OnGuard

Guardian of your vote

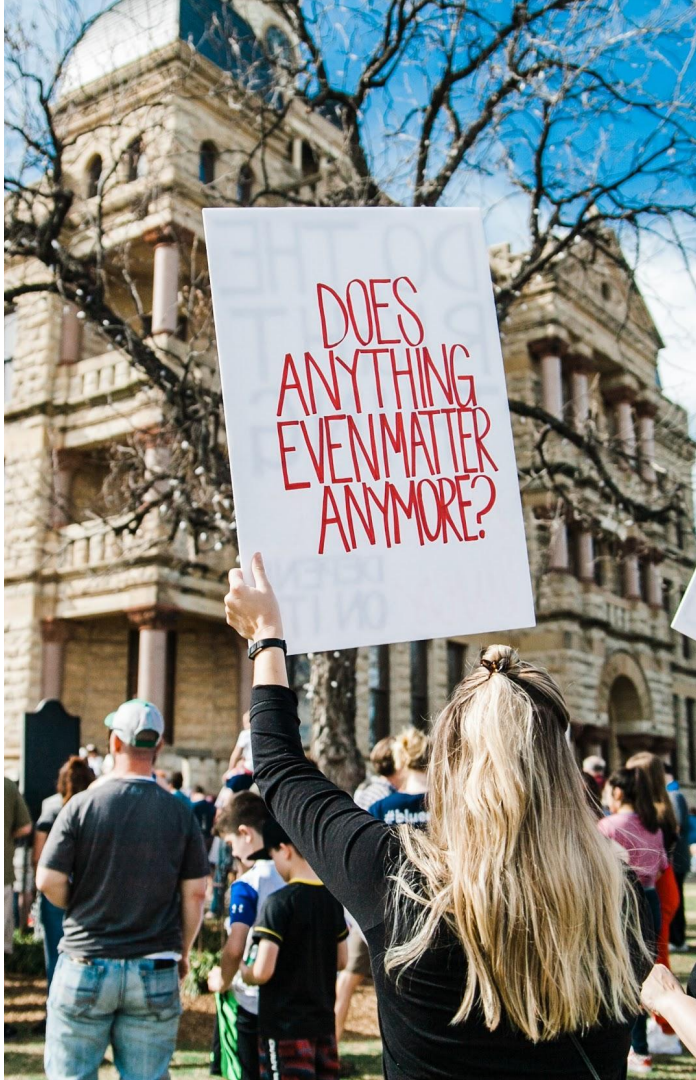
Hazal A.
Alexander J.
Giancarlo G.
Albert A.

Problem

Participation is low.

Governments are not trustworthy.

Referendums are costly.



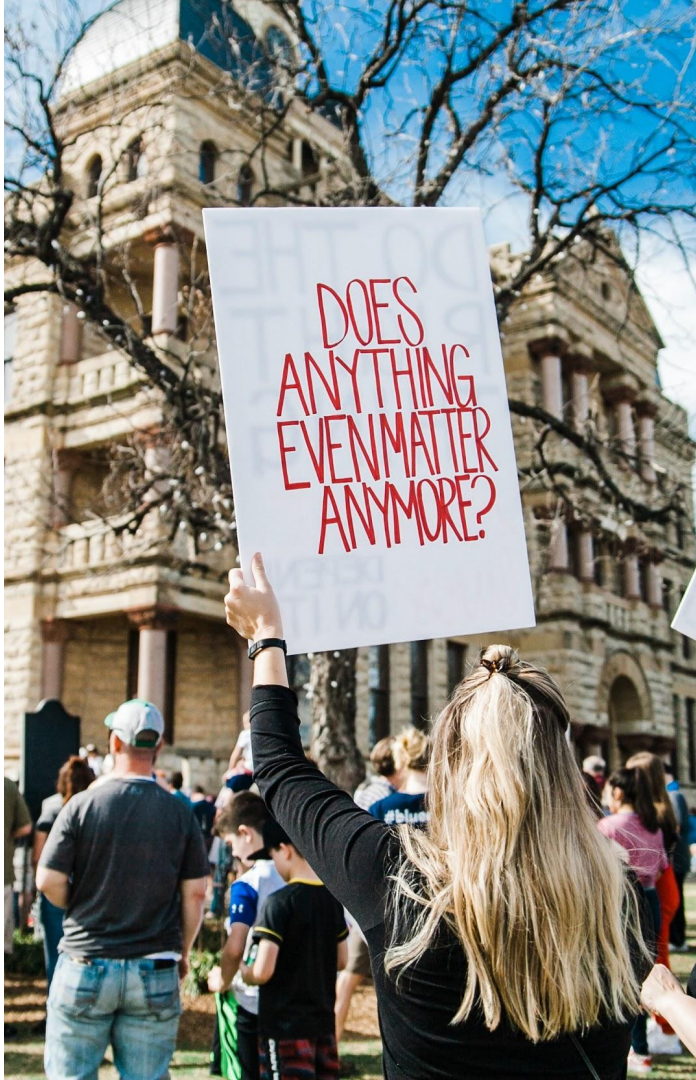
Problem

2018 US Midterm Election Turnout

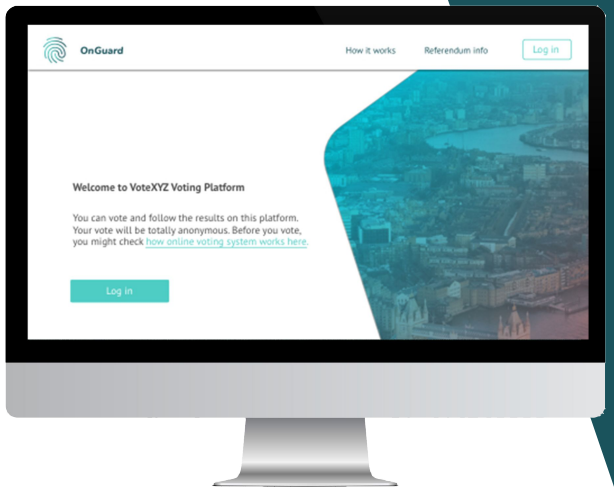
%55

2018 Macedonia Name Referendum Turnout

%39



OnGuard



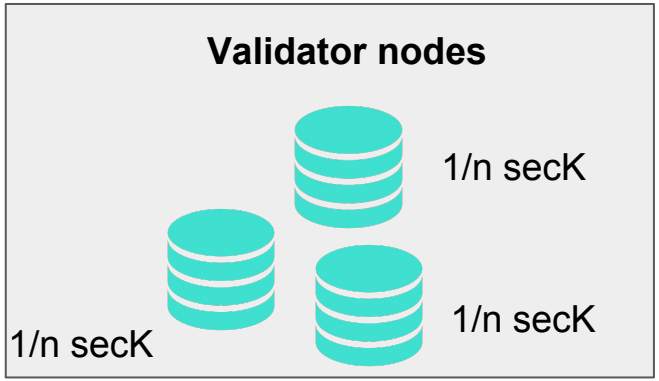
Prove your identity - Vote anonymously - Check impact of your vote

Underlying algorithm: T. HE

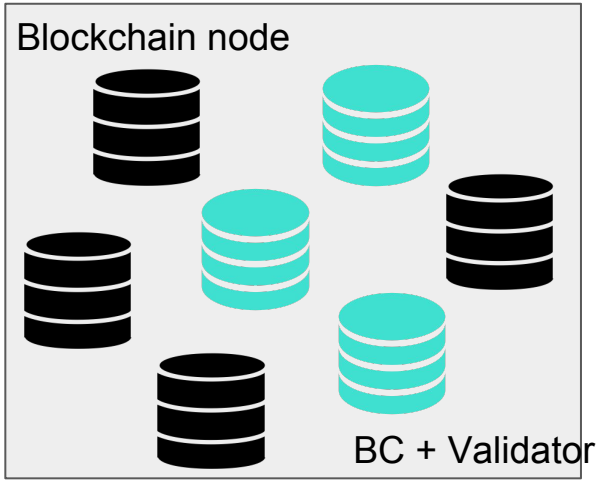
CUTTING EDGE

- Aggregate votes without decrypting them individually
- Consent of all validators before decrypting anything

Vote (y/n, random)	**Cypher**		**Plaintext**
pubK(0, xxxxxx) →	0x23af72fa7fa7faf7	↛	(0 , xxxxxx)
… →	+0x6ae7ae7ae7ae7a	↛	(1 , xxxxxx)
	+0xae6ae6ea6eaee6	↛	(1 , xxxxxx)
	+0xa8ea7ae8aeea8a	↛	(0 , xxxxxx)
	+0xa9e8aea9e8a9ea	↛	(1 , xxxxxx)
	= 0x9d898e8989e98d	→ secK	(3, xxxxxx)



DAO Architecture



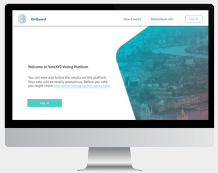
= 9d898e8989e98d98 → (65, xxxxxx)

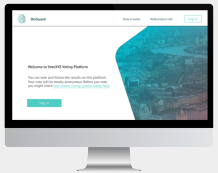
PK(1 , xxxxxx) → 0xad5ad6e234

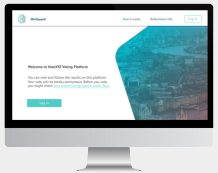
PK(0 , xxxxxx) → 0x23af72fa7fa7faf7

= 9d898e8989e98d98
0xad5ad6e234
+0x23af72fa7fa7faf7
...

= 9d898e8989e98d98
0xad5ad6e234
+0x23af72fa7fa7faf7
...



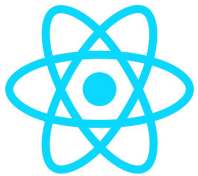




Tech Stack

NEO
smart economy

HELib



React

Future development

- Identity registration → Anonymously issued by government
- Government IDs list is checked against Web of Trust (Further analysis)
- Neo Proposal to decentralize anonymous voting