# ENFORCING CONFIDENTIALITY IN TORNADO CASH-BASED E-VOTING SYSTEMS

STEFANO BISTARELLI, IVAN MERCANTI AND FRANCESCO SANTINI

A.D. 1308
unipg
UNIVERSITÀ DEGLI STUDI
DI PERUGIA

DLT 2023 25/05/2023

# AGENDA

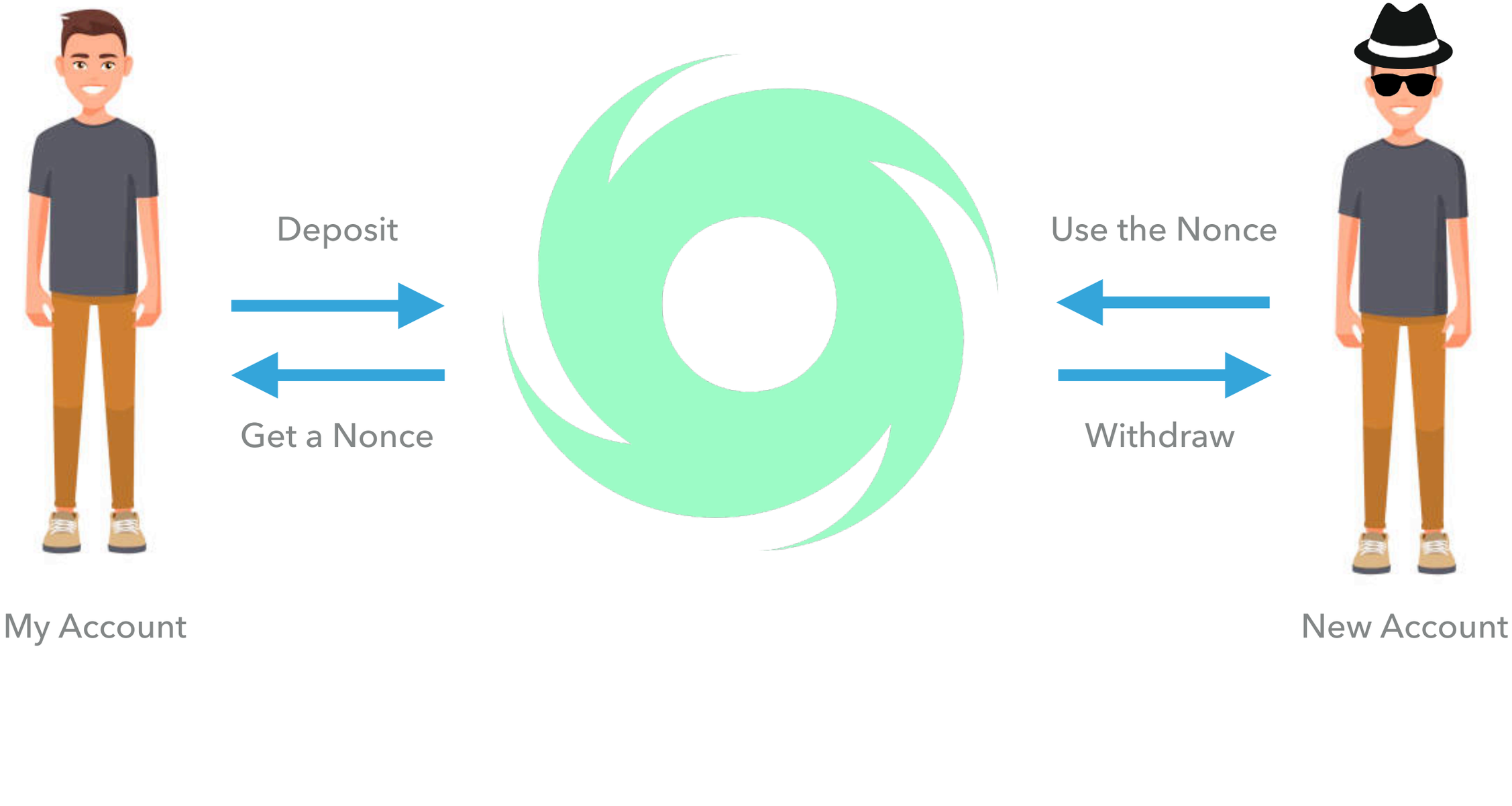
- Background
- Model
- Satisfied Properties
- Conclusion

# THE ERC20 STANDARD

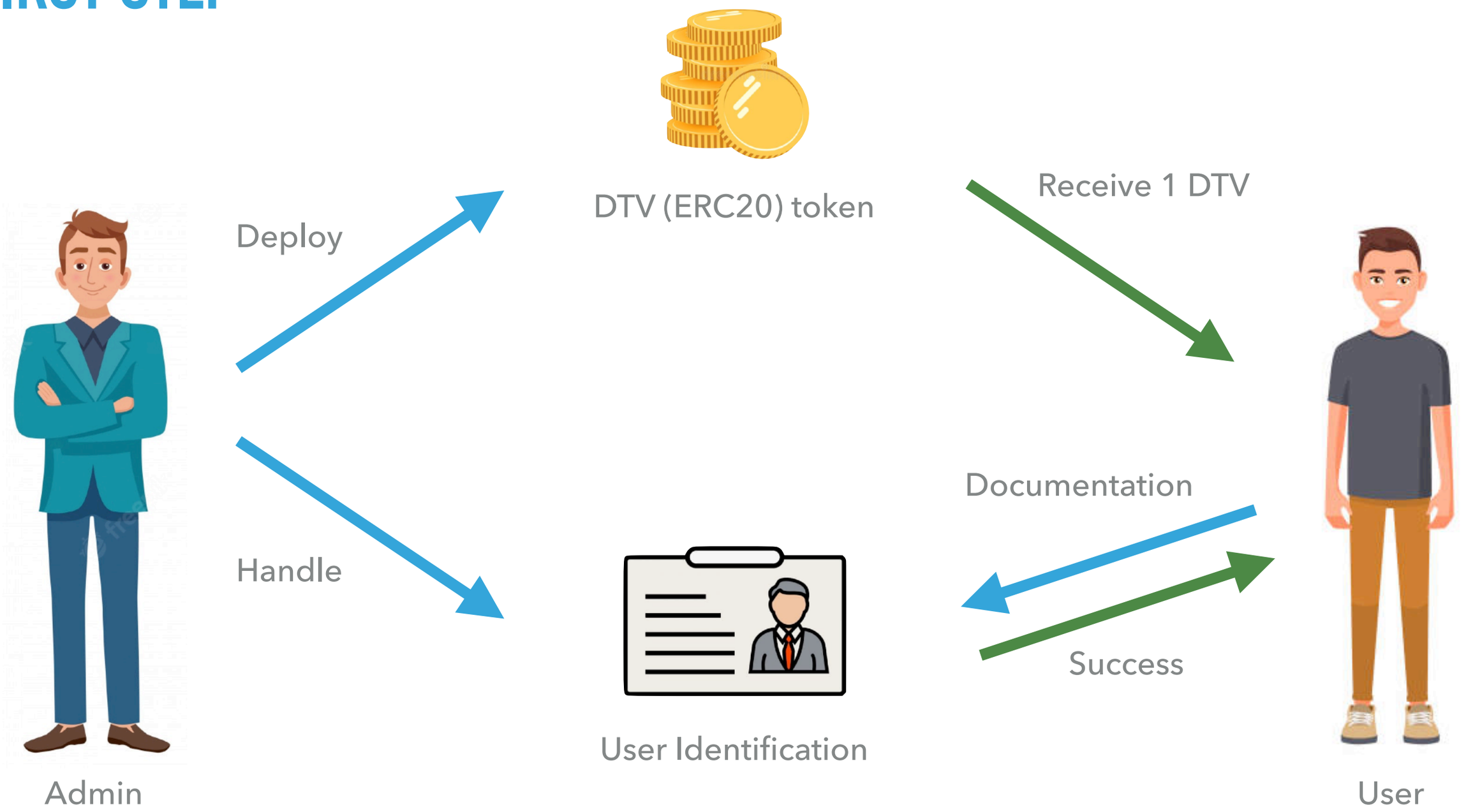
ethereum

**ERC-20**

# TORNADO CASH



# FIRST STEP


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

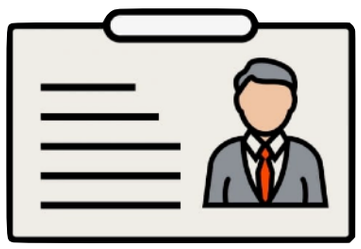
# FIRST STEP

Admin

Deploy

Handle

DTV (ERC20) token



User Identification

Documentation

Fail

User

# PSEUDO-ANONYMIZATION

Admin

Deploy

Set


TornadoCash-Relayer SC

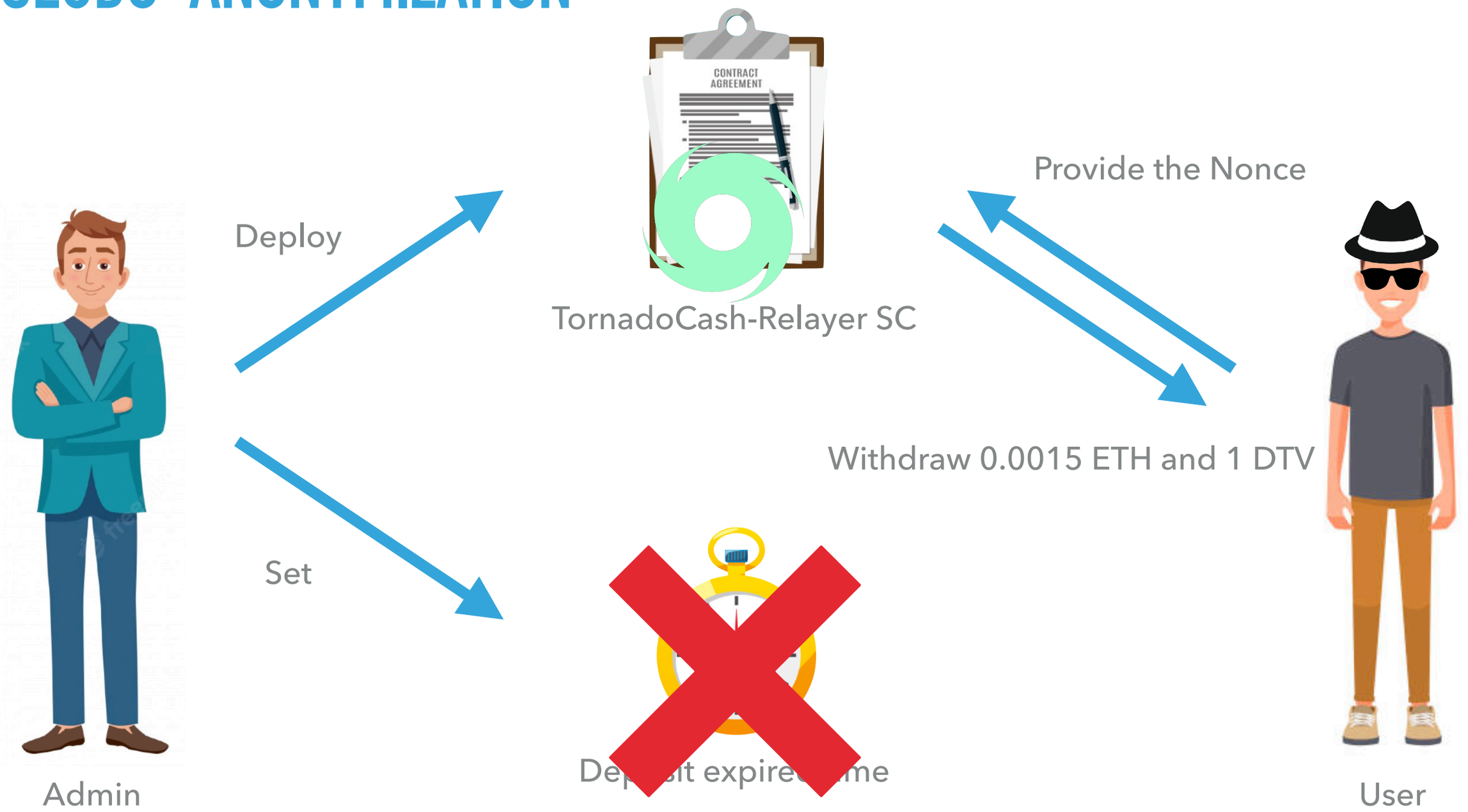
Deposit expired time

Deposit 0.0015 ETH and 1 DTV

Receive a Nonce

User

# PSEUDO-ANONYMIZATION

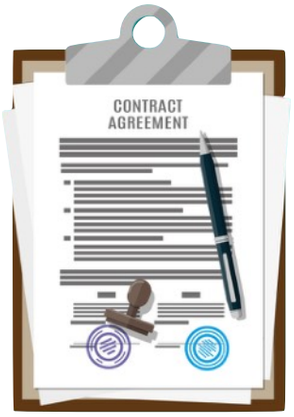


# VOTE

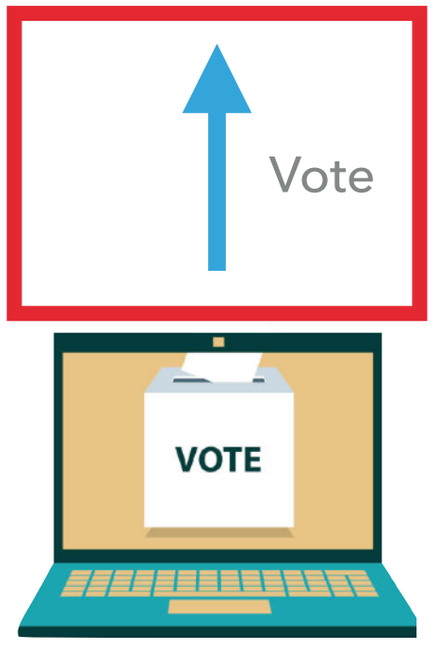
Admin

Deploy

Public




Voting SC




Vote Webpage

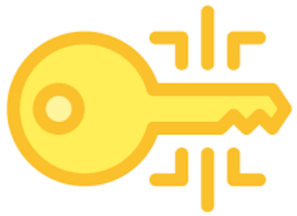
Send 1 DTV to vote

User

# VOTE ENCRYPTION

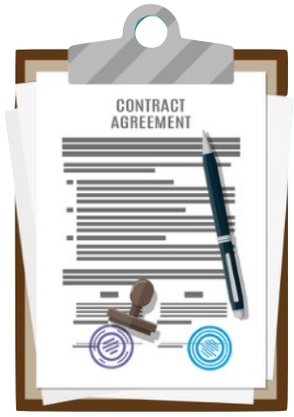
Candidates

Register



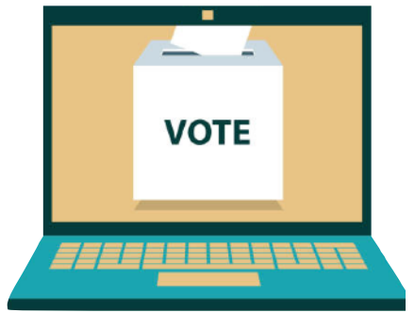
Public keys

Encrypt vote




Voting SC

Encrypt




Vote Webpage

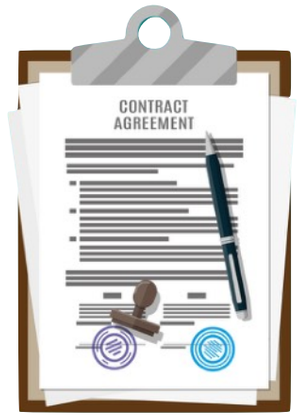
Send 1 DTV to vote

User

# VOTE COUNTING

Private keys

Get votes




Voting SC

Reveal

Candidates

Decryption


Decrypted Votes

Counting

Admin

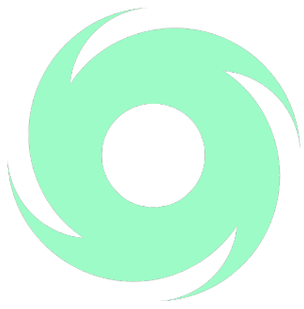
# OUR PROPERTIES

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



# OUR PROPERTIES

- **Privacy**



- **Authentication**

Admin

- **Confidentiality**

Encryption

# OUR PROPERTIES

- **Lack of evidence**

- **Reliability**

# CONCLUSION AND FUTURE WORK

- Enforcing Confidentiality E-voting system
- Use distributed public key
- Implement a Web dApp
- Enforce more properties: Lack of evidence
- Enforce authentication: OAuth and OpenID protocol

# Enforcing Confidentiality in Tornado Cash-based E-voting Systems

Stefano Bistarelli, **Ivan Mercanti** and Francesco Santini

## THANKS FOR THE ATTENTION. QUESTIONS?

**Email: ivan.mercanti@unipg.it**


A.D. 1308
unipg
UNIVERSITÀ DEGLI STUDI
DI PERUGIA

**DLT 2023 25/05/2023**