# TOWARDS A DECENTRALIZED AND PRIVACY-PRESERVING VOTING SYSTEM

IVAN MERCANTI


A.D. 1308
unipg
UNIVERSITÀ DEGLI STUDI
DI PERUGIA

05/02/2026

# AGENDA

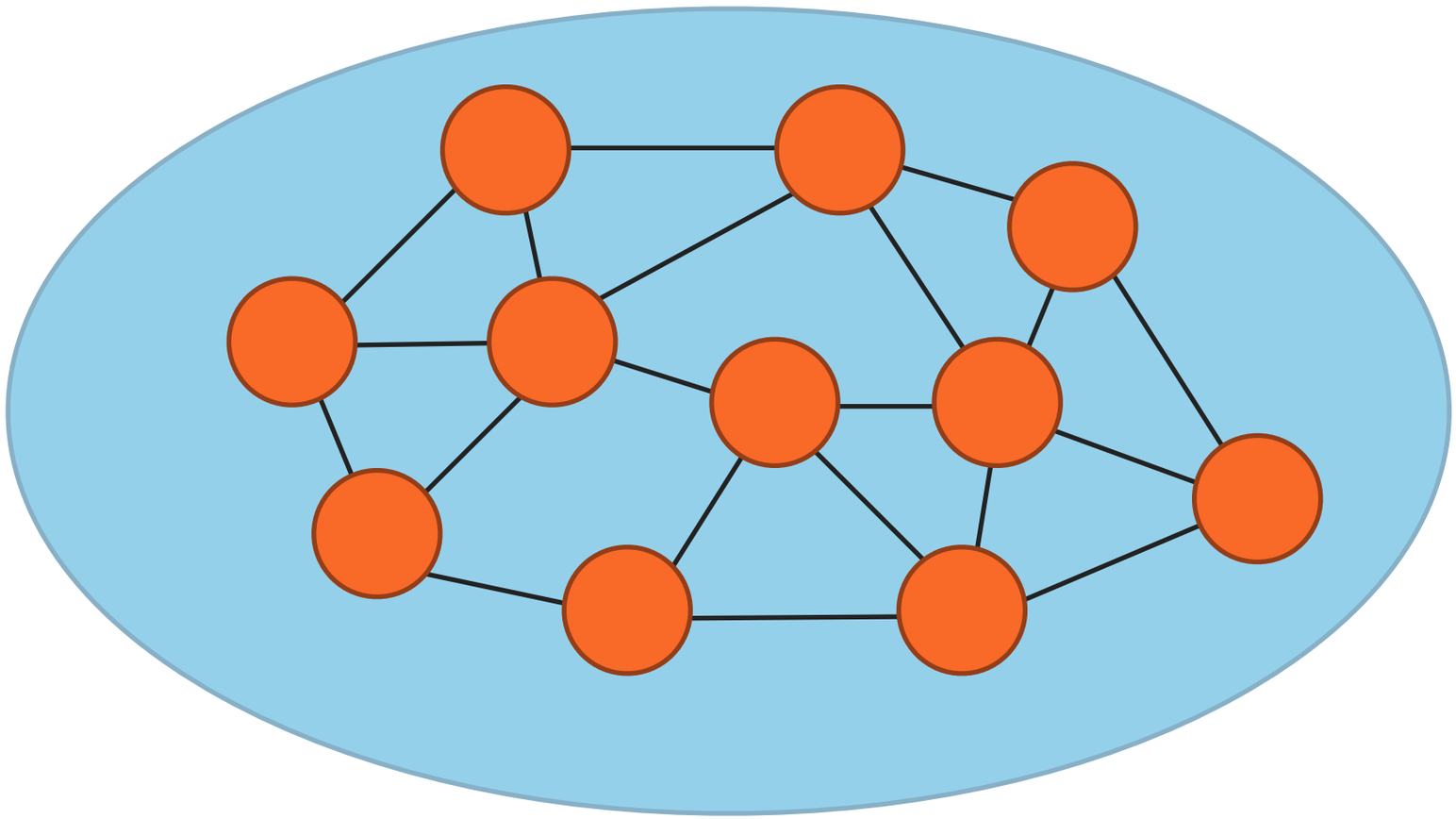
# AGENDA

- Background
- Bitcoin
- Multichain
- Ethereum
- Enigma
- Conclusion

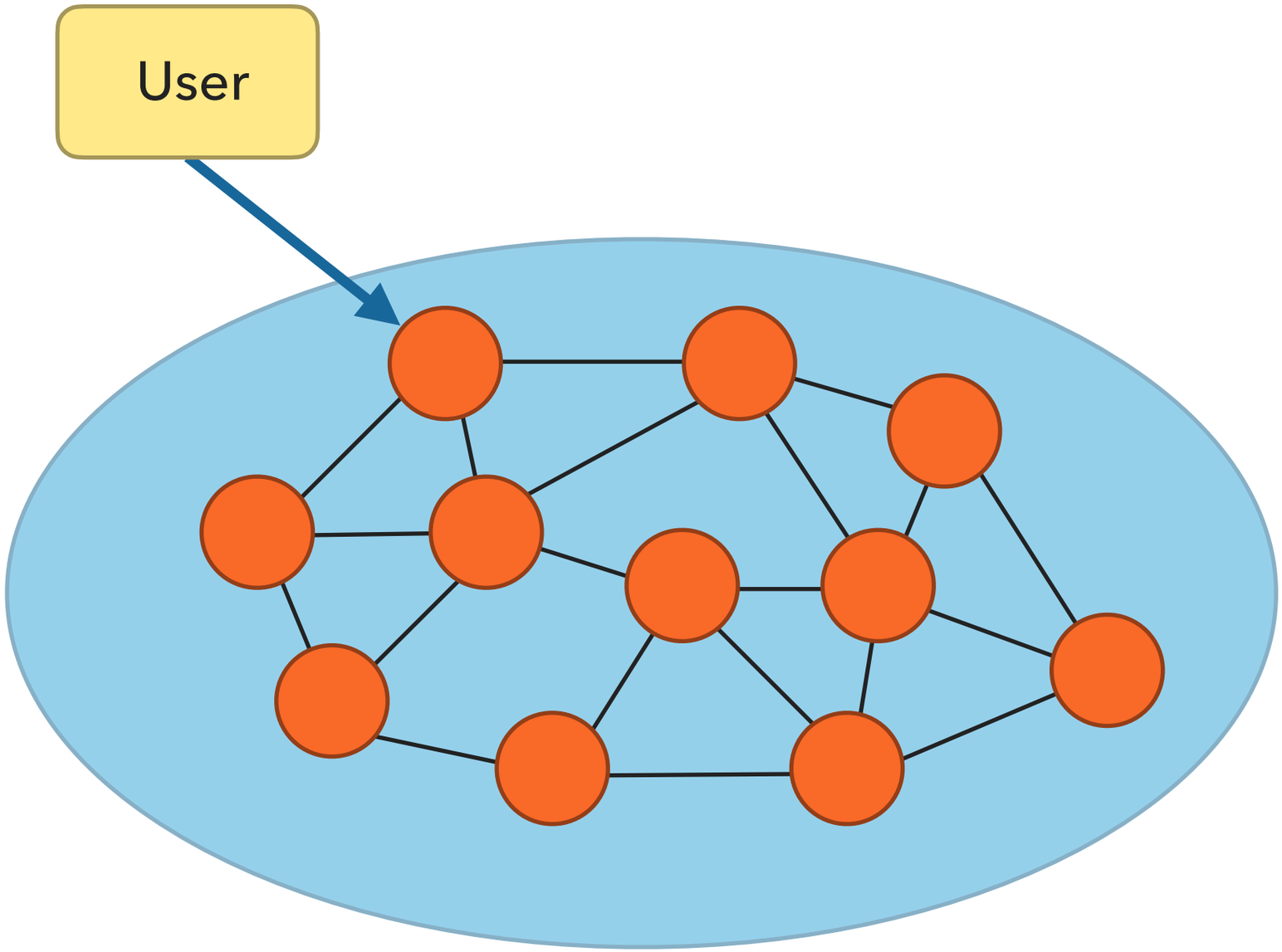
# VOTING PROPERTIES

- **Verifiability**: it is possible to verify that the counting of votes has been performed correctly.
- **Uniqueness**: a user is not allowed to vote more than once.
- **Integrity**: none can change or delete a vote without revealing it.
- **Privacy**: it is not possible to determine the vote of a user.
- **Counting**: the vote count has to be verifiable by everyone.
- **Authentication**: only users who have correctly identified themselves can vote.
- **Confidentiality**: intermediate results cannot be obtained during the proceedings.
- **Lack of evidence**: users cannot prove for whom they voted.
- **Reliability**: the voting system must be reliable and stable.

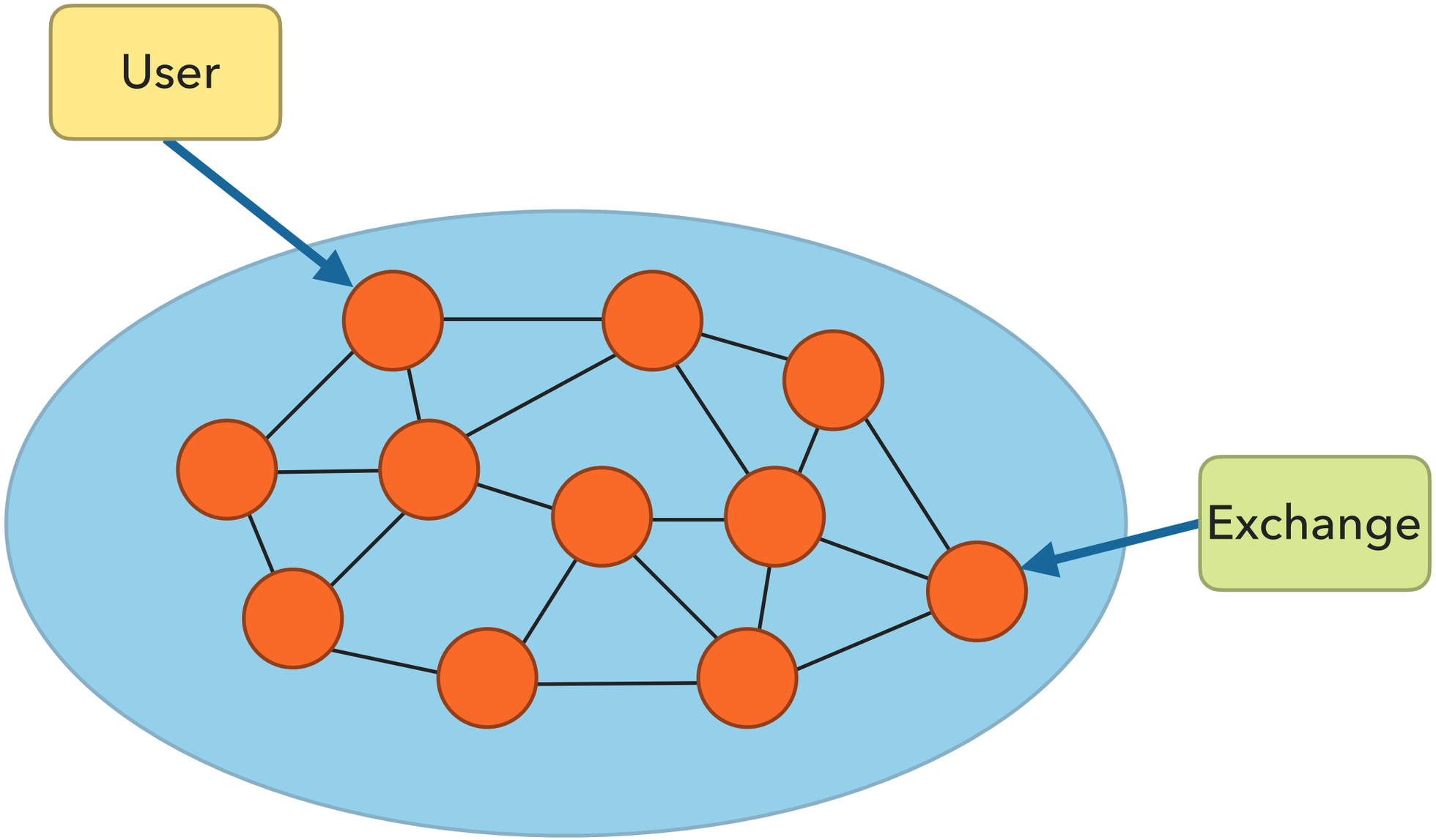
# SISTEMA BITCOIN



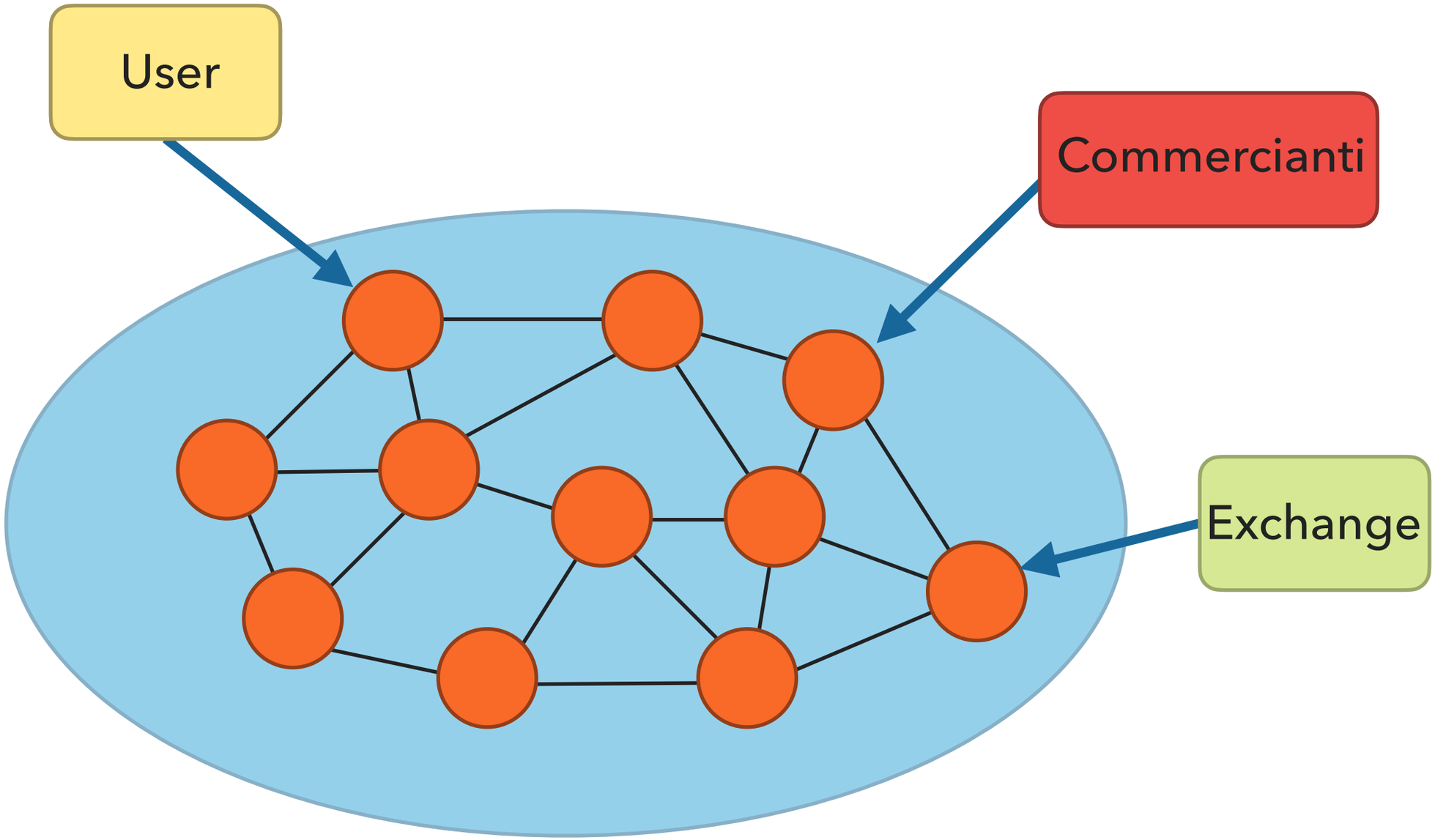
# SISTEMA BITCOIN



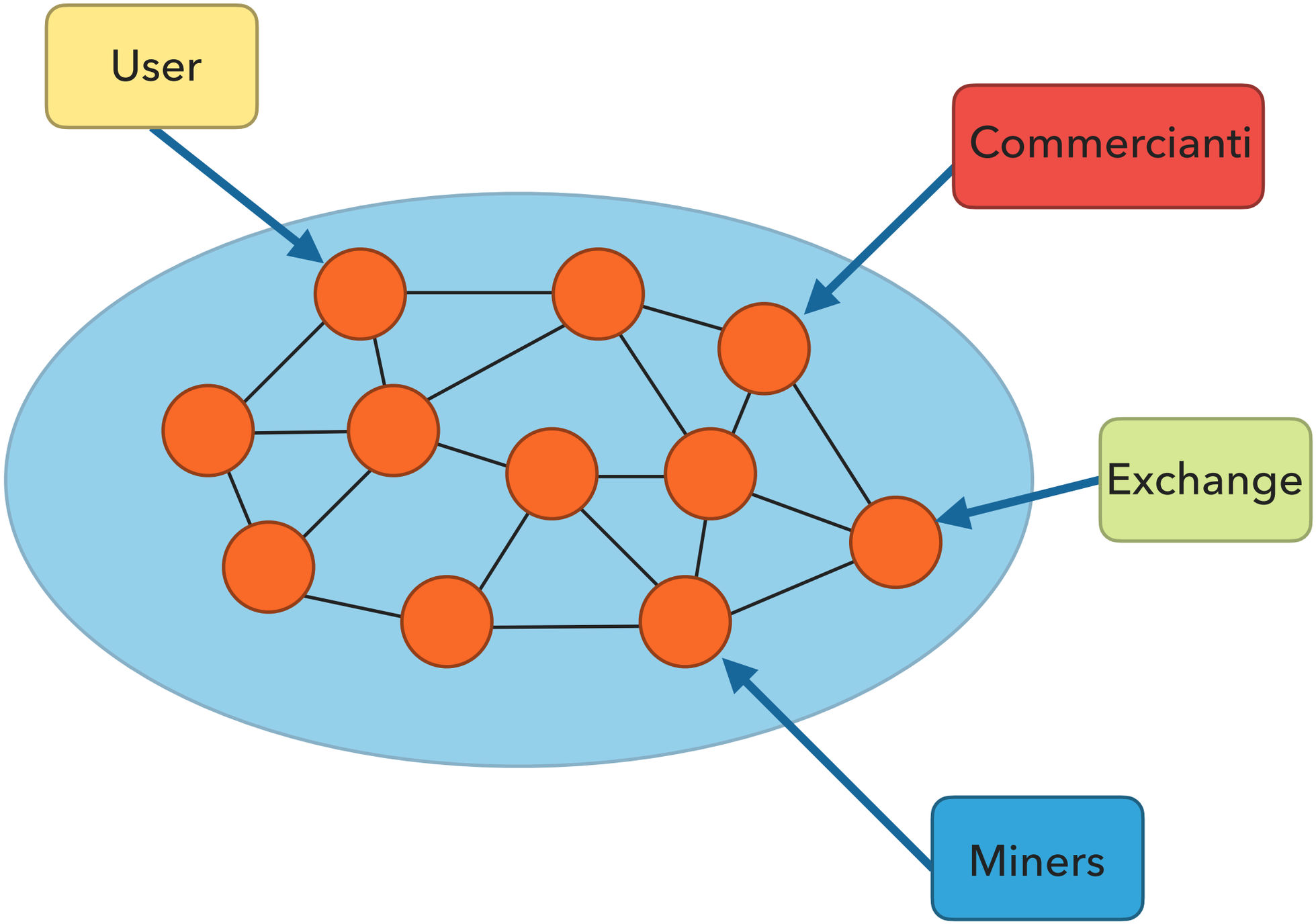
# SISTEMA BITCOIN



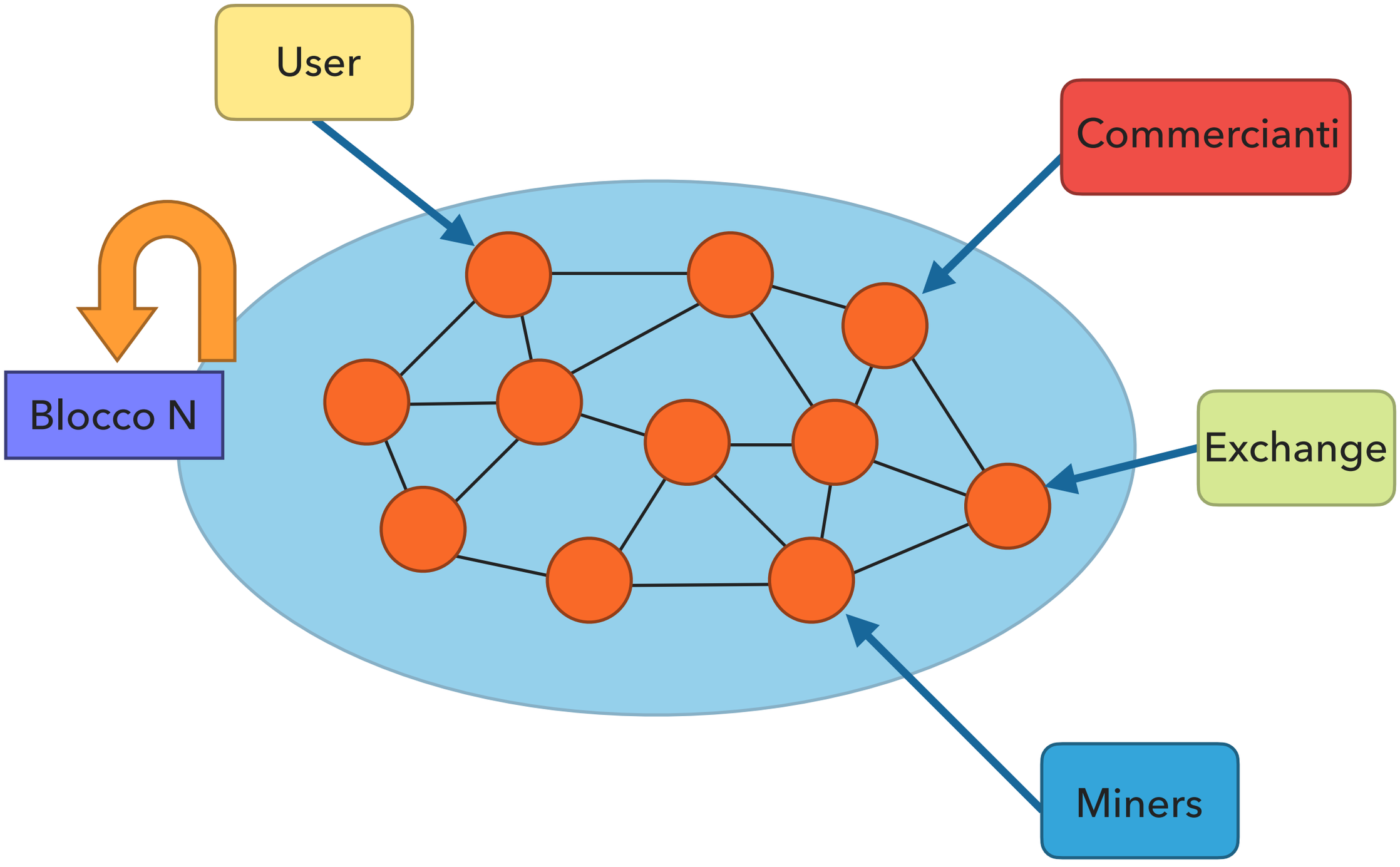
# SISTEMA BITCOIN



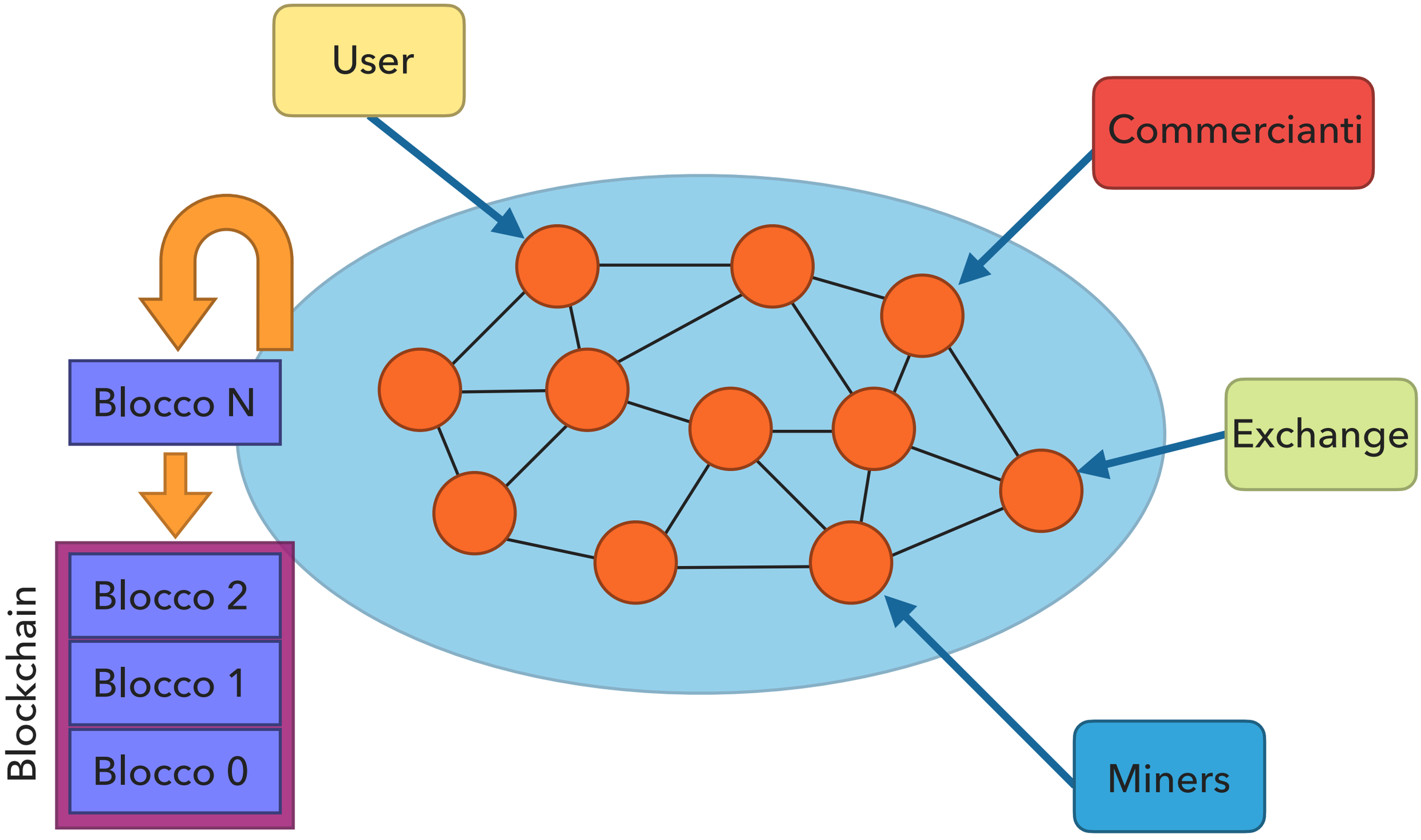
# SISTEMA BITCOIN



# SISTEMA BITCOIN



# SISTEMA BITCOIN



# BITCOIN

# CANDIDATE REGISTRATION

Candidate

Documentation

Identification

# CANDIDATE REGISTRATION

Candidate

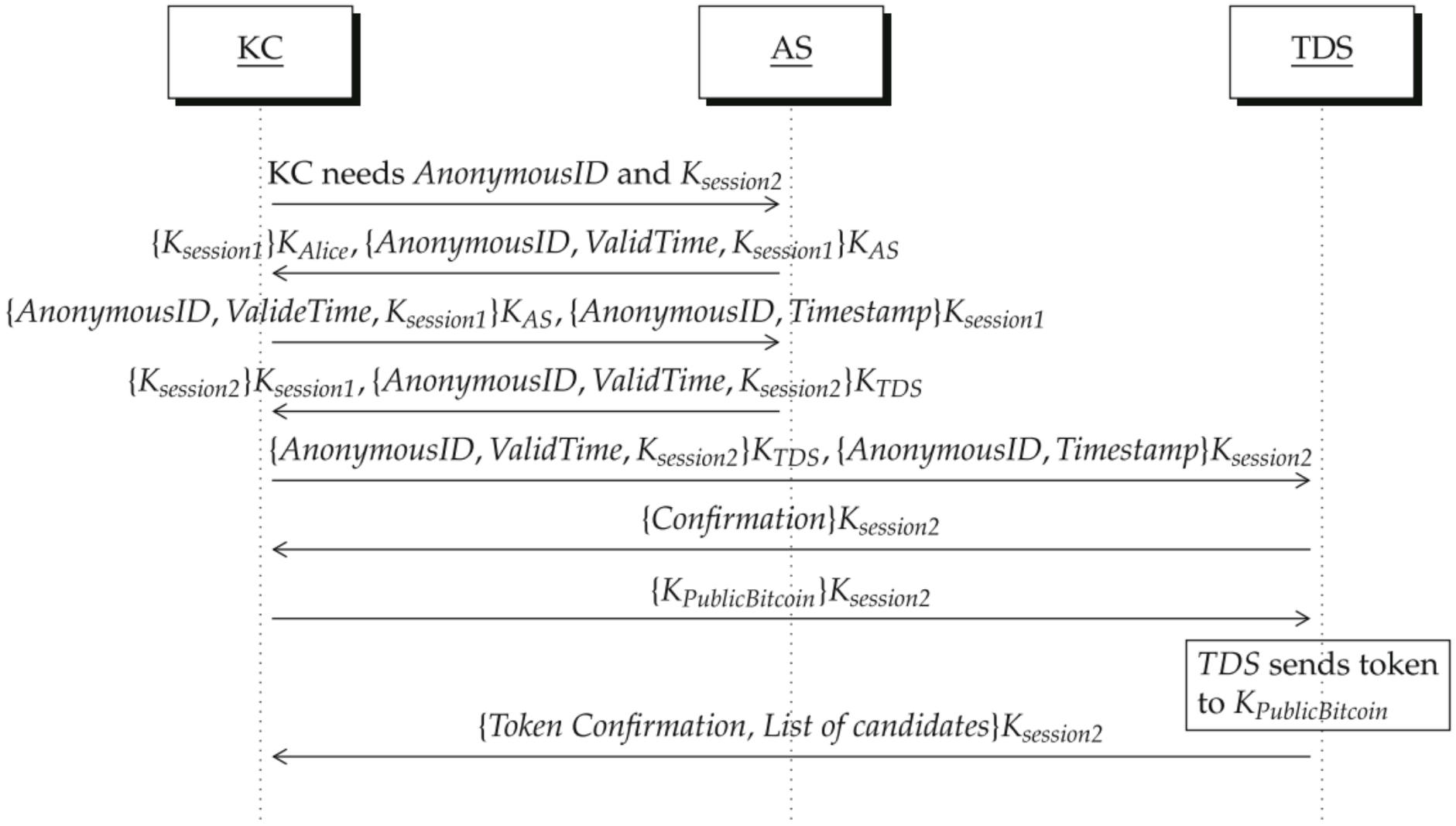
Documentation

Receive an Address

Identification

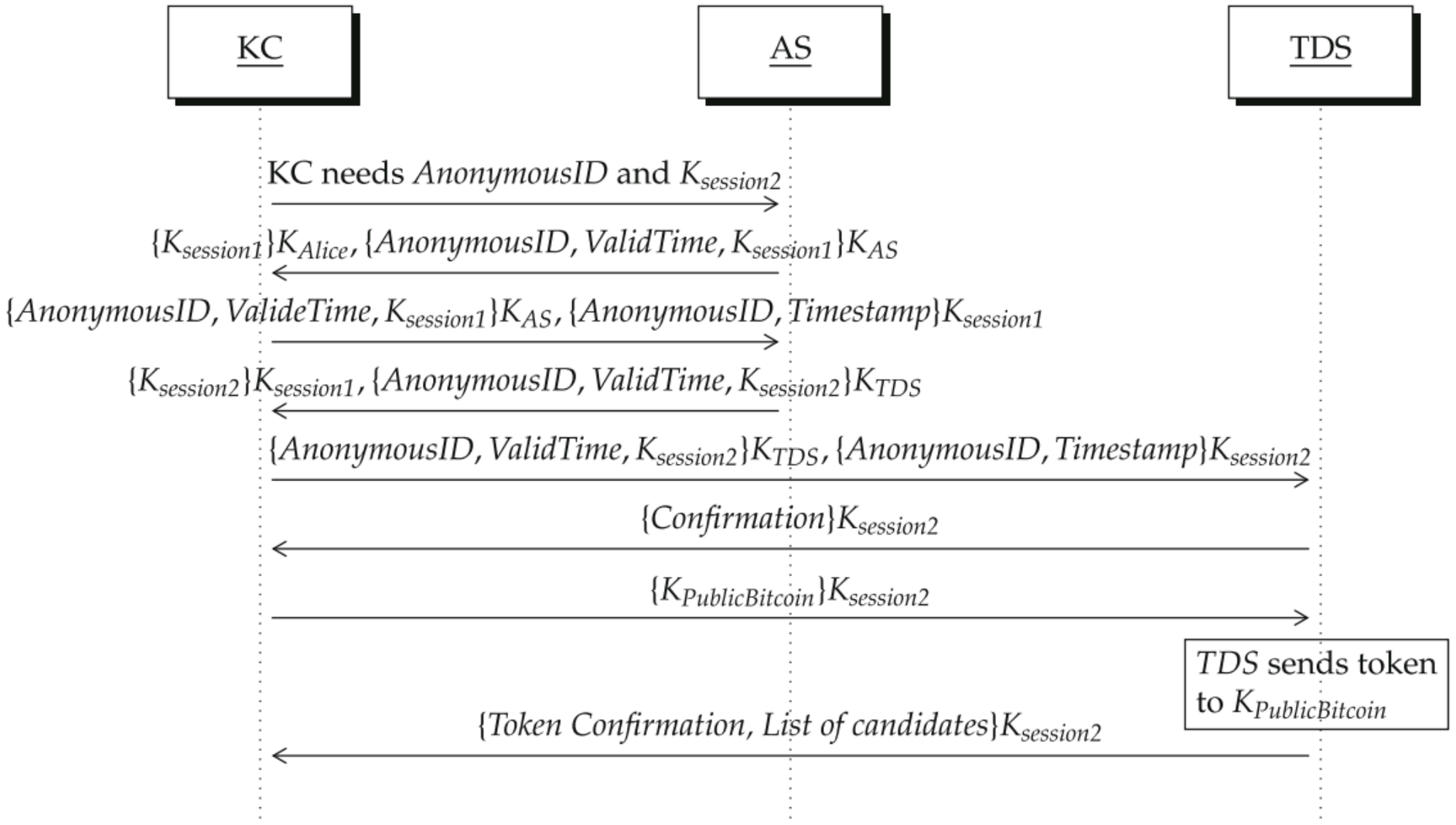
# VOTER REGISTRATION

Voter



# VOTER REGISTRATION

Voter



# VOTE PHASE

Voter

Vote (1 Satoshi or 1OAP)

Miner confirmed

Candidate

# VOTE PHASE

Voter

Vote (1 Satoshi or 1OAP)

Miner confirmed

Candidate

# COUNTING

Candidate

Wallet

# OUR PROPERTIES

- **Verifiability**
- **Uniqueness**
- **Integrity**
- **Counting**

# OUR PROPERTIES

- **Privacy** 

  Kerberos

- **Authentication** 

  Pre-voting phase

- **Confidentiality** 

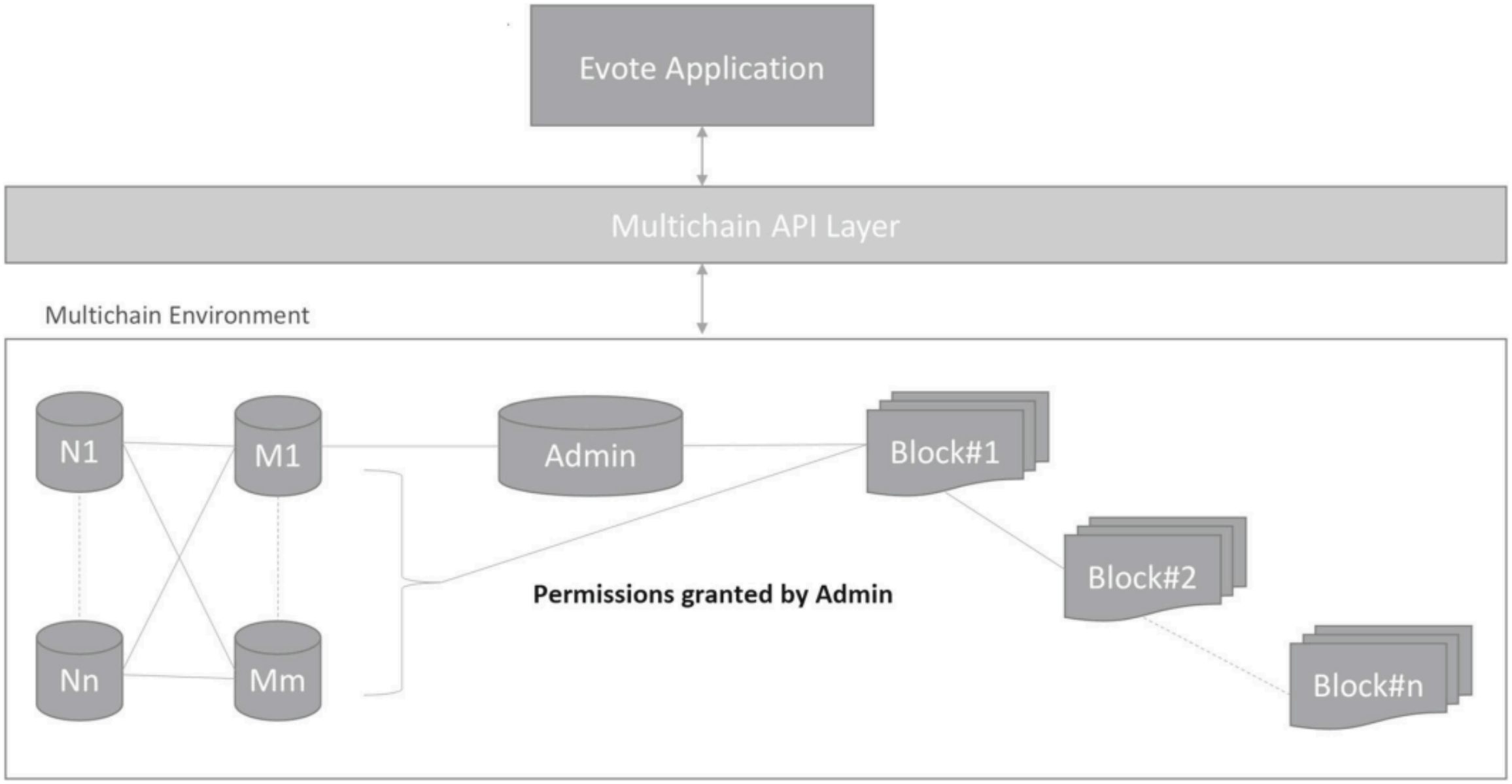
# OUR PROPERTIES

- **Lack of evidence**

- **Reliability**

# MULTICHAIN

# THE ARCHITECTURE

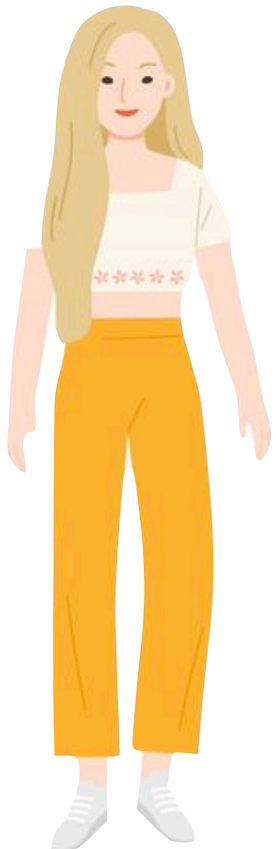


# CANDIDATE REGISTRATION

Admin

Register voter and Candidate

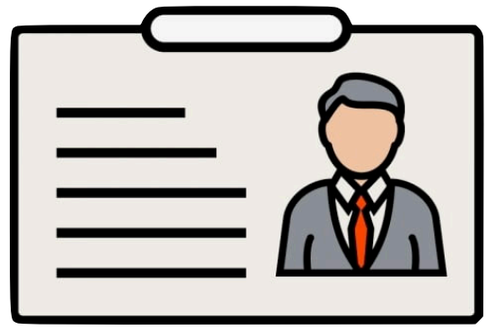
# CANDIDATE REGISTRATION



Voter

Documents

AnonymousID



Identification

AnonymousID

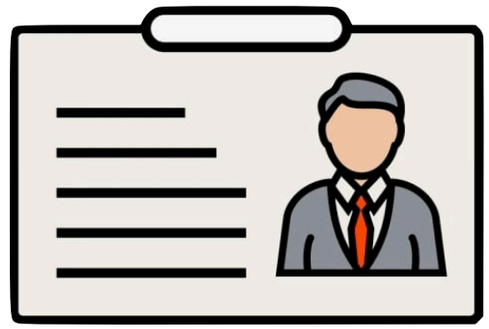
Token

# CANDIDATE REGISTRATION

Voter

Documents

AnonymousID



Identification

AnonymousID

Token

# OUR PROPERTIES

- **Verifiability**
- **Uniqueness**
- **Integrity**
- **Counting**

# OUR PROPERTIES

- **Privacy**

- **Authentication**

Pre-voting phase

- **Confidentiality**

# OUR PROPERTIES

- **Lack of evidence**

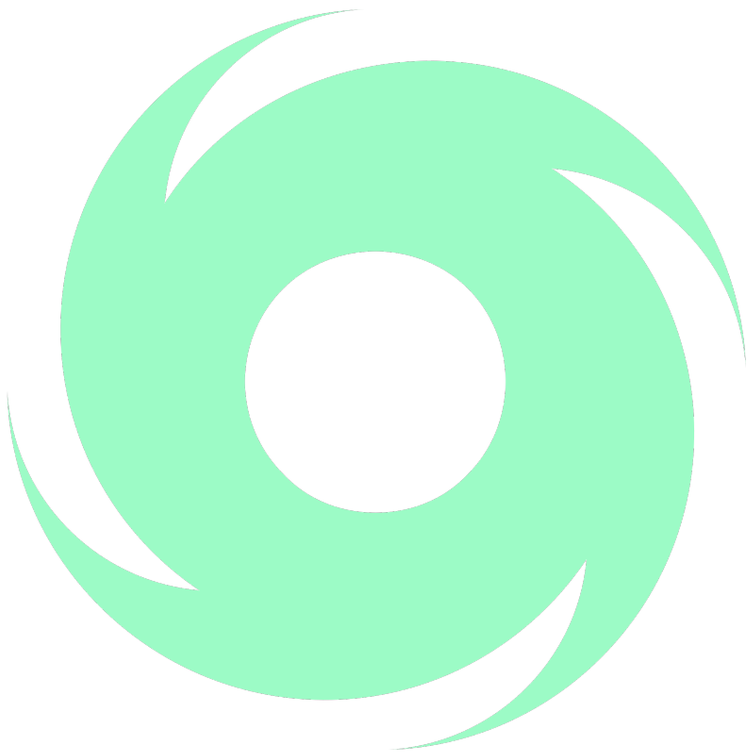
- **Reliability**




# THE ERC20 STANDARD

# TORNADO CASH

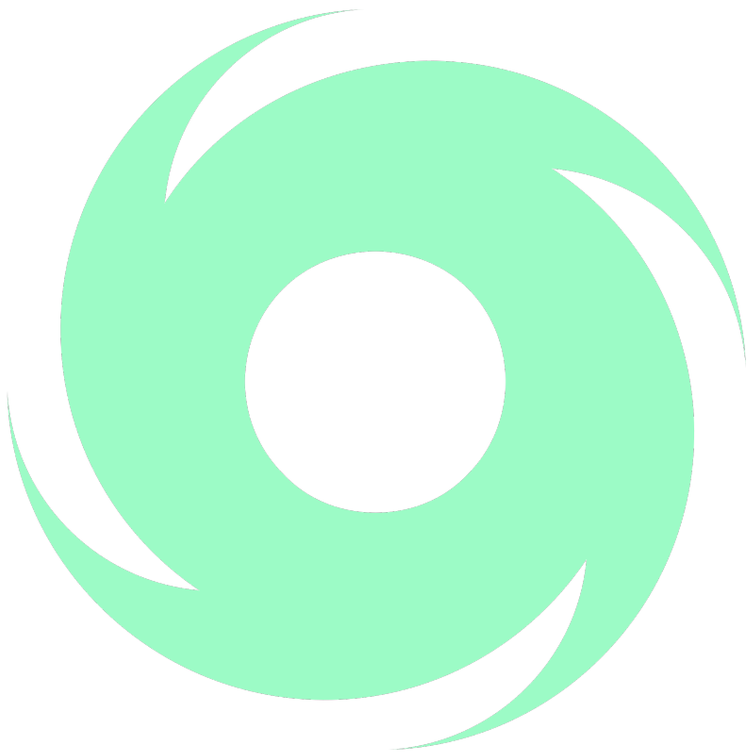
My Account



# TORNADO CASH

My Account

Deposit

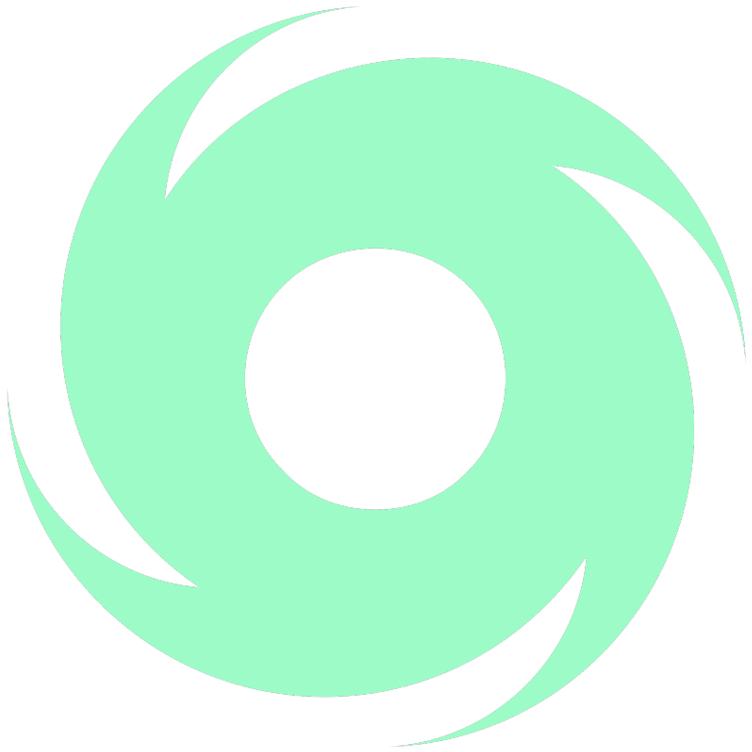


# TORNADO CASH

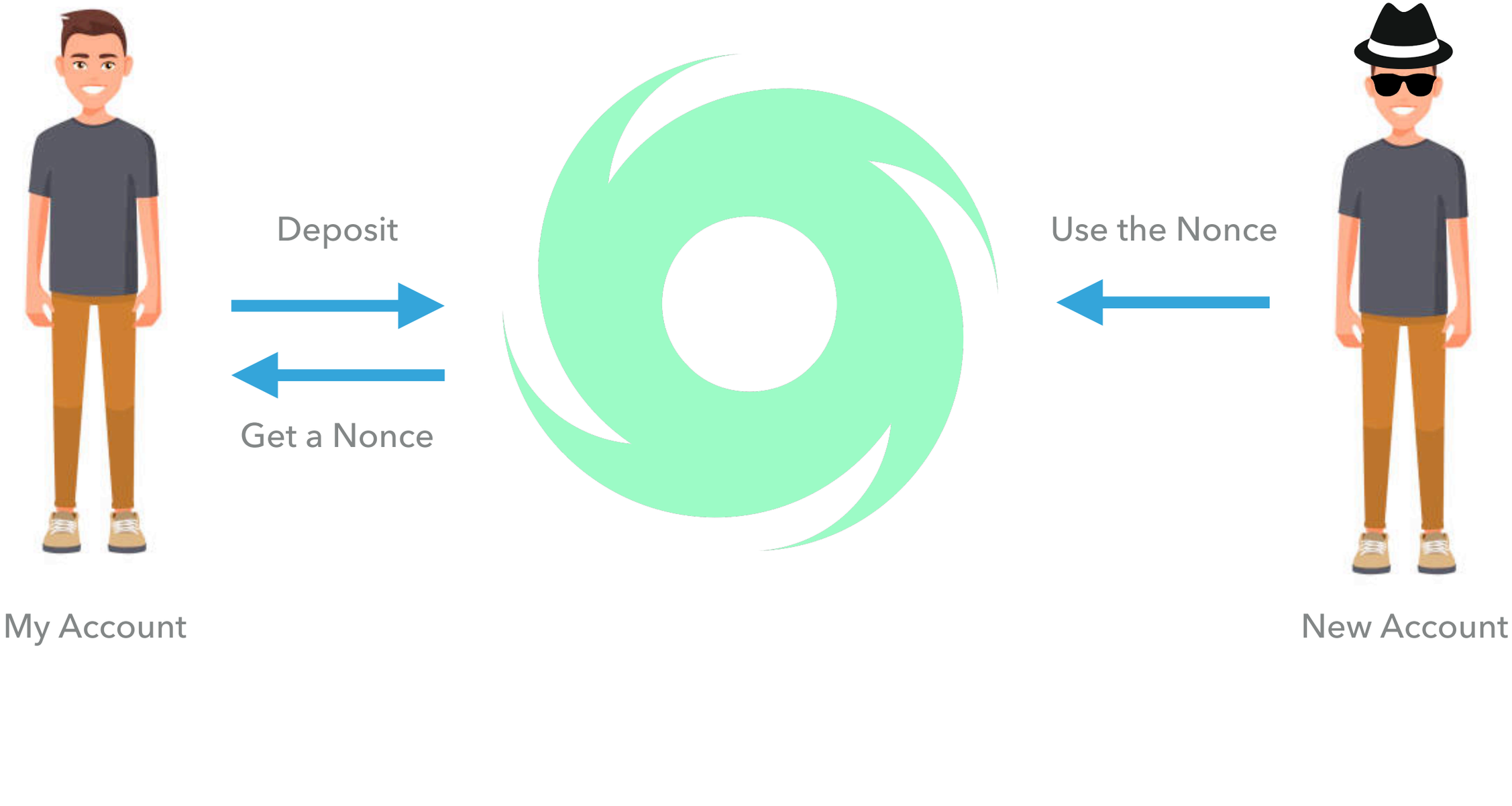
My Account

Deposit

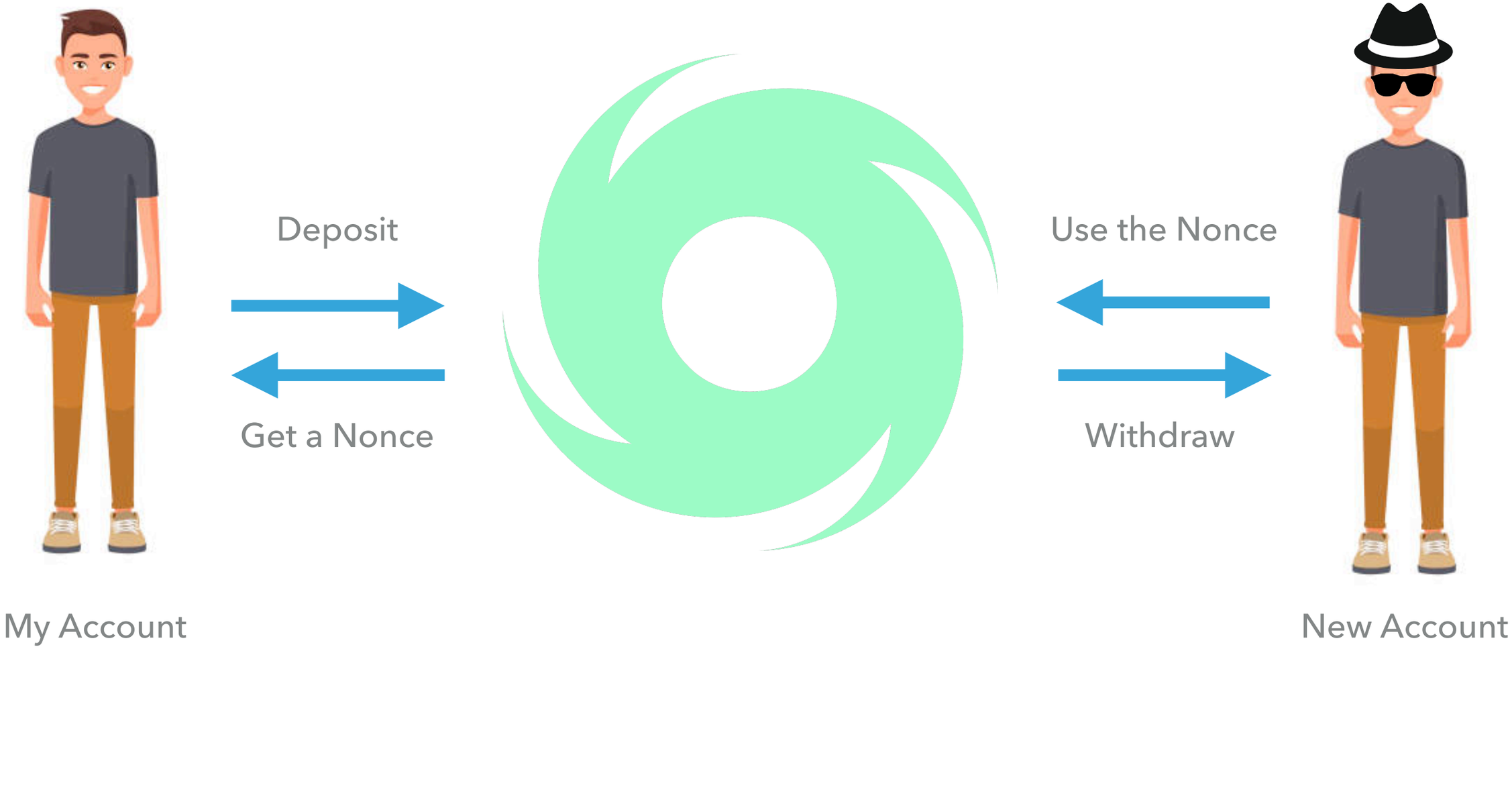
Get a Nonce



# TORNADO CASH



# TORNADO CASH



# FIRST STEP

Admin

User

# FIRST STEP

DTV (ERC20) token

Admin

Deploy

User

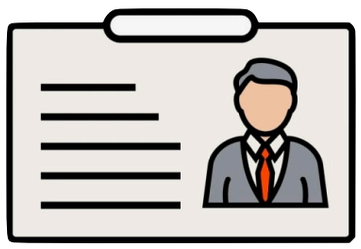
# FIRST STEP

Admin

Deploy

DTV (ERC20) token

Handle



User Identification

User

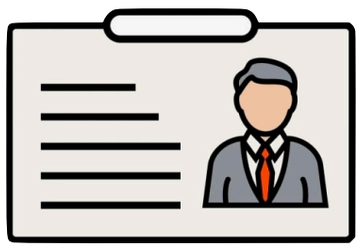
# FIRST STEP

Admin

Deploy

DTV (ERC20) token

Handle

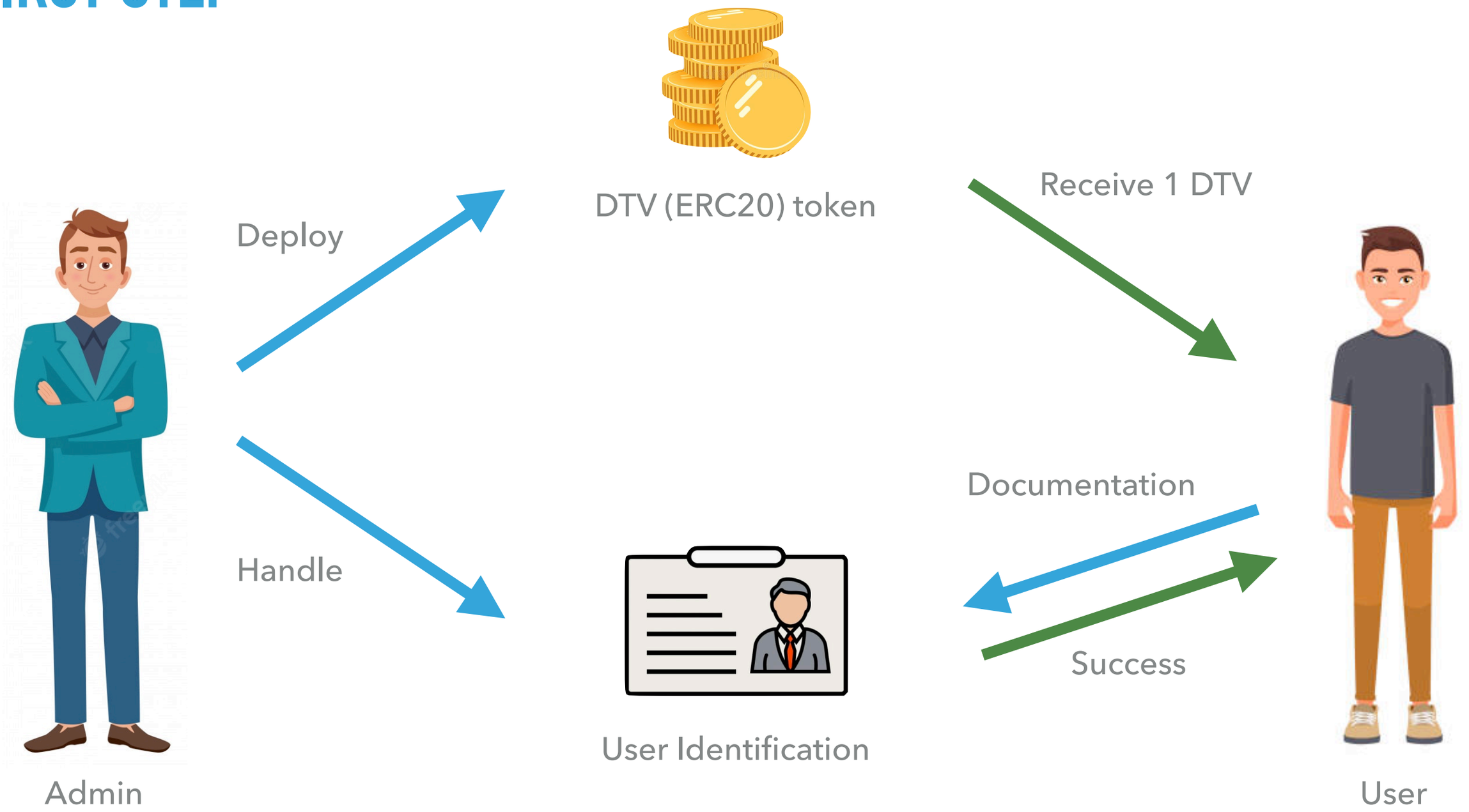


User Identification

Documentation

User

# FIRST STEP


Deploy
DTV (ERC20) token
Receive 1 DTV
Handle
Documentation
Success
User Identification
Admin
User

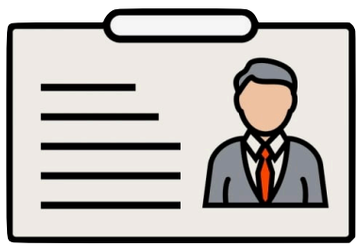
# FIRST STEP

Admin

Deploy

DTV (ERC20) token

Handle



User Identification

Documentation

Fail

User

# PSEUDO-ANONYMIZATION

Admin

User

# PSEUDO-ANONYMIZATION

Admin

Deploy


TornadoCash-Relayer SC

User

# PSEUDO-ANONYMIZATION

Admin

Deploy

Set


TornadoCash-Relayer SC

Deposit expired time

User

# PSEUDO-ANONYMIZATION

Admin

Deploy

Set


TornadoCash-Relayer SC

Deposit expired time

Deposit 0.0015 ETH and 1 DTV

Receive a Nonce

User

# PSEUDO-ANONYMIZATION

Admin

Deploy

Set


TornadoCash-Relayer SC

Deposit expired time

Provide the Nonce

Withdraw 0.0015 ETH and 1 DTV

User

# VOTE

Admin

User

# VOTE

Admin

Deploy


Voting SC

User

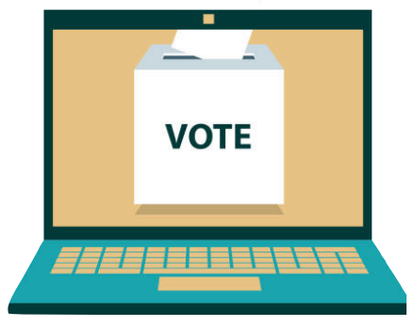
# VOTE

Admin

Deploy


Voting SC

Public




Vote Webpage

User

# VOTE

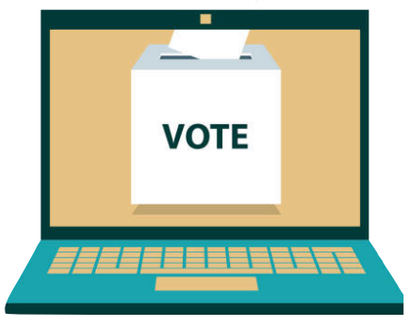
Admin

Deploy

Public


Voting SC

Vote




Vote Webpage

Send 1 DTV to vote

User

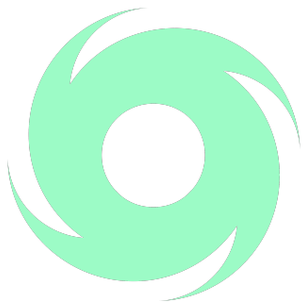
# OUR PROPERTIES

- **Verifiability**
- **Uniqueness**
- **Integrity**
- **Counting**



# OUR PROPERTIES

- **Privacy**



- **Authentication**

Admin

- **Confidentiality**

# OUR PROPERTIES

- **Lack of evidence**

- **Reliability**

# VOTE

Admin

User

# VOTE

Admin

Deploy


Voting SC

User

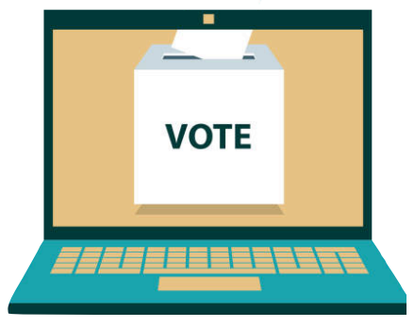
# VOTE

Admin

Deploy


Voting SC

Public




Vote Webpage

User

# VOTE

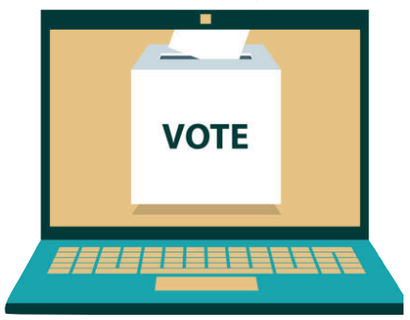
Admin

Deploy

Public


Voting SC

Vote




Vote Webpage

Send 1 DTV to vote

User

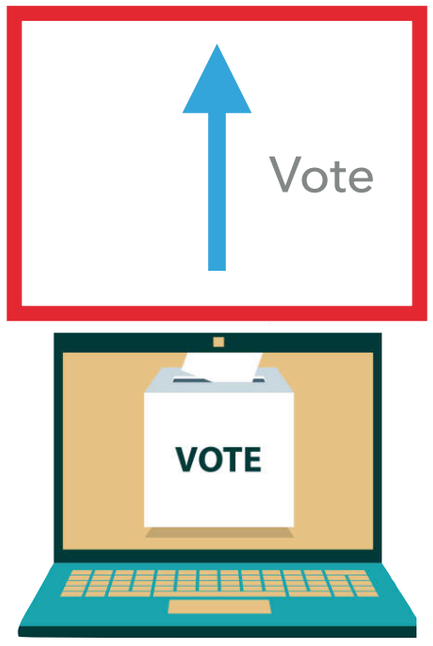
# VOTE

Admin

Deploy

Public


Voting SC




Vote Webpage

Send 1 DTV to vote

User

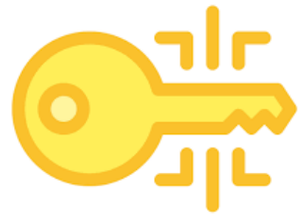
# VOTE ENCRYPTION

Candidates

Voting SC

User

# VOTE ENCRYPTION



Register

Public keys

Voting SC

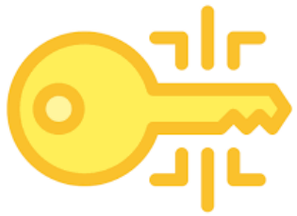
Candidates

User

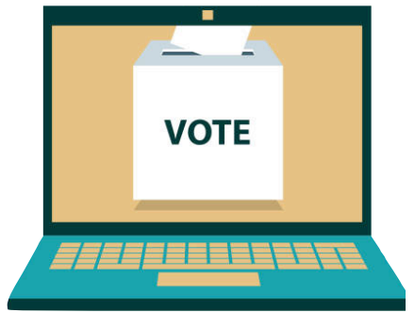
# VOTE ENCRYPTION

Candidates

Register



Public keys



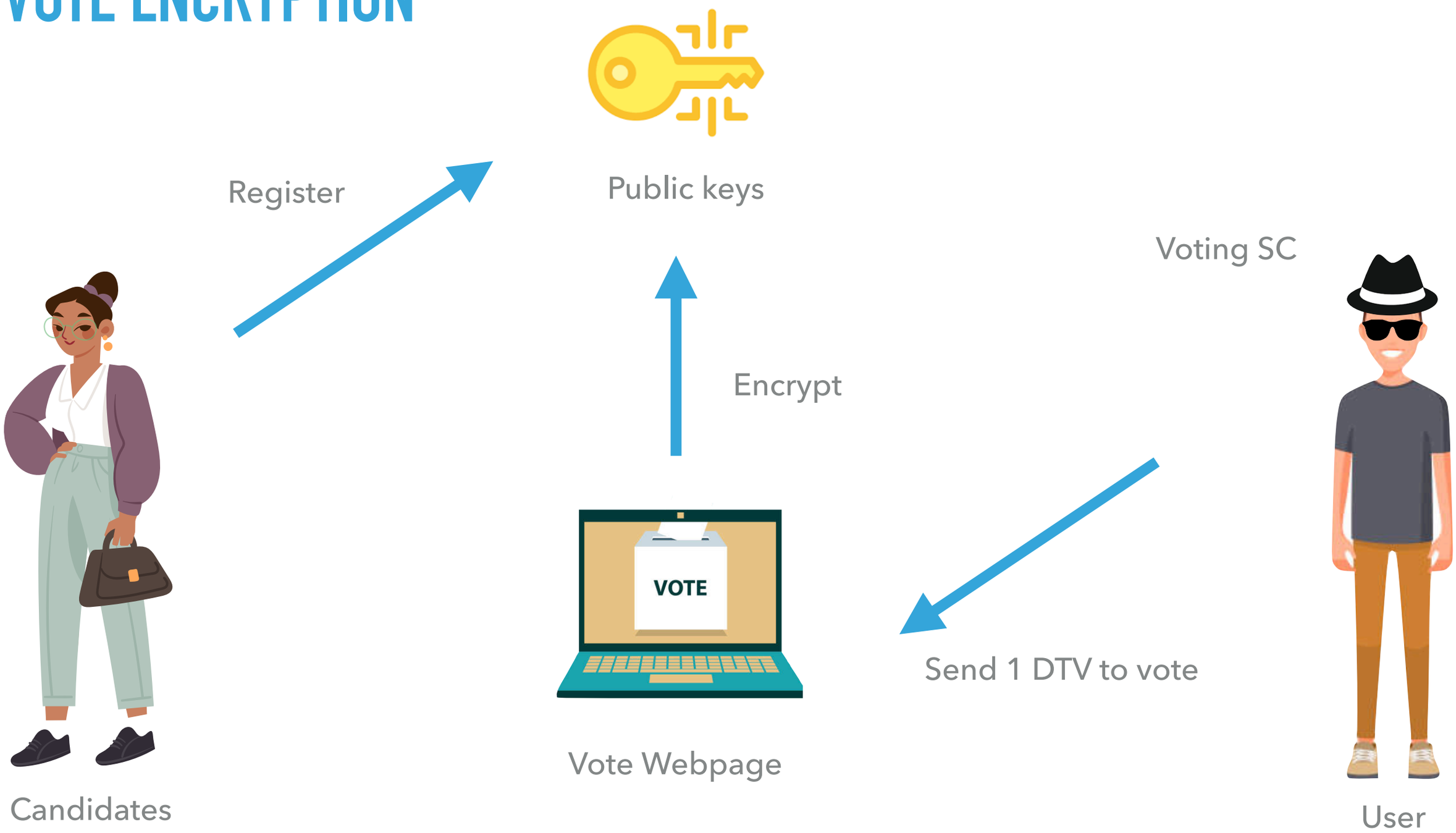

Vote Webpage

Send 1 DTV to vote

Voting SC

User

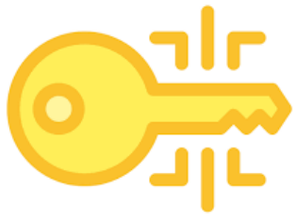
# VOTE ENCRYPTION



# VOTE ENCRYPTION

Candidates

Register

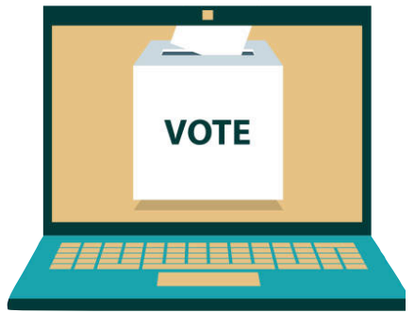


Public keys

Encrypt vote


Voting SC

Encrypt




Vote Webpage

Send 1 DTV to vote

User

# VOTE COUNTING

Candidates

Admin

# VOTE COUNTING

Private keys

Reveal

Candidates

Admin

# VOTE COUNTING

Private keys

Get votes


Voting SC

Reveal

Candidates

Admin

# VOTE COUNTING

Private keys

Get votes


Voting SC

Reveal

Candidates

Decryption


Decrypted Votes

Admin

# VOTE COUNTING

Private keys

Get votes


Voting SC

Reveal

Candidates

Decryption


Decrypted Votes

Counting

Admin

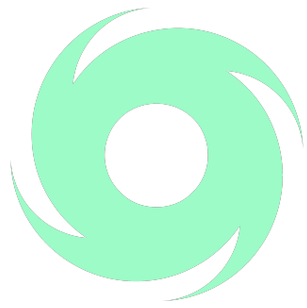
# OUR PROPERTIES

- **Verifiability**
- **Uniqueness**
- **Integrity**
- **Counting**



# OUR PROPERTIES

- **Privacy**



- **Authentication**

Admin

- **Confidentiality**



Encryption

# OUR PROPERTIES

- **Lack of evidence**

- **Reliability**

enigma

# ENIGMA

# K-TIMES ANONYMOUS AUTHENTICATION

Group Manager

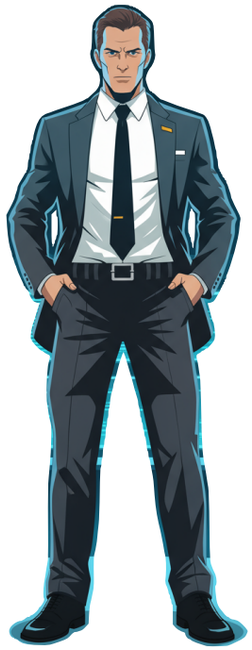
Service Providers

Users

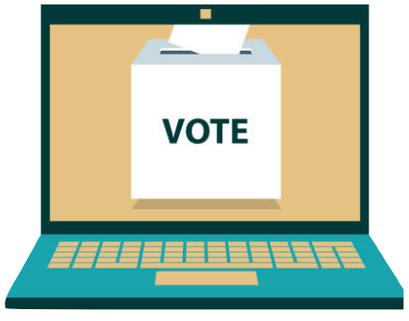
I. Teranishi, J. Furukawa, and K. Sako, “k-times anonymous authentication,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol. 92-A, no. 1, pp. 147–165, 2009.

# ARCHITECTURE

Group Manager



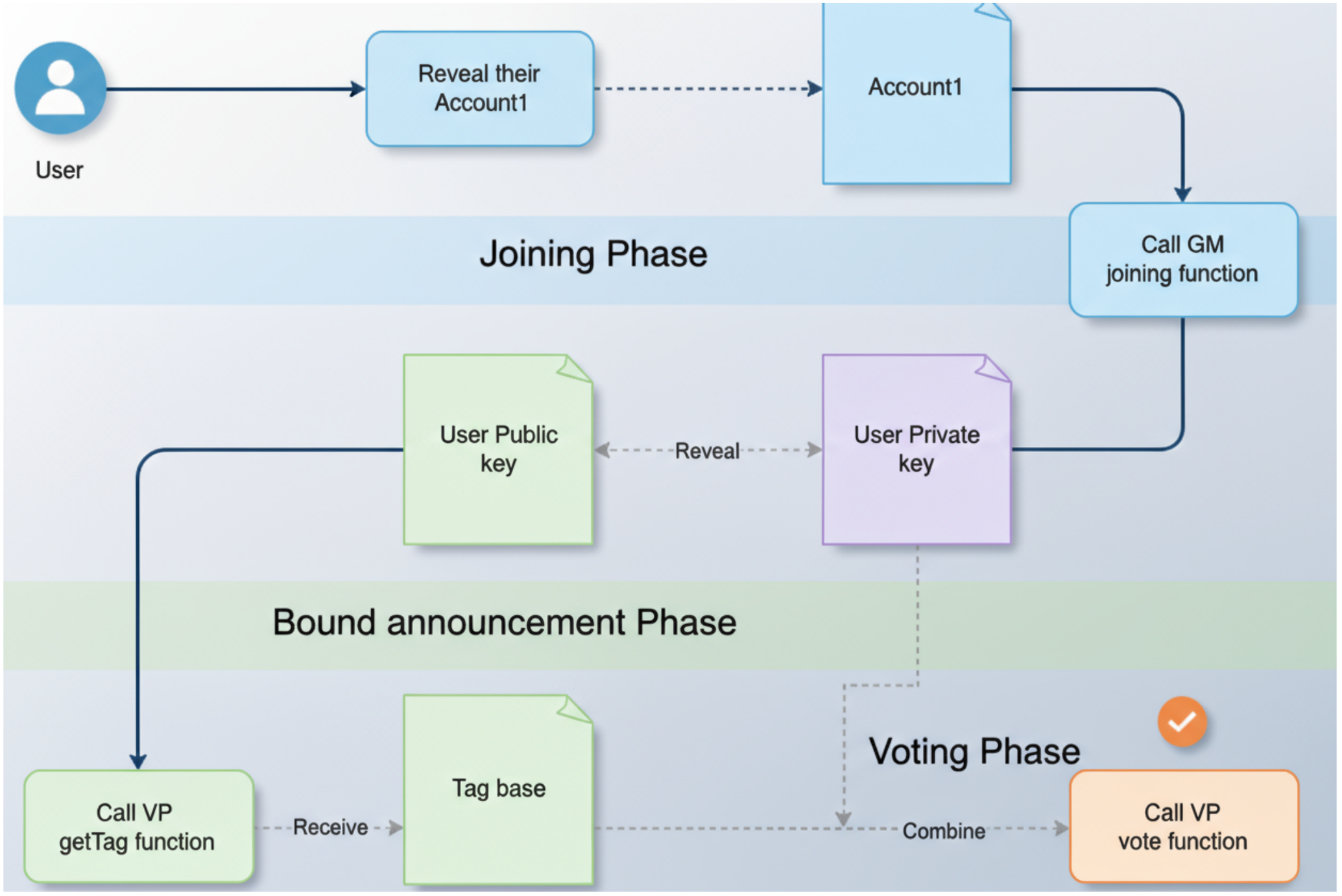
Admin




Voting Providers

Users

# ACTIVITY DIAGRAM



# KEY PHASES

- Setup: GM creates cryptographic parameters and proofs.
- Joining: Users register and receive public/secret keys.
- Bound Announcement: Tag base (voting card) distributed.
- Voting: User votes anonymously via Account2.
- Public Tracing: Detects double voting while preserving anonymity.
- Counting: Results verifiable on-chain.

# OUR PROPERTIES

- **Verifiability**
- **Uniqueness**
- **Integrity**
- **Counting**



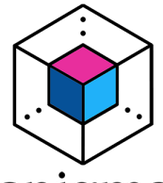


k-times anonymous authentication

# OUR PROPERTIES

- **Privacy**

k-times anonymous authentication




- **Authentication**

k-times anonymous authentication

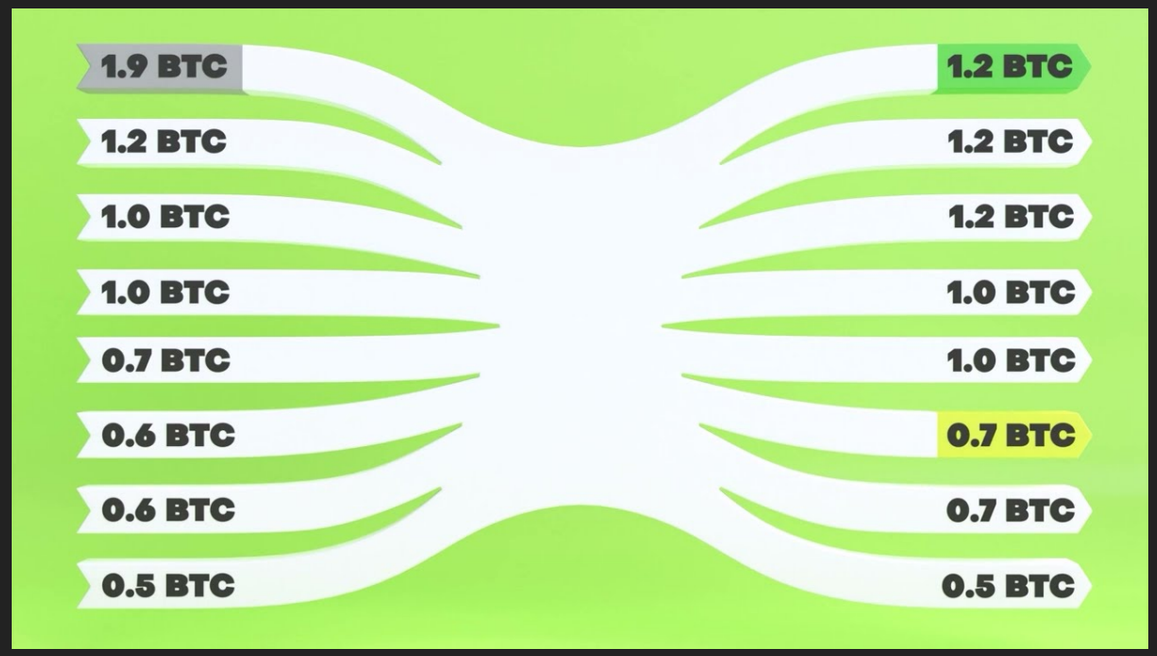
- **Confidentiality**

k-times anonymous authentication

# OUR PROPERTIES

- **Lack of evidence**

- **Reliability**


1.9 BTC
1.2 BTC
1.0 BTC
1.0 BTC
0.7 BTC
0.6 BTC
0.6 BTC
0.5 BTC
1.2 BTC
1.2 BTC
1.2 BTC
1.0 BTC
1.0 BTC
0.7 BTC
0.7 BTC
0.5 BTC

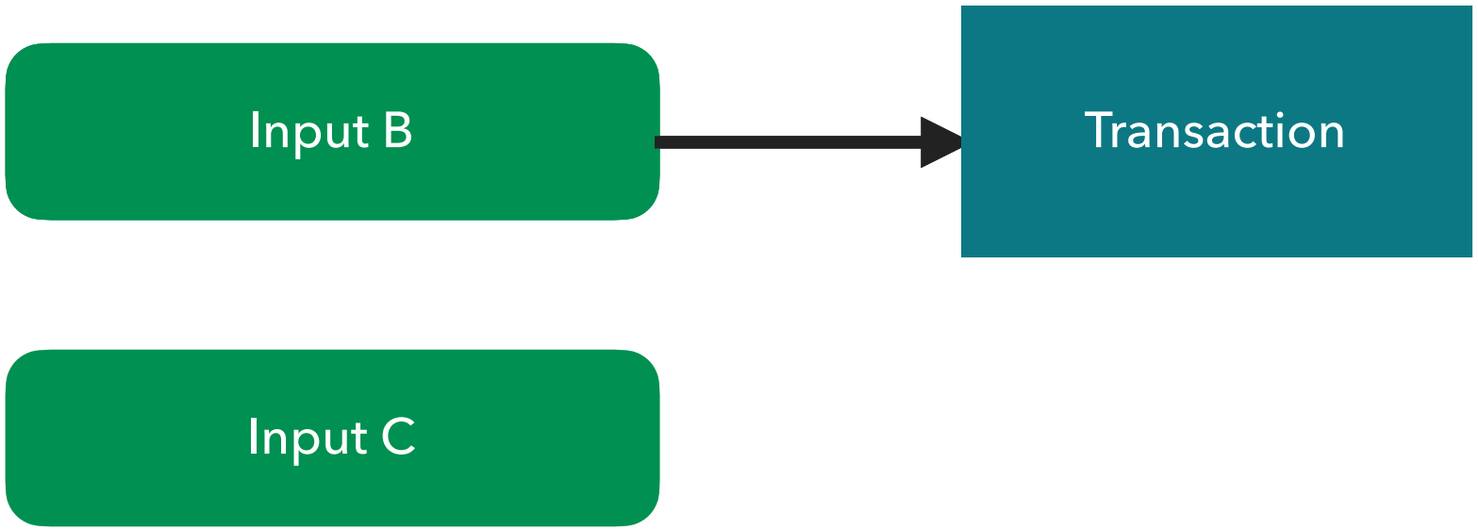
# COINJOIN??

# COINJOIN

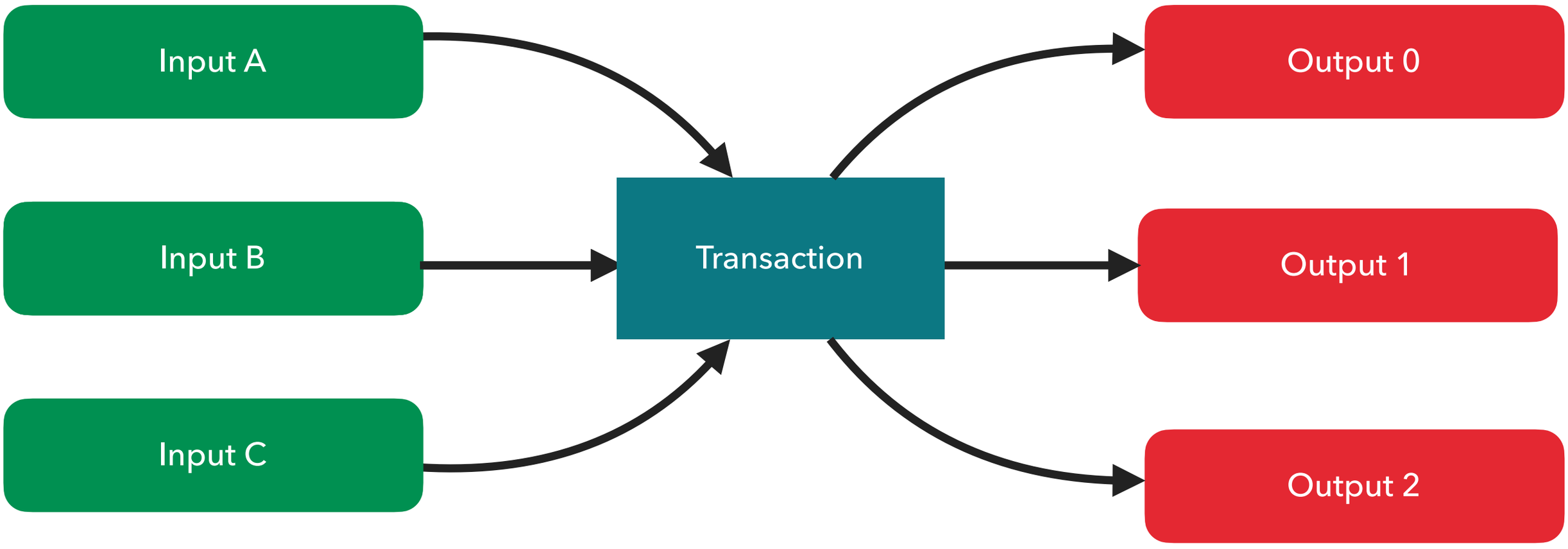
Transaction

# COINJOIN

Input A



# COINJOIN


Input A
Input B
Input C
Transaction
Output 0
Output 1
Output 2

# CONCLUSION AND FUTURE WORK

# CONCLUSION AND FUTURE WORK

- Enforce Lack of evidence

# CONCLUSION AND FUTURE WORK

- Enforce Lack of evidence
- E-voting system using litecoin and conjoin

# CONCLUSION AND FUTURE WORK

- Enforce Lack of evidence
- E-voting system using litecoin and conjoin
- Enforce authentication: SSI or OAuth and OpenID protocols

# CONCLUSION AND FUTURE WORK

- Enforce Lack of evidence
- E-voting system using litecoin and conjoin
- Enforce authentication: SSI or OAuth and OpenID protocols
- Increase privacy: Thor

# Towards a Decentralized and Privacy-Preserving Voting System

**Ivan Mercanti**

## THANKS FOR THE ATTENTION.
## QUESTIONS?


A.D. 1308
unipg
UNIVERSITÀ DEGLI STUDI
DI PERUGIA

**05/02/2026**