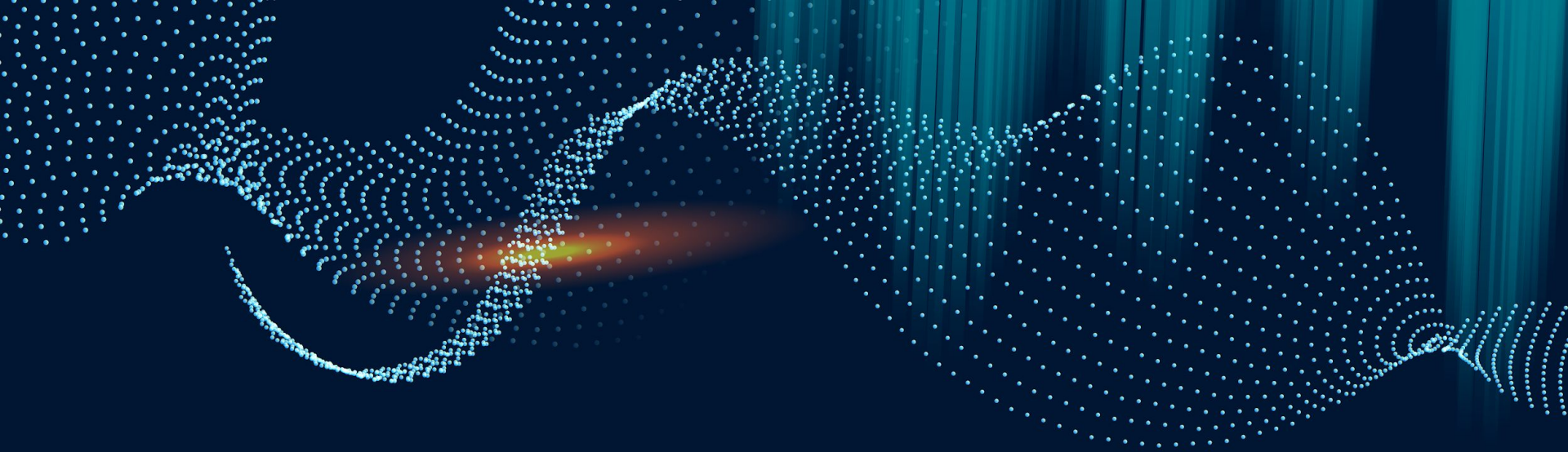
Decentralized Blockchain Voting System

Prototype and Research Study

Alexei & Philip



01 INTRO & MOTIVATION

Why are we doing this?

Problem Statement

Modern voting systems face long-standing issues that are difficult to fix with centralized infrastructure:

- Centralized authorities control voter data and ballot counting
- Limited transparency means voters must trust intermediaries
- Slow verification and potential administrative error
- Difficult to audit results independently

Why Blockchain Voting?

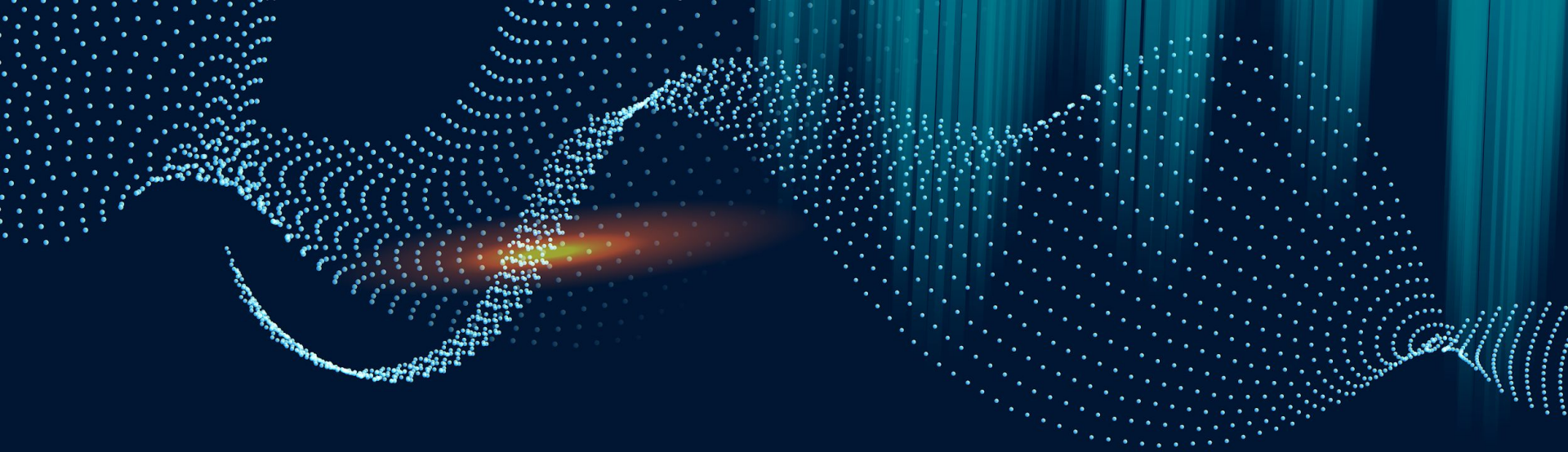
We believe that the issues we mentioned previously can be addressed by the blockchain's core properties:

- Transparency: all vote transfers recorded on-chain
- Immutability: once cast, votes cannot be altered
- Decentralization: removes reliance on a single authority
- Verifiability: anyone can audit the final vote tally

Goals of Our Project

Our project has two parallel objectives – combining practical implementation and research:

- Prototype: build a working on-chain voting system using Solidity and Remix
- Evaluate: test functionality, identify strengths, analyze limitations
- Research: explore scalability, privacy, and approaches used in real systems
- Outcome: understand what works today and what's required for real-world deployment



02 PROTOTYPE IMPLEMENTATION

Building a Functional Prototype

Our Desired Voting Lifecycle

Simple majority Voting:

1. Register eligible voters (whitelisting)
2. Register candidate addresses
3. Issue tokens (1 per voter)
4. Voters cast vote (token transfer)
5. Close voting (votingOpen = false)
6. Compute winner
7. Burn all remaining tokens → End

=> How do we implement this?

System Requirements

What do we need?

- Distributor wallet to manage elections and issue voting tokens
- Voter wallets to receive tokens and cast vote
- Candidate wallets to collect vote tokens
- Enough gas (Eth) to run the system
- Smart contract to enforce all lifecycle rules

Smart Contract Design

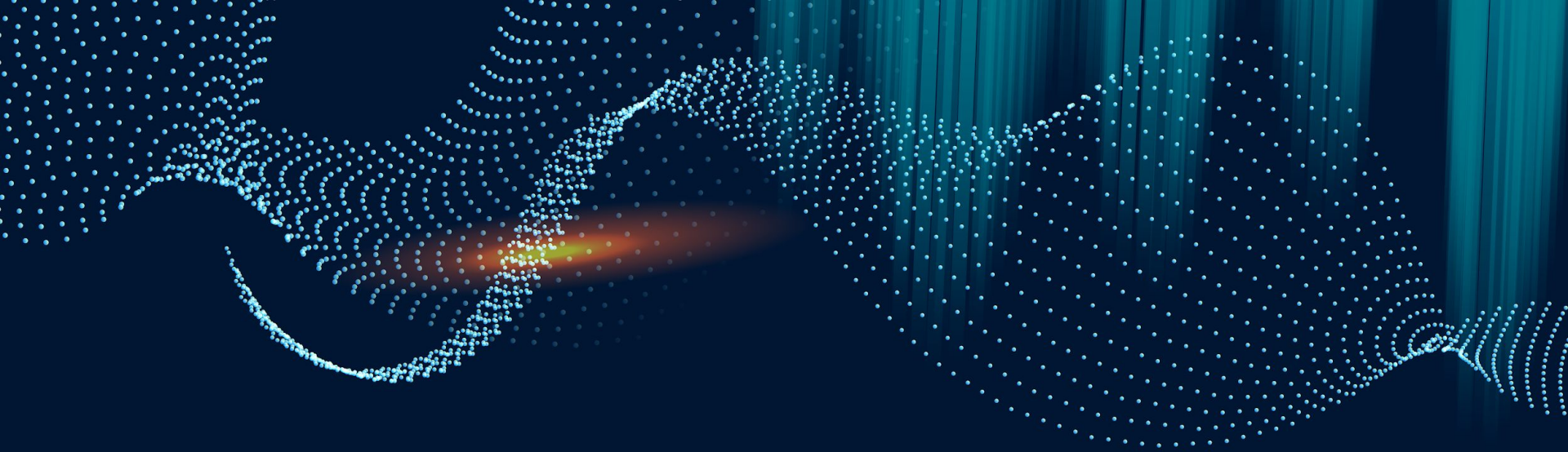
To make this happen, our smart contract needs the following:

- Distributor wallet address
- List of voter addresses
- List of candidate addresses
- Bool for election state

- addVoter(address)
- addCandidate(address)
- startElection()
- castVote(candidate address)
- endElection() => returns results

Along with some more mappings...

SHOW ME THE CODE !!!



03 PROTOTYPE RESULTS

Strengths and Limitations

Prototype Successes

After running a few simulations...

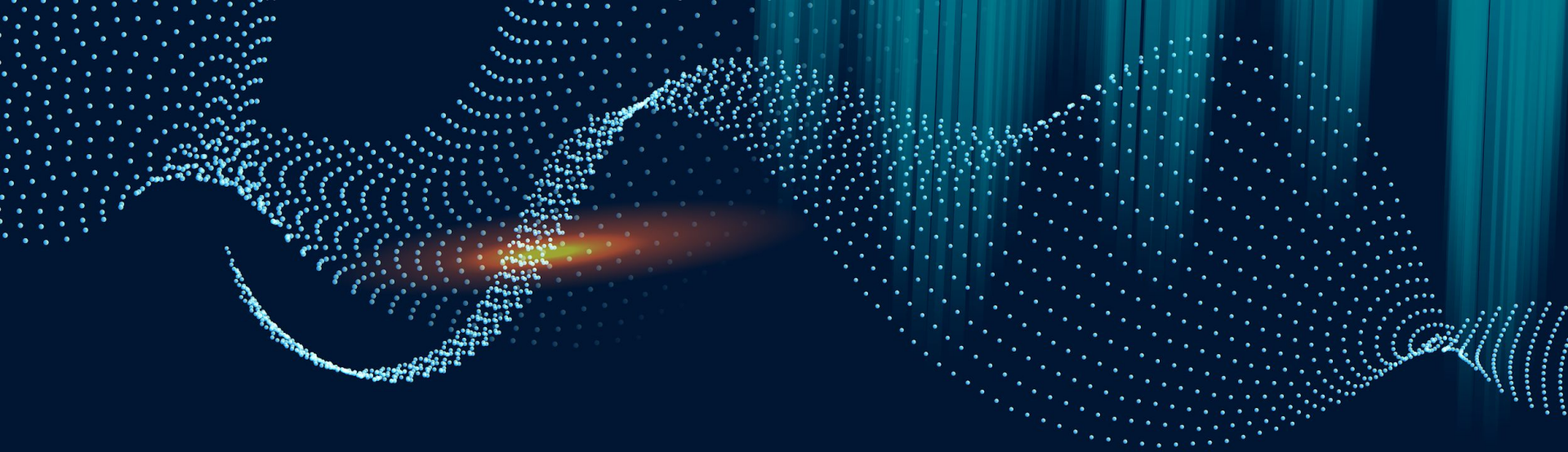
- ✔ Vote tokens enforced correct voting
- ✔ Repeated elections supported
- ✔ No double voting possible
- ✔ System works for small scale transparent majority vote elections

Prototype Limitations

Challenges	Impact
Requires ETH for transaction fees	Barrier to real use
Not fully anonymous	Voter could be exposed
Only majority voting	Currently doesn’t support others
One distributor	Centralized identity control
Votes are visible as they occur	Vulnerable to bribery

Immediate Opportunities for Improvement

- Use a cheaper network for less gas fees
  - Arbitrum, Optimism
- Have someone pay gas on behalf of users
  - Real world elections tend to cost money
- Commit-reveal voting
  - Votes are submitted hashed and then revealed later
- Support for weighted voting by introducing classes of voters



04 FURTHER RESEARCH

Does This Work in Practice?

Has Anyone Actually Done This?

In 2018, West-Virginia allowed voters to cast their ballot on a mobile phone through an app called **Voatz**:

- Voatz claims to use a blockchain, biometrics, a mixnet, and hardware-backed key storage module on the user's device
- Blockchain is only used in data centers (AWS/Azure), phones are not part of chain integrity
- Independent security analysis found serious vulnerabilities and limited benefit from the blockchain layer

Has Anyone Actually Done This?

Helios focuses on open audit voting and usability rather than blockchain:

- Helios is: open-audit, web-based and anonymous but not on blockchain
- Product bridges gap in user's technological understanding through a clean, simple UI
- Designed for small communities, student governments, clubs because they cannot mitigate coercion risks
- Offers secret ballots and public auditability

Has Anyone Actually Done This?

Academic projects push the boundaries further by combining blockchain with advanced cryptography to protect anonymity:

- Some academic prototypes combine private chains, mixers, and homomorphic encryption for anonymous tallying
- Often run on custom testnets (Docker/Kubernetes) with Proof of Work for simplicity
- Results in strong privacy/security, but tested only on small toy examples and not deployed at scale

Existing Voting-Style Blockchain Approaches

Proof-of-Stake (PoS)

- PoS is effectively a weighted vote based on stake where proposals are validated by economic actors
- Our system avoids token-based voting because there is no need for stake when no proposal is invalid

DAOs: Two Common Models

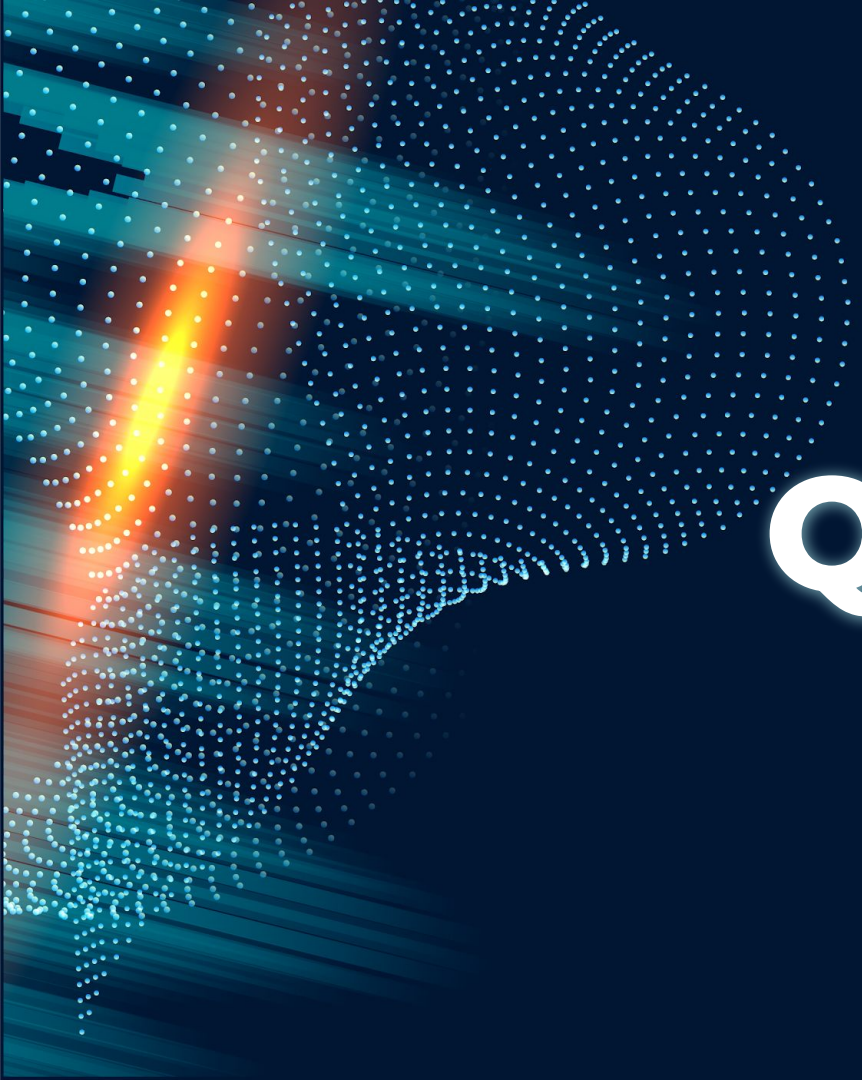
- Token-based: # tokens = # votes. Tokens can be bought/sold like crypto
- Wallet-based: 1 wallet = 1 vote. Must bind an identity to the wallet
- Our system is a hybrid of these two models

Why Large-Scale Success Is Still Missing

Key real-world barriers: transaction fees, endpoint security, voter privacy, coercion, identity management, and scalability

Next Steps:

- Short-term improvements to explore: cheaper networks or private chains, gas sponsorship, commit-reveal schemes, mixers, homomorphic tallying
- Longer-term research: privacy-preserving tallying at scale, decentralized identity management



QUESTIONS

?

Works Cited

Adida, B. (n.d.). *Helios: Web-based open-audit voting*. https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf

Michael A. Specter, James Koppel, & Daniel Weitzner. (n.d.). *The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in u. S. Federal elections.* https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

Pereira, B. M. B., Torres, J. M., Sobral, P. M., Moreira, R. S., Soares, C. P. d. A., & Pereira, I. (2023). Blockchain-Based Electronic Voting: A Secure and Transparent Solution. *Cryptography*, 7(2), 27. https://doi.org/10.3390/cryptography7020027

Set up your dao governance in 8 steps | aragon resource library. (n.d.). Retrieved 1 December 2025, from https://www.aragon.org/how-to/set-up-your-dao-governance-in-8-steps

Understanding proof-of-stake: How pos transforms cryptocurrency. (n.d.). Investopedia. Retrieved 1 December 2025, from https://www.investopedia.com/terms/p/proof-stake-pos.asp