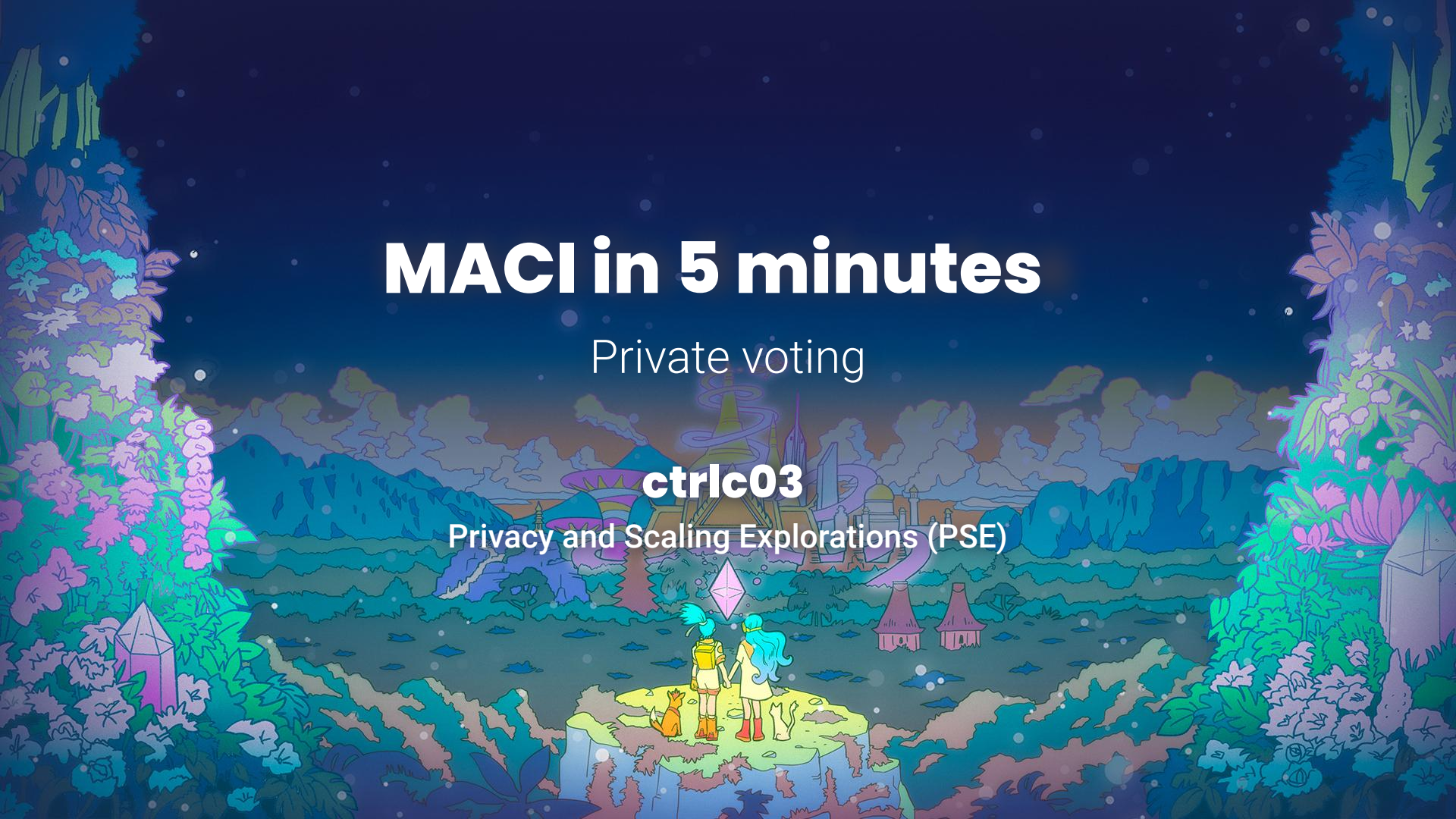


# MACI in 5 minutes

Private voting

**ctrlc03**

Privacy and Scaling Explorations (PSE)



# Agenda

- **What** is MACI
- **Why** do we need it
- **How** it works
- **The future**



# **Minimal Anti Collusion Infrastructure**



# Minimal Anti Collusion Infrastructure

- **Increased collusion resistance** - only the coordinator can be certain of the validity of a vote
- **Receipt-freeness** - cannot prove how you voted
- **Privacy** - only user and coordinator can decrypt a vote
- **Non-censorable** - no one can censor votes
- **Non-repudiation** - cannot edit or delete a vote, but can be nullified
- **Correct execution** - cannot produce false output



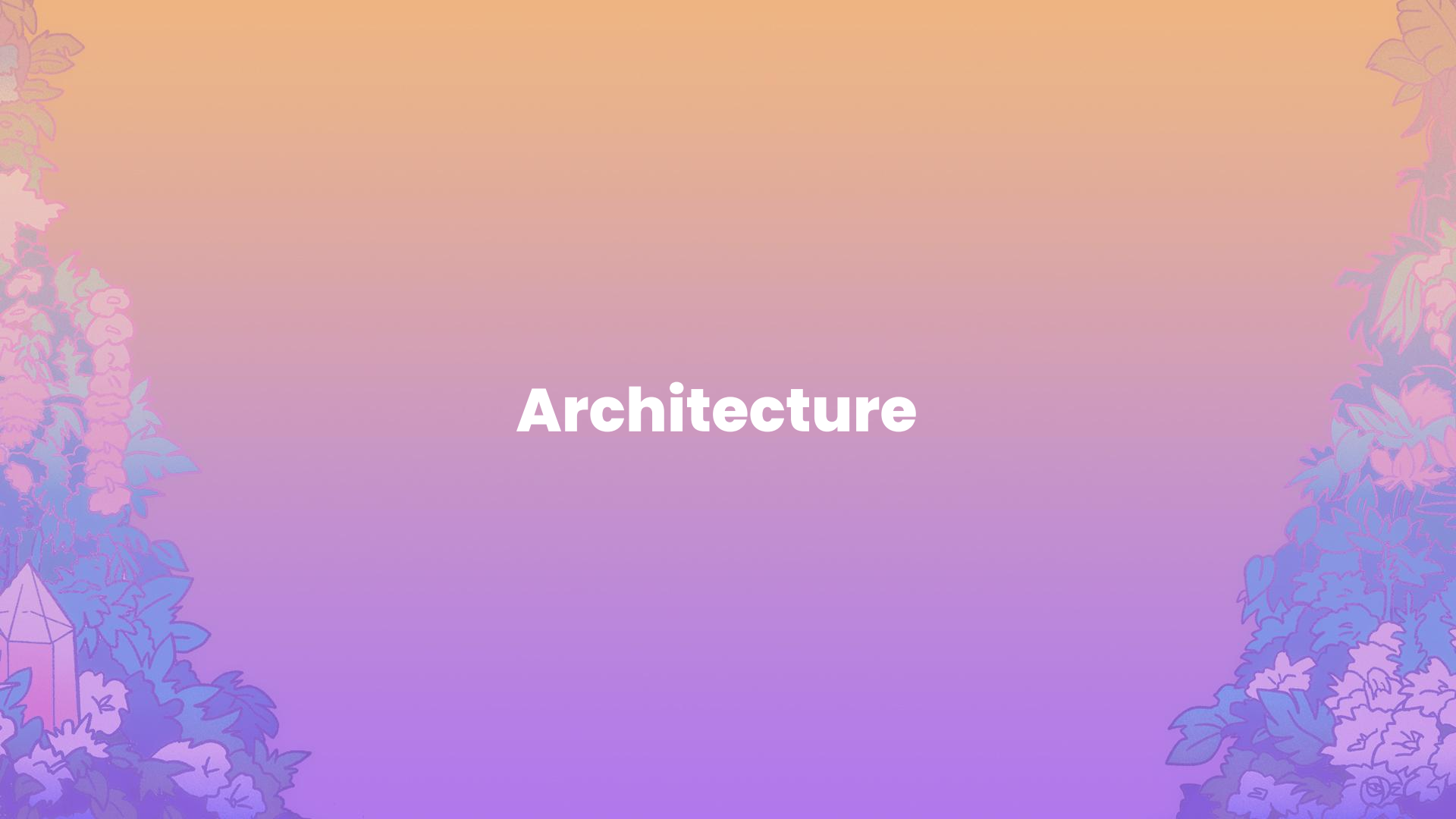
**Why do we need private voting?**



# Why do we need private voting

- Voting in general is susceptible to bribery/collusion
- In QF/QV the majority of people can make the difference
- If collusion is easy, then results can be gamed
- Public votes could condition other voters
- If a briber cannot be certain of your vote, why would they bribe you?
- Goal is more democracy in voting

# Architecture





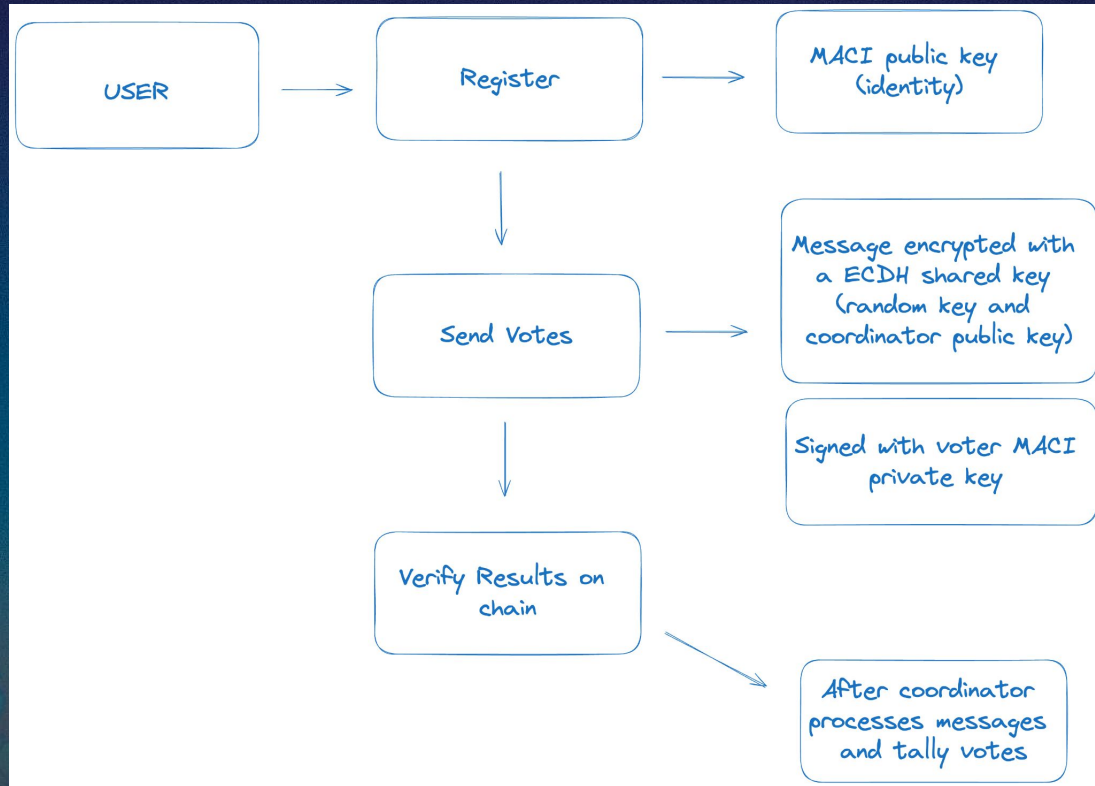
# Architecture

- **Smart contracts** - EVM compatible only
- **Circom circuits**
  - Process messages - validation of votes
  - Tally votes - summing them up
- **TypeScript**
  - Smart contracts clone for local coordinator processing
  - SDK to integrate with the protocol
  - Primitives (maci keys, encryption, hashing algorithms, Ballots, etc.)



# User Flow

# User Flow



# MACI Votes

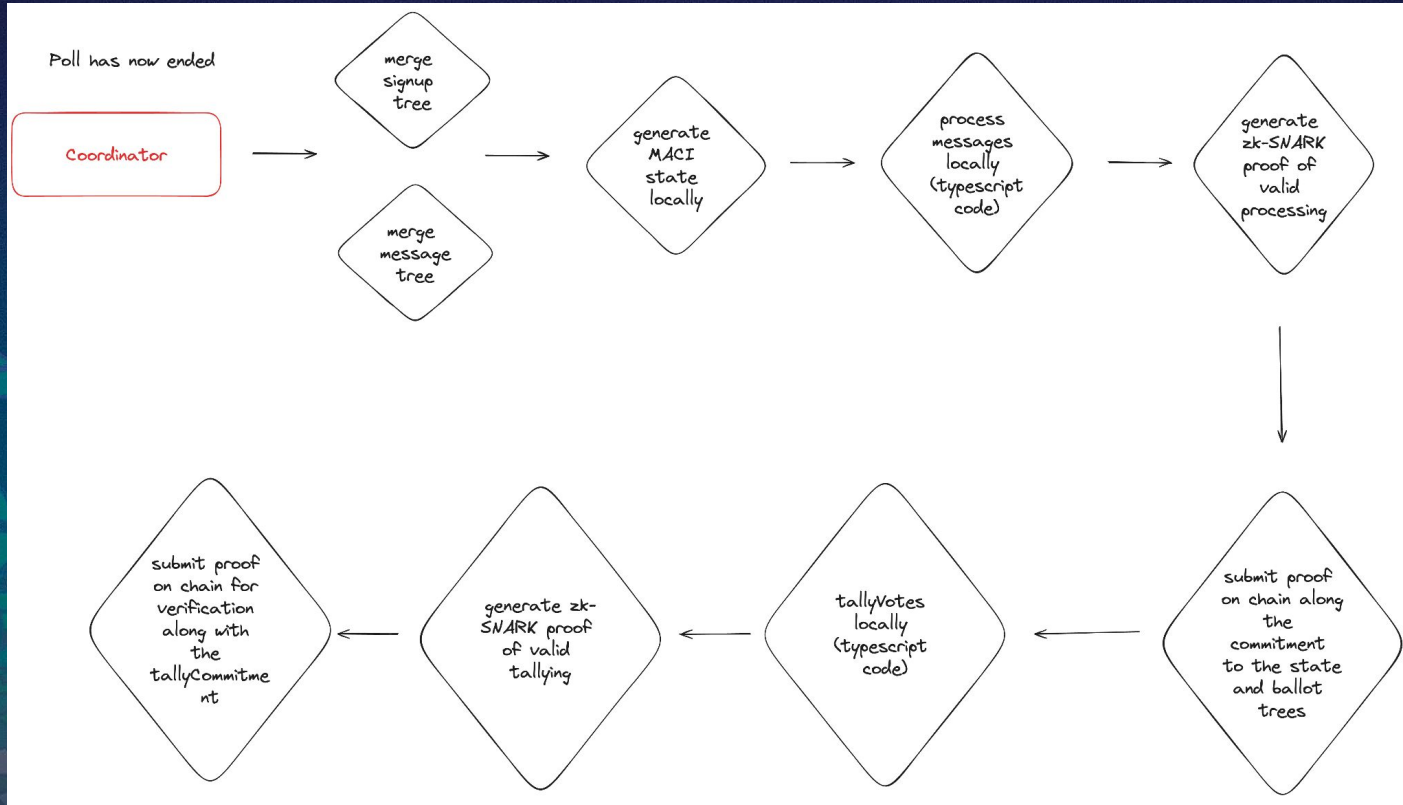


# MACI Votes

- **Shared key**
  - ECDH – ephemeral key and Coordinator public key
- Message is signed with **EDdSA**
- **Nonce** to track message order – can be used to invalidate previous votes
- **Vote weight**
- **User public key** (can pass in a new public key to change identify key)
- **Vote option**
- **The encryption public key** (ephemeral key)

# Poll Finalisation

# Poll Finalisation





# Our Plans

# Our Plans


- Improve adoption
- Improve ease of integration
- Decentralisation of the coordinator with MPC
- Research more anti collusion detection techniques
- Research new voting mechanisms that can be integrated into MACI
- Rethink the architecture and how (where) it fits with other protocols (Semaphore, RLN, Excubia)

# Devcon Round



# Devcon Round

Come and vote @ [vote.devcon.org](https://vote.devcon.org)




PROJECTS

MY BALLOT

LOGOUT

ROUND

 DASHBOARDS

VOTING POWER

0 OF 1000 VOTES USED

VOTING ENDS IN

11 Days 13 Hours 44 Minutes 24 Seconds

APPLICATION

11 - 11 Nov 2024

VOTING

11 - 24 Nov 2024


TALLYING

24 - 24 Nov 2024

RESULTS

24 - 24 Nov 2024


PROJECTS



**BUNDLEBEAR**

BundleBear tracks ERC-4337 smart account adoption. Smart accounts offer Ethereum users a 10X better UX than EOA wallets...


ADD TO BALLOT



**HILDOBBY'S DUNE DASHBOARDS**

I have created and maintain several dashboards, some of the most notable include: Ethereum staking, Ethereum blobs, Bitcoin ETFs...


ADD TO BALLOT



**BLOCKSCOUT - BLOCK EXPLORER**

Our open-source Ethereum block explorer offers detailed visibility into onchain activity, enabling users to track transactions, verify...


ADD TO BALLOT



**ETHROADMAP**

Ethroadmap aims to simplify Ethereum's Roadmap for everyday users, and to help them track past and future hard forks to the...


ADD TO BALLOT



**GROWTHEPIE.XYZ**

At growthpie we aim to make the usage of the Ethereum ecosystem as transparent and as accessible as possible. We help...


ADD TO BALLOT



**L2 BEHAVIORAL DASHBOARD**


The dashboard aggregates the current blobmarket saturation levels and then clearly demonstrates whether L2s are changing their...

ADD TO BALLOT



**DeFiScan**

ADD TO BALLOT



**Dune**

ADD TO BALLOT

# Thank you!

**ctrlc03**

Privacy and Scaling Explorations (PSE)

@ctrlc03 (Twitter/Telegram/GitHub)





**Any questions?**

