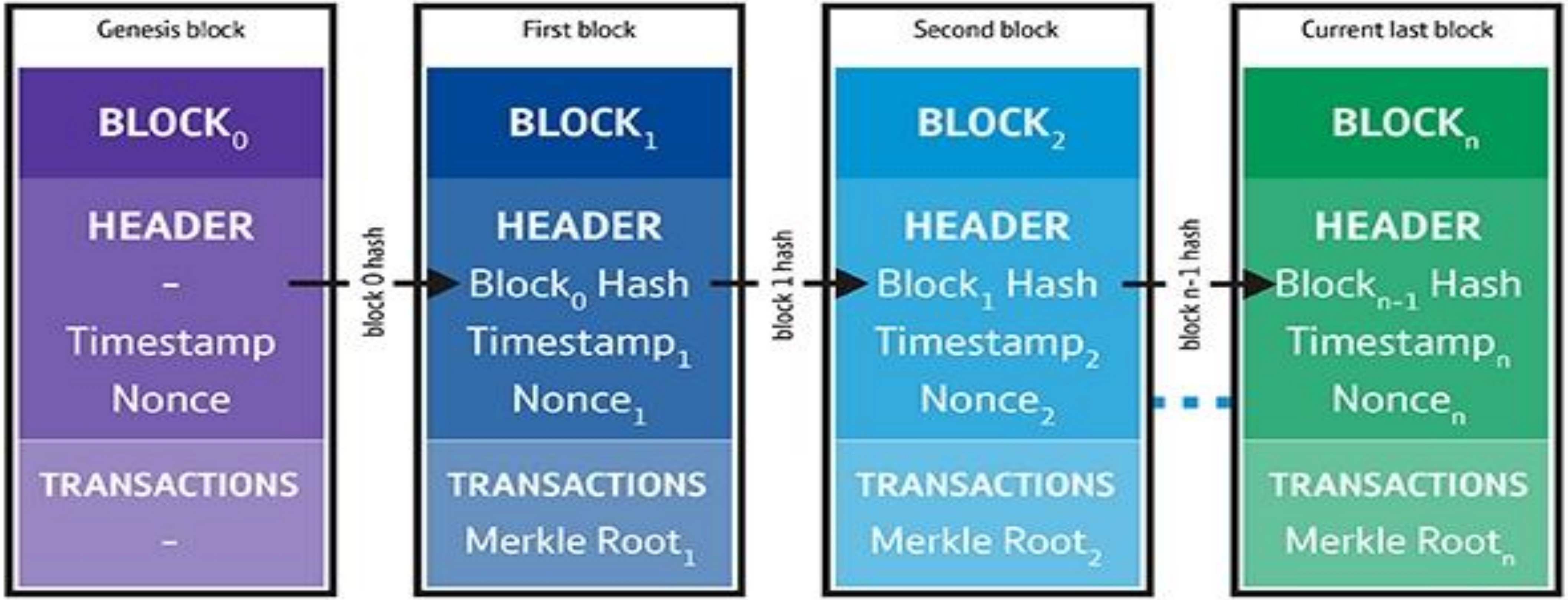
With our system they can now easily cast a vote but this time it is not generic voting process, it is protected with the BioVote BlockChain.

We ensure that everybody gets to vote only once and cannot recast or change their vote later on. This ensures completely scalability and immutability with adding the community trust and security to the entire process.

What is BlockChain?

- The blockchain is a decentralized ledger, where each block is linked to the previous one such that no modifications can be made.
- Blocks hold batches of valid vote data that is hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two.
- This iterative process confirms the integrity of the previous block, all the way back to the original genesis block. In this way, we use the blockchain ledger to store votes in an immutable and verifiable format.

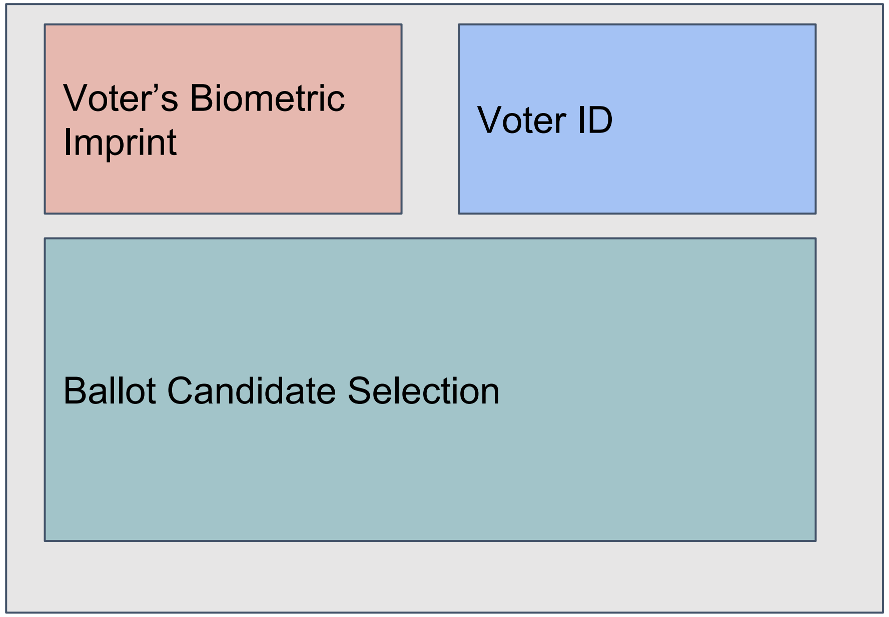
Blockchain - The Immutable Ledger



Every block of data is linked to the next block

Bio-Authentication-based Hash

- A hashed version of the fingerprint taken at the time of voting is stored in the chain to prevent voter identity fraud.
- If the same person tries to vote again, the face hash will produce a conflict and prevent vote from being cast.
- If the same voter ID has already cast a vote, further voting is prevented.
- Finally, the candidate selections are tallied.



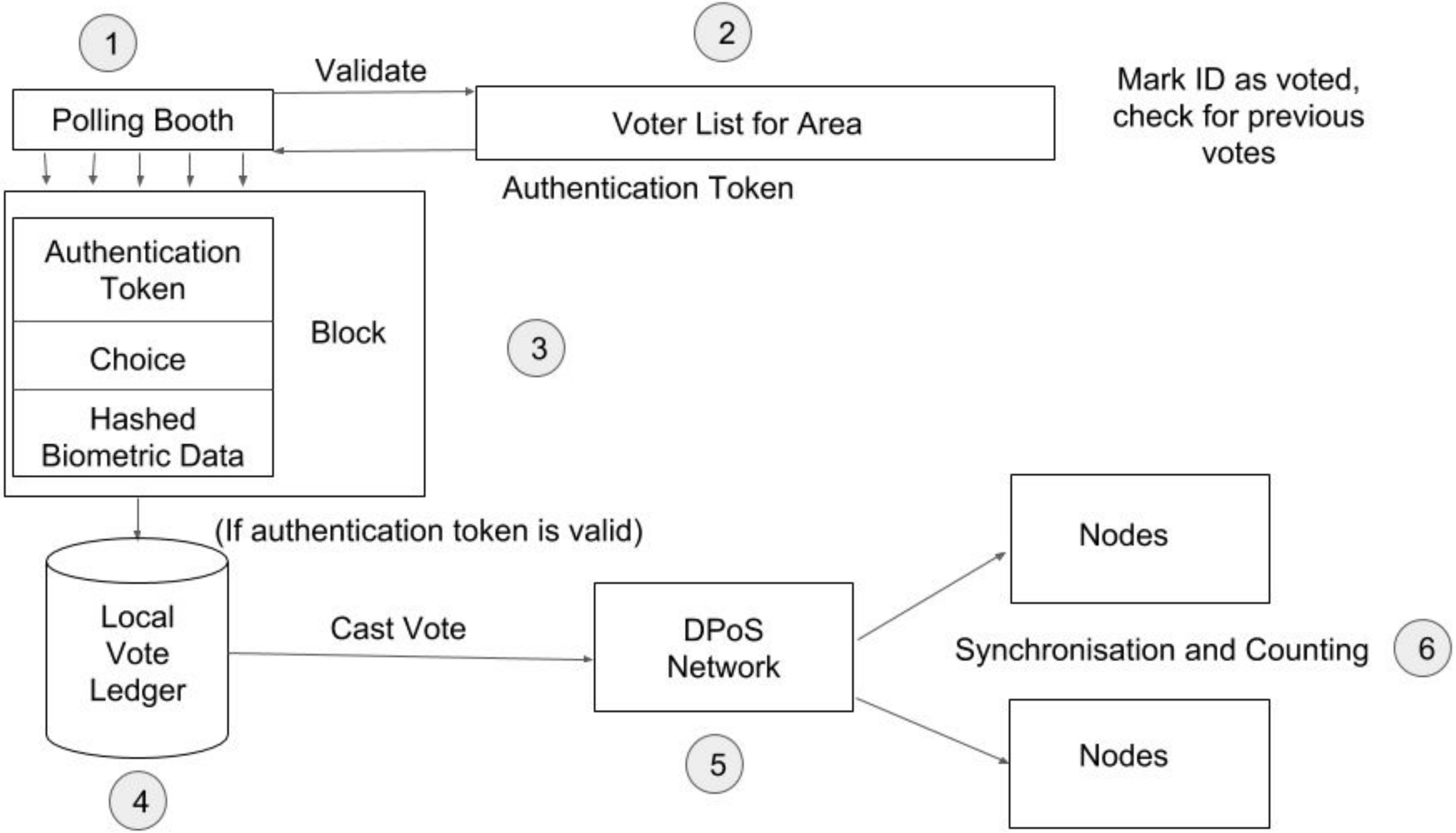
Voter's Biometric Imprint

Voter ID

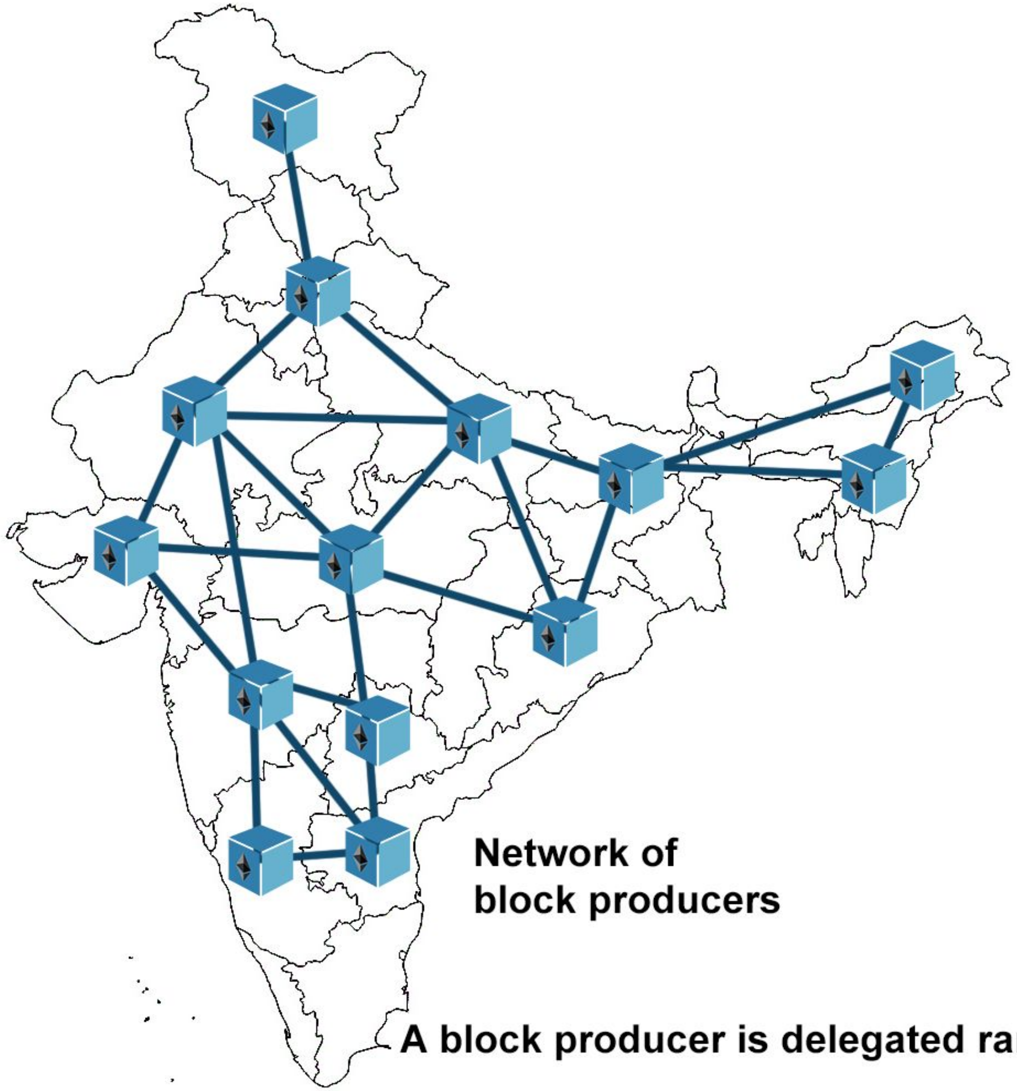
Ballot Candidate Selection

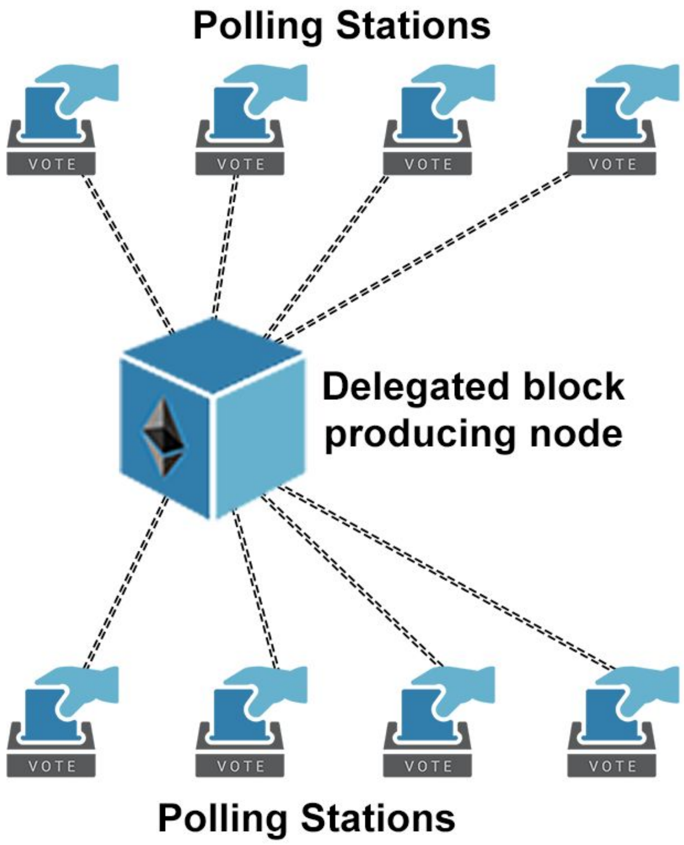
Fig. One Vote as represented by voting hash function

Flowchart


1
Validate
2
Polling Booth
Voter List for Area
Mark ID as voted, check for previous votes
Authentication Token
Authentication Token
Choice
Hashed Biometric Data
Block
3
(If authentication token is valid)
Local Vote Ledger
Cast Vote
DPoS Network
Nodes
Synchronisation and Counting
6
Nodes
5
4

Consensus Algorithm and Synchronisation over the Network





A block producer is delegated randomly for each epoch.

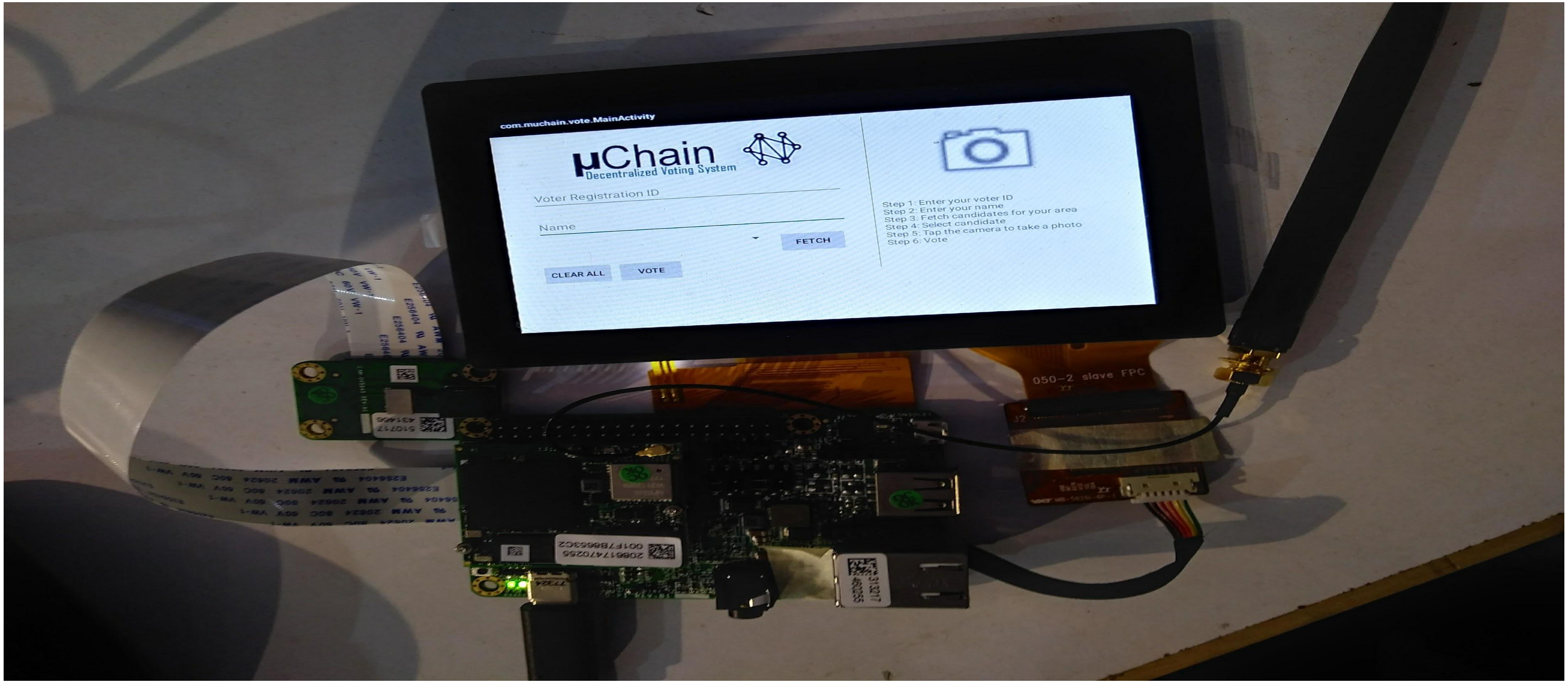
Advantages

- Outside of the constituency voting
- Sharding
- Finding and prevention of duplicate voters easily
- Biometric authentication - Post election verification
- Low cost hardware
- Robust technology (has been proven at scale by bit coin network)

Limitations

- Establishing infrastructure
- Distribution of the voting machine

Prototype of the Proposed Hardware



Step 1: Enter your voter ID
Step 2: Enter your name
Step 3: Fetch candidates for your area
Step 4: Select candidate
Step 5: Tap the camera to take a photo
Step 6: Vote