AN E-VOTING SYSTEM BASED ON TORNADO CASH*

STEFANO BISTARELLI, BRUNO LAZO LA TORRE MONTALVO

IVAN MERCANTI AND FRANCESCO SANTINI

* PRESENTATO A ETAA22 @ESORICS 2022

A.D. 1308

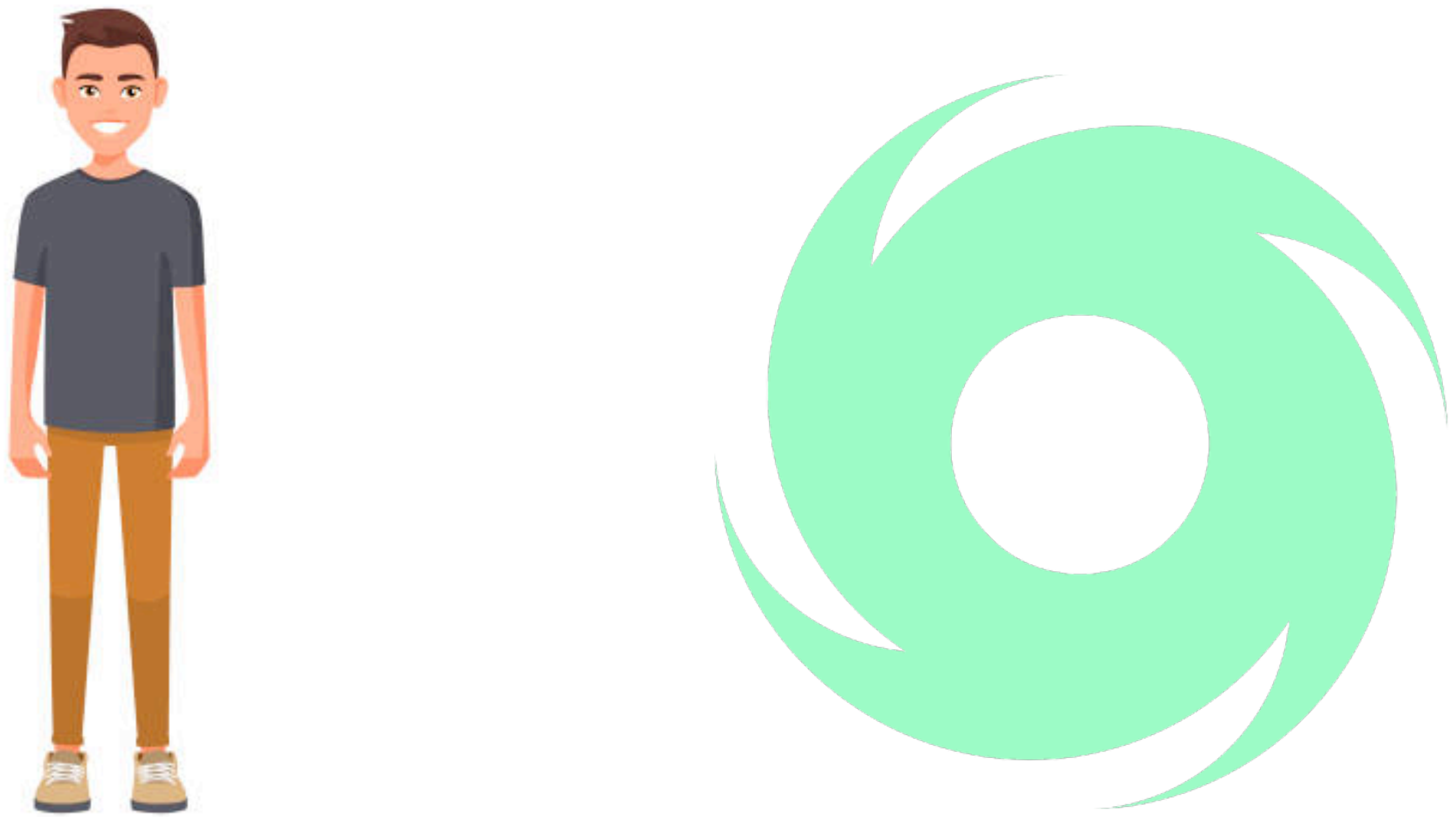
unipg

UNIVERSITÀ DEGLI STUDI
DI PERUGIA

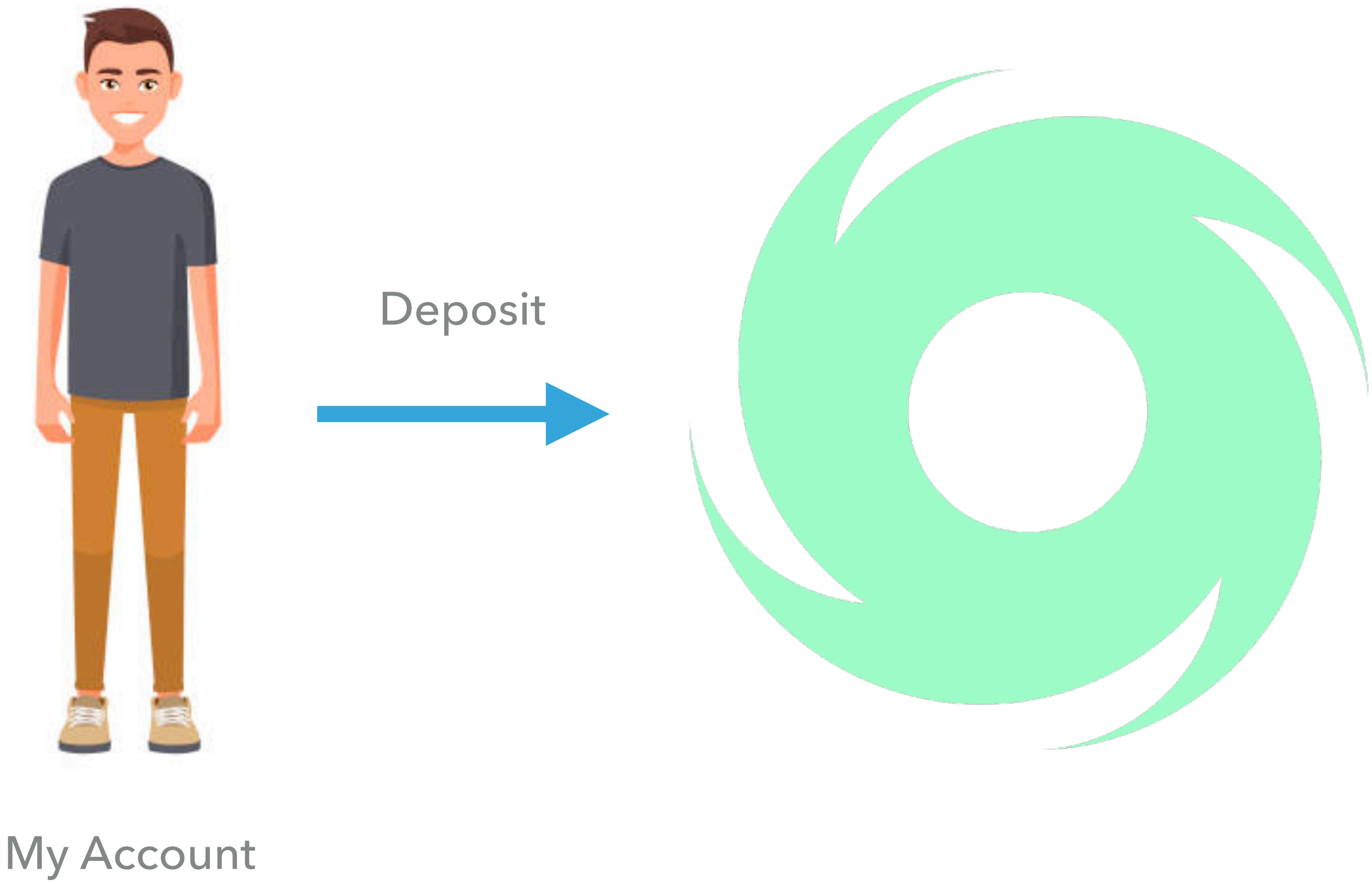
DLT FIRENZE 2022 08/11/2022

THE ERC20 STANDARD

TORNADO CASH



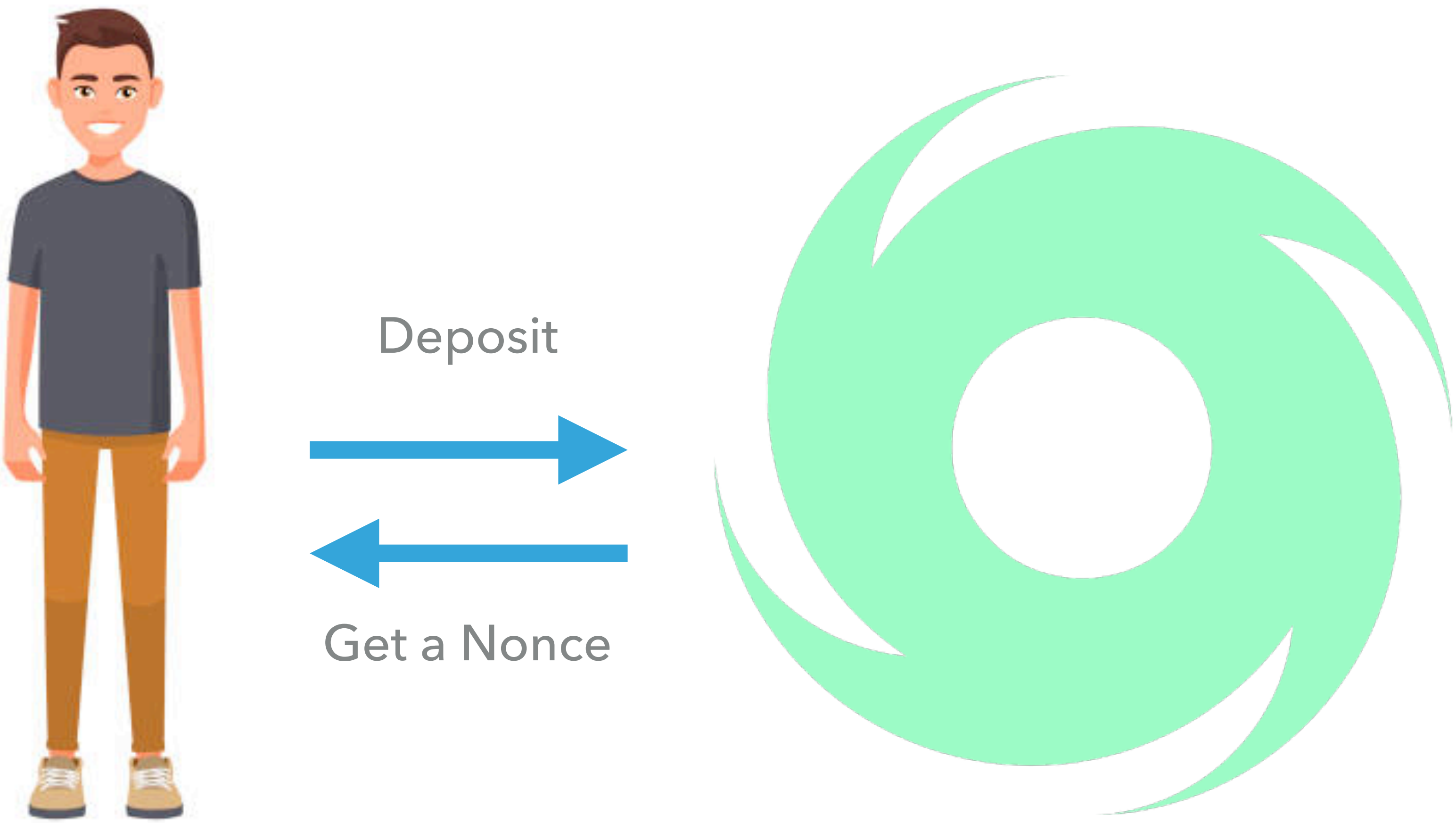
TORNADO CASH



Deposit

My Account

TORNADO CASH

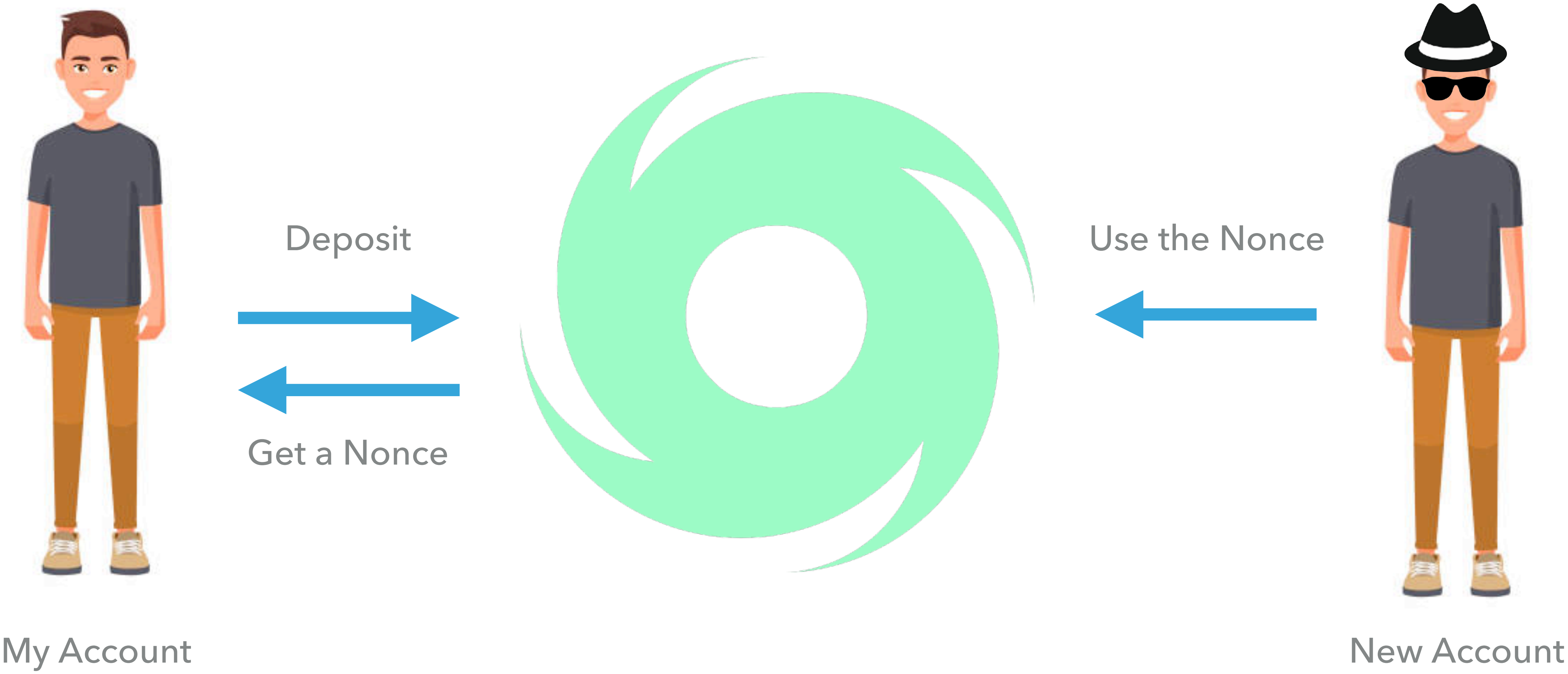


Deposit

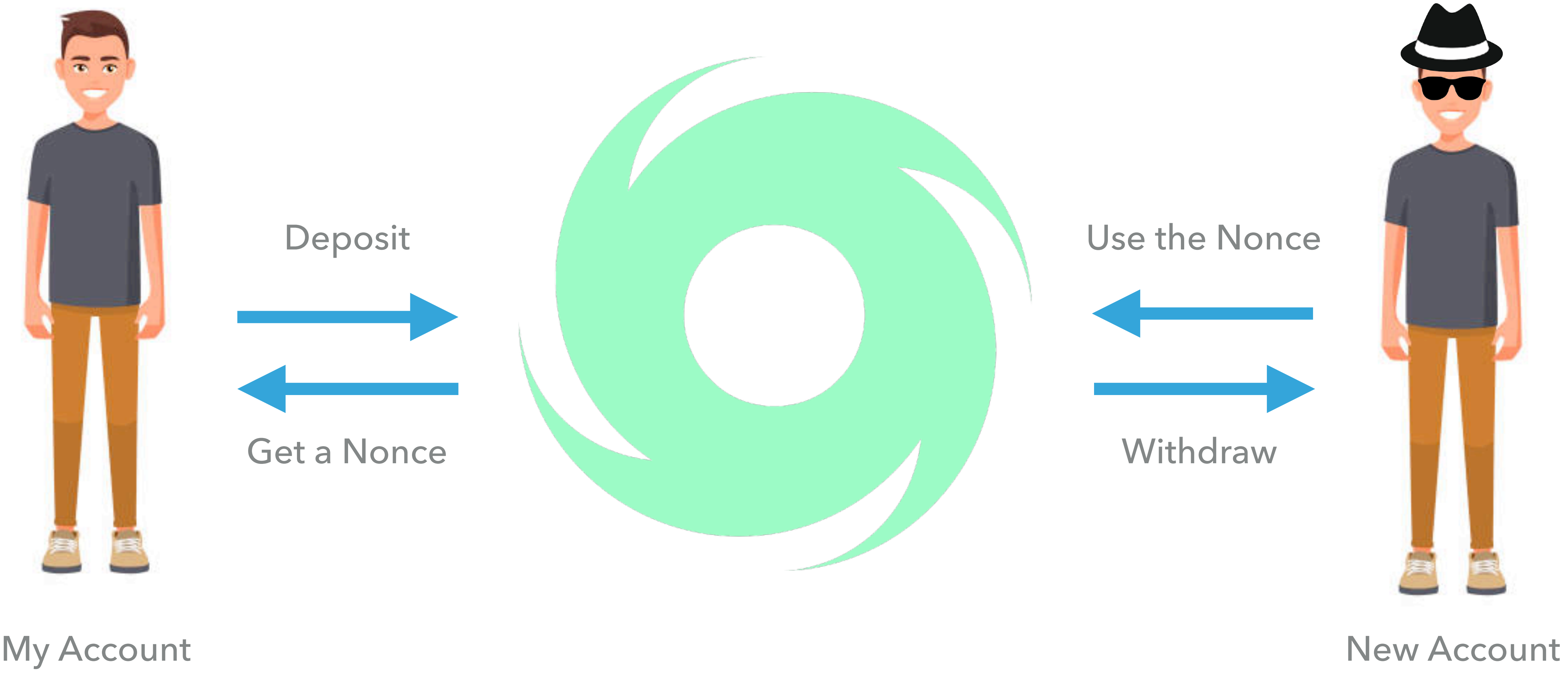
Get a Nonce

My Account

TORNADO CASH



TORNADO CASH



Deposit

Get a Nonce

Use the Nonce

Withdraw

My Account

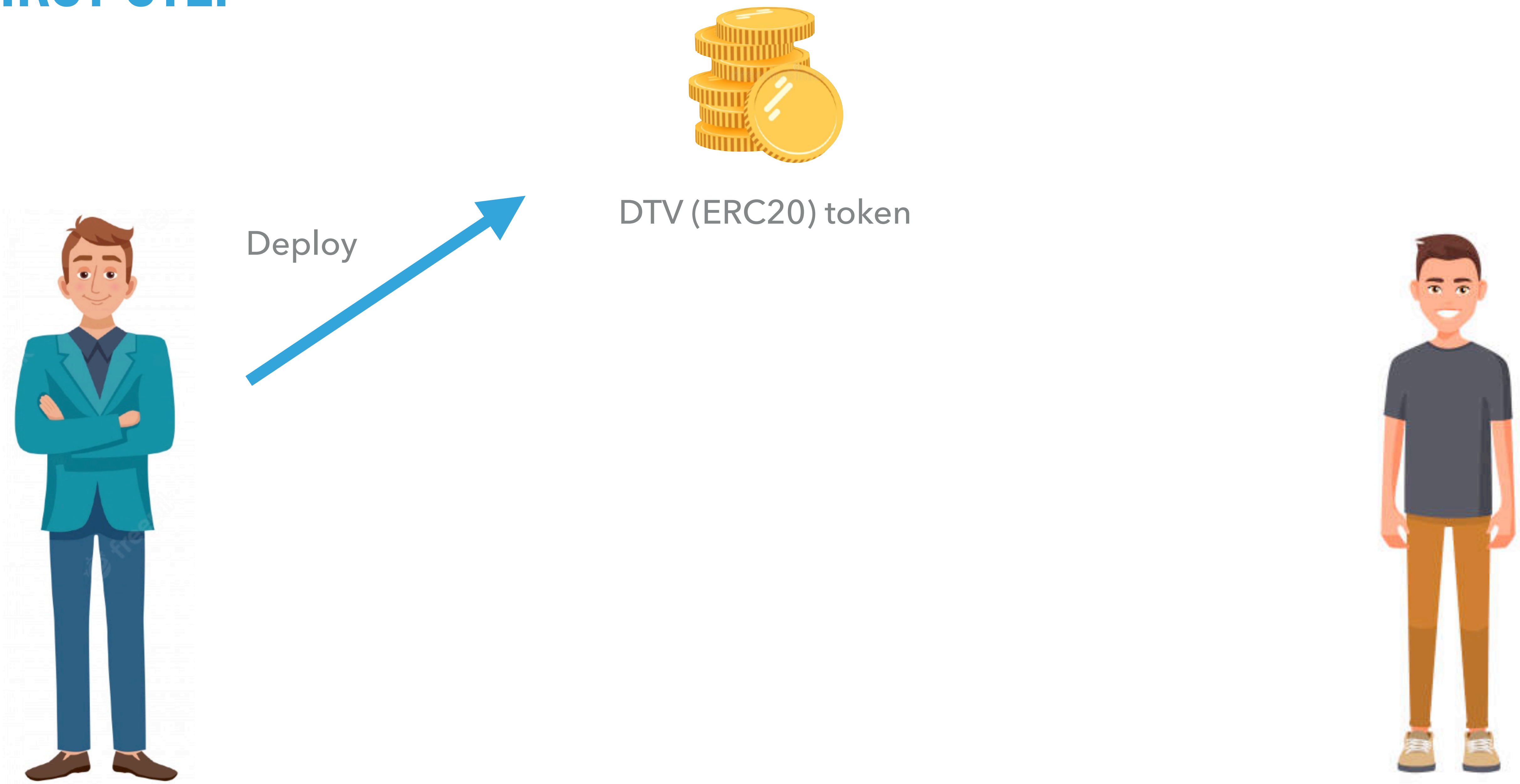
New Account

FIRST STEP

Admin

User

FIRST STEP



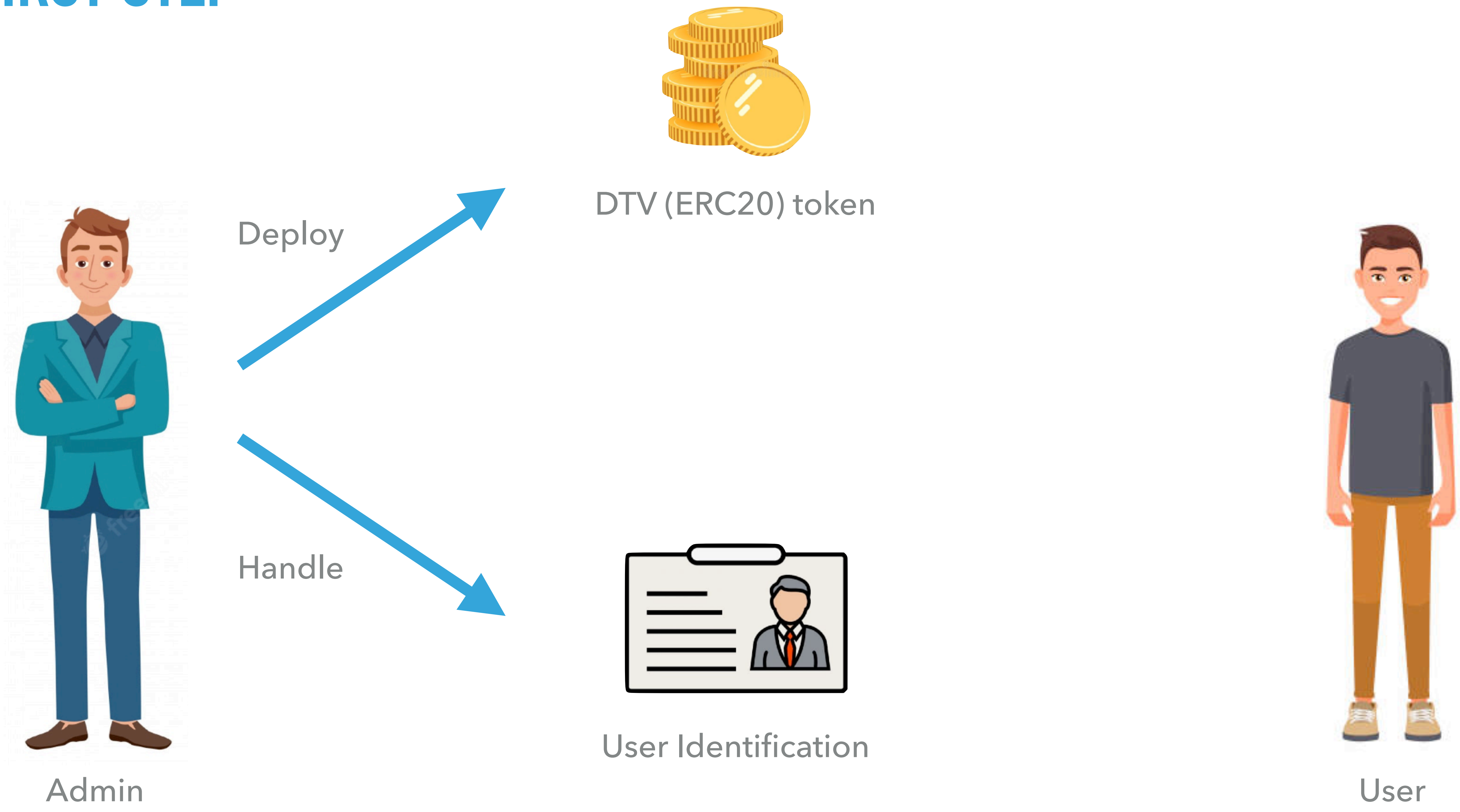
Deploy

DTV (ERC20) token

Admin

User

FIRST STEP



Deploy

DTV (ERC20) token

Handle

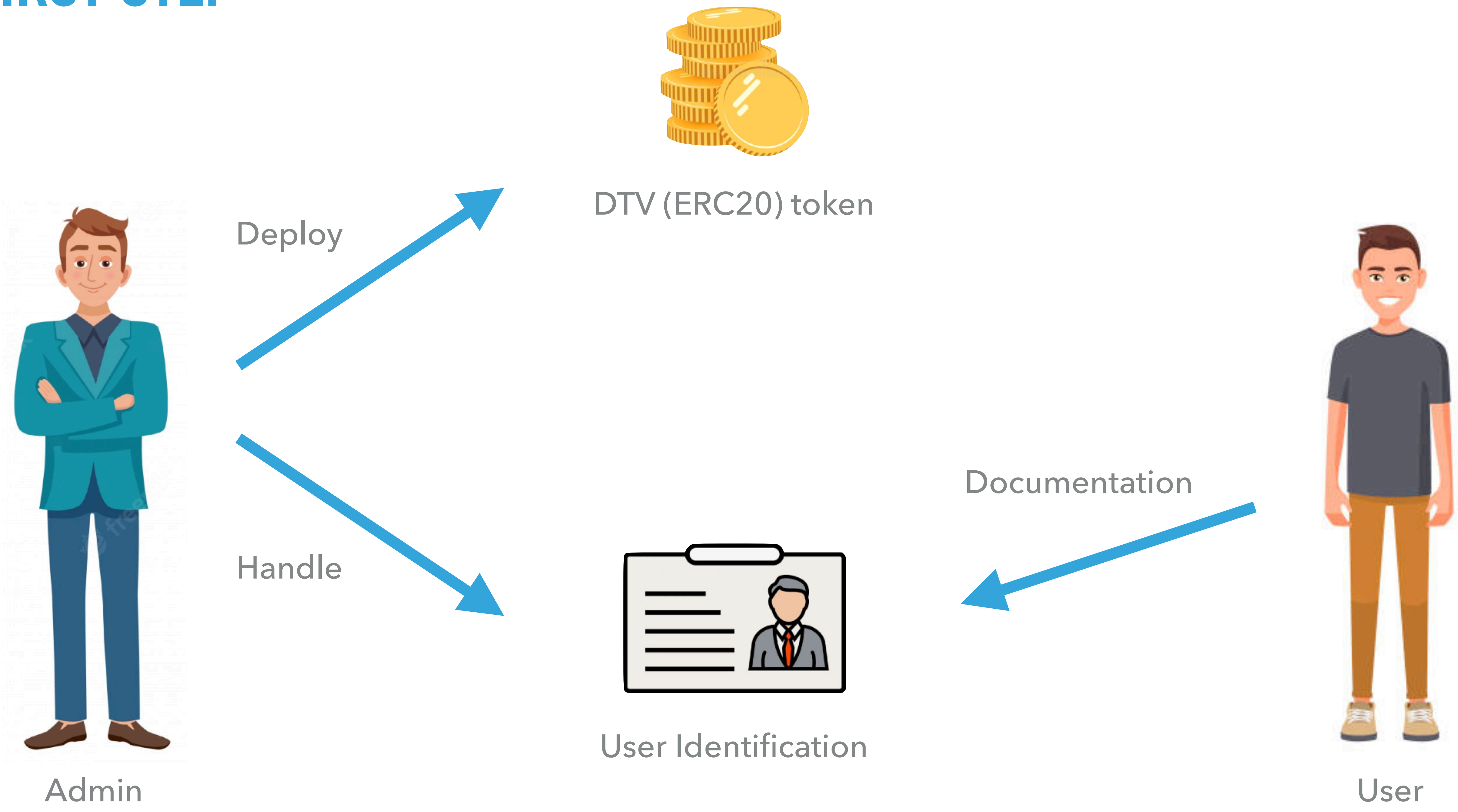
User Identification

Admin

User

OUR MODEL

FIRST STEP



DTV (ERC20) token

Deploy

Handle

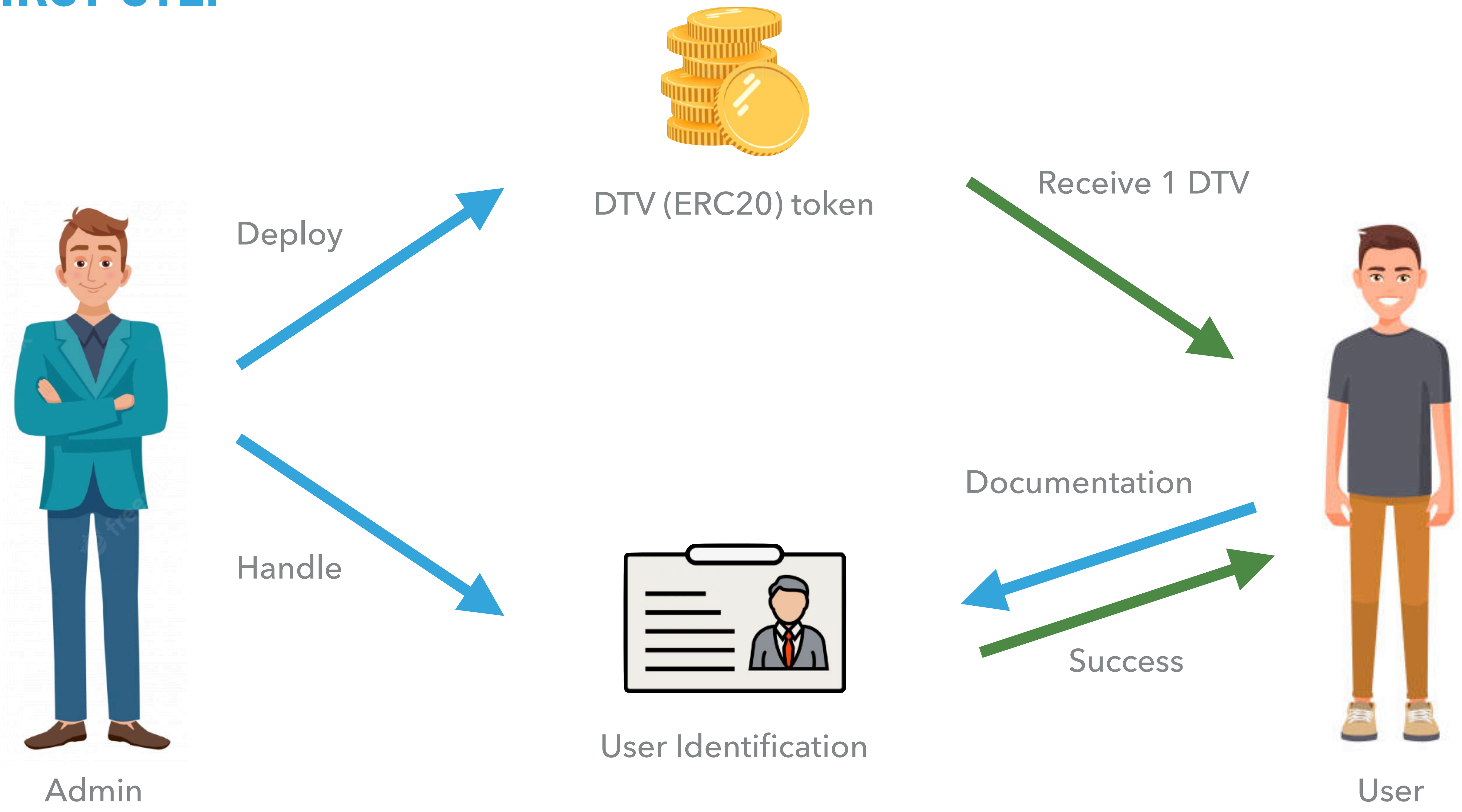
Documentation

User Identification

Admin

User

FIRST STEP



DTV (ERC20) token

Deploy

Receive 1 DTV

Handle

Documentation

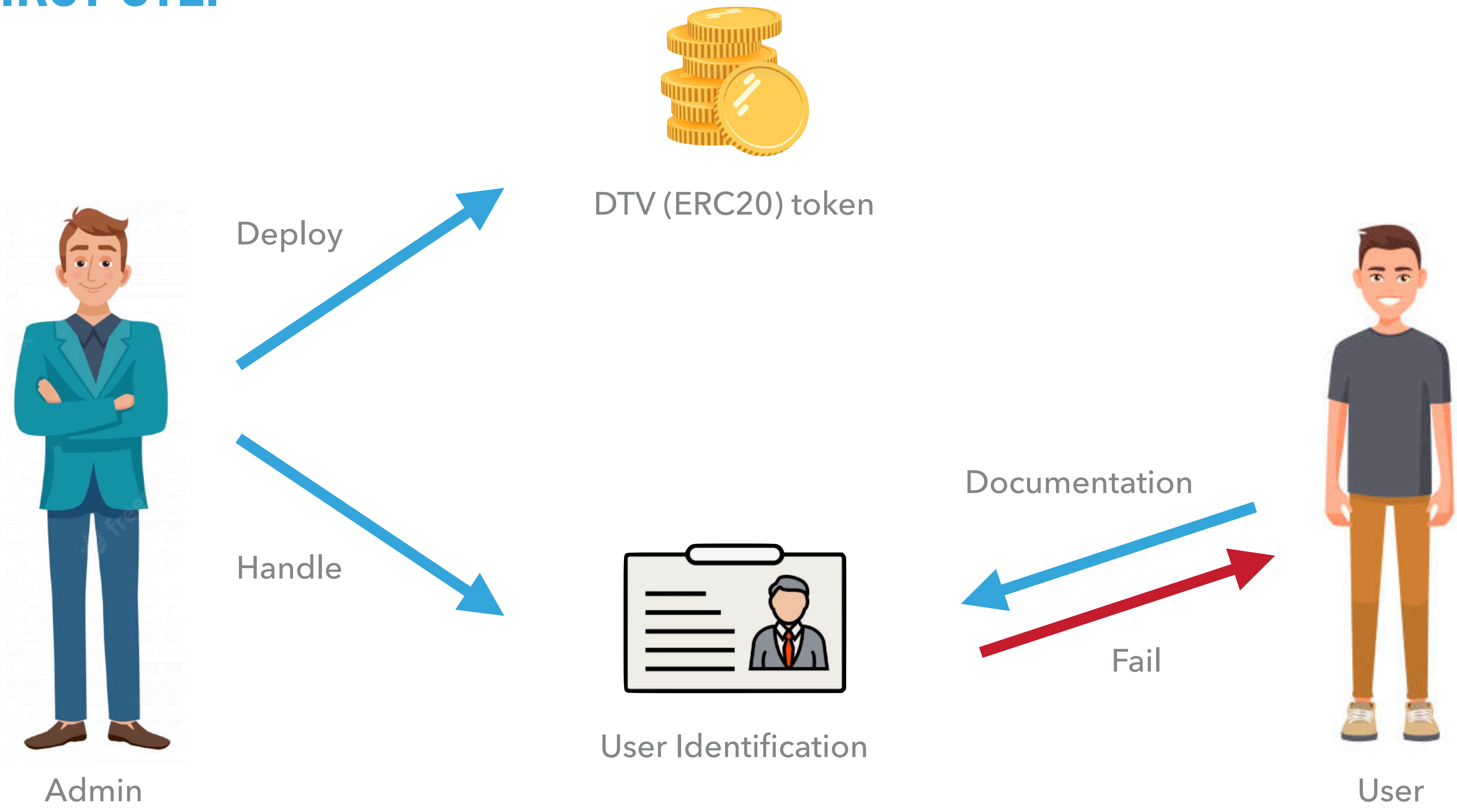
Success

User Identification

Admin

User

FIRST STEP



DTV (ERC20) token

Deploy

Handle

Documentation

Fail

User Identification

Admin

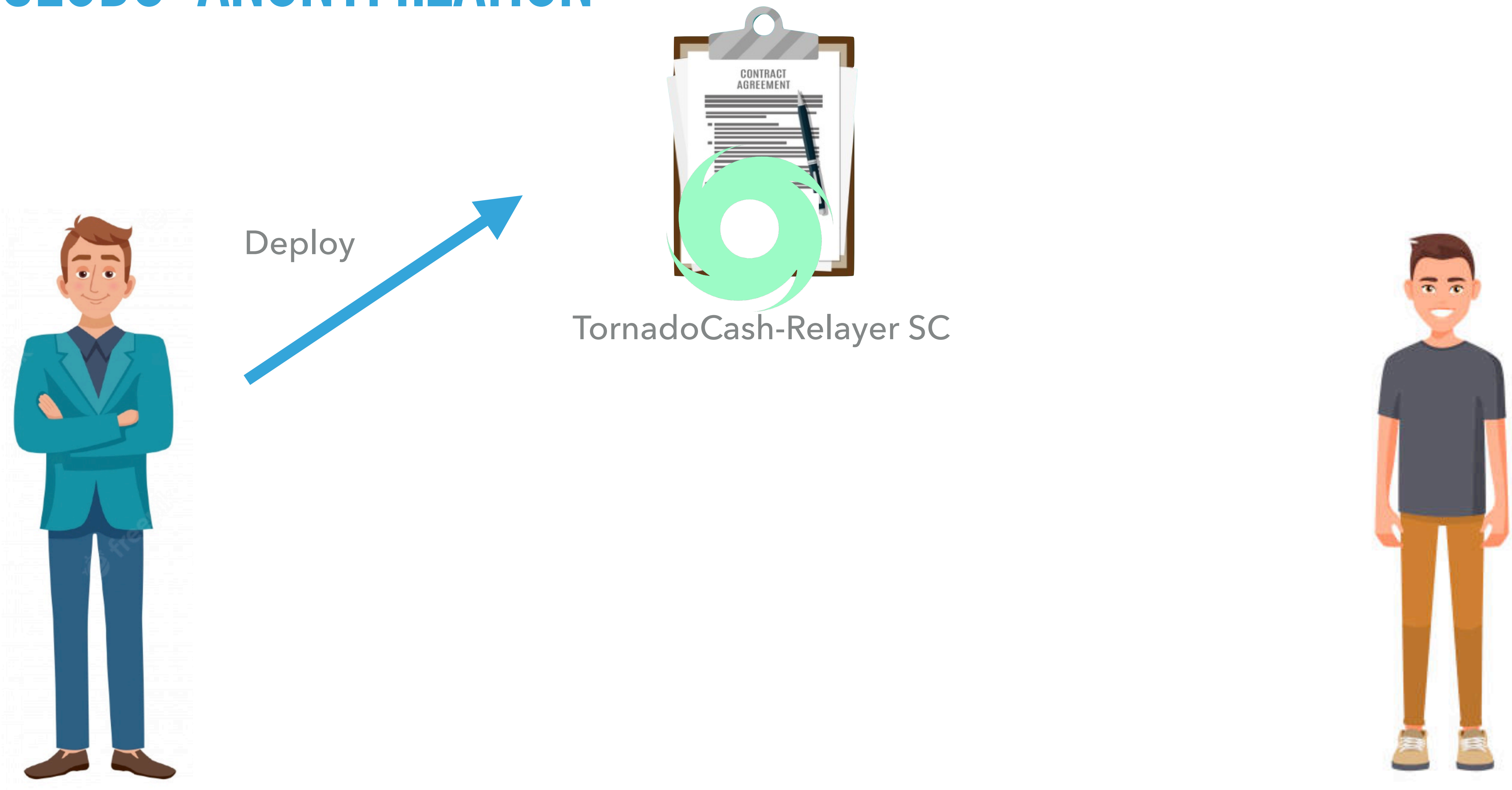
User

PSEUDO-ANONYMIZATION

Admin

User

PSEUDO-ANONYMIZATION



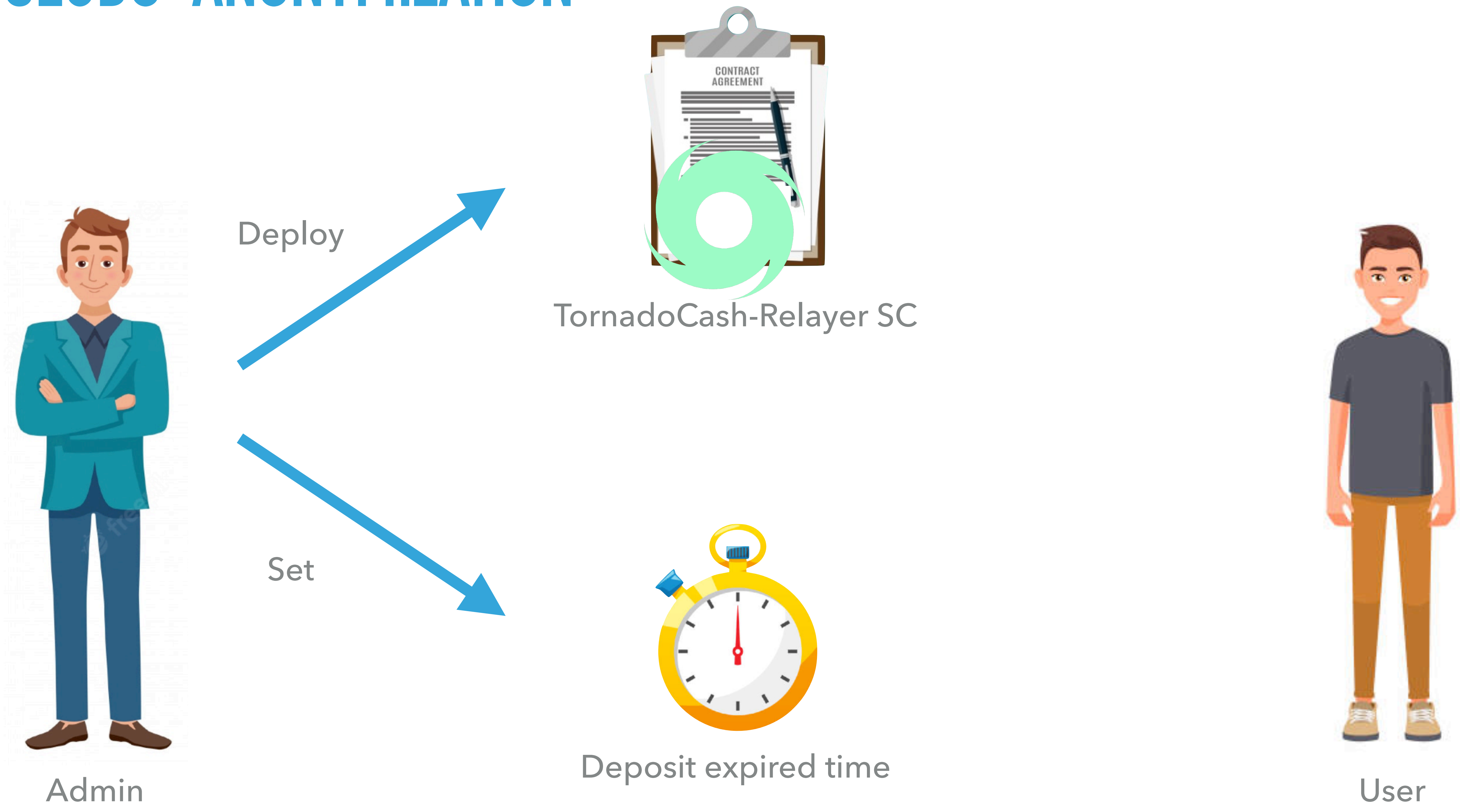
Deploy

TornadoCash-Relayer SC

Admin

User

PSEUDO-ANONYMIZATION



Deploy

TornadoCash-Relayer SC

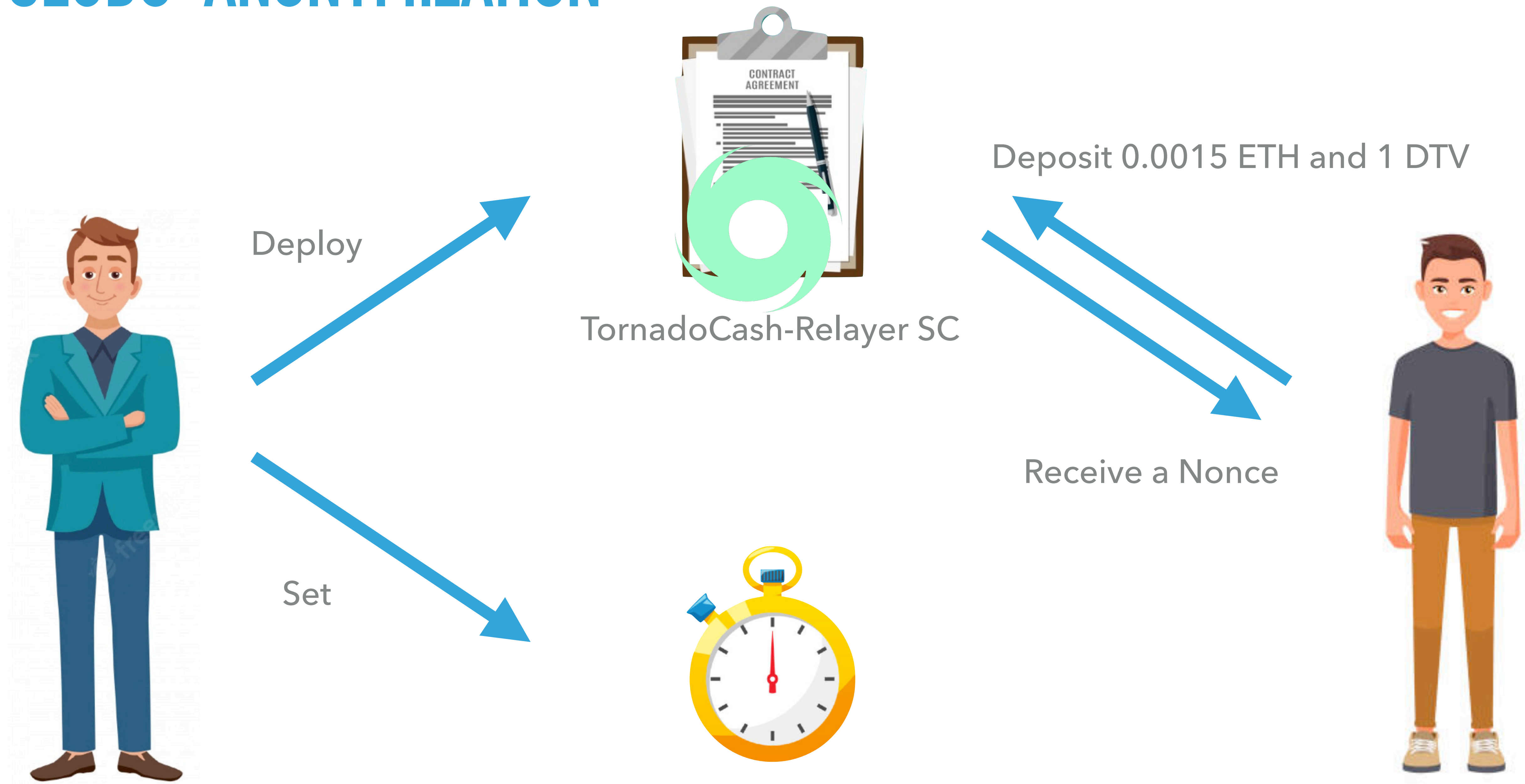
Set

Deposit expired time

Admin

User

PSEUDO-ANONYMIZATION



Deploy

TornadoCash-Relayer SC

Deposit 0.0015 ETH and 1 DTV

Receive a Nonce

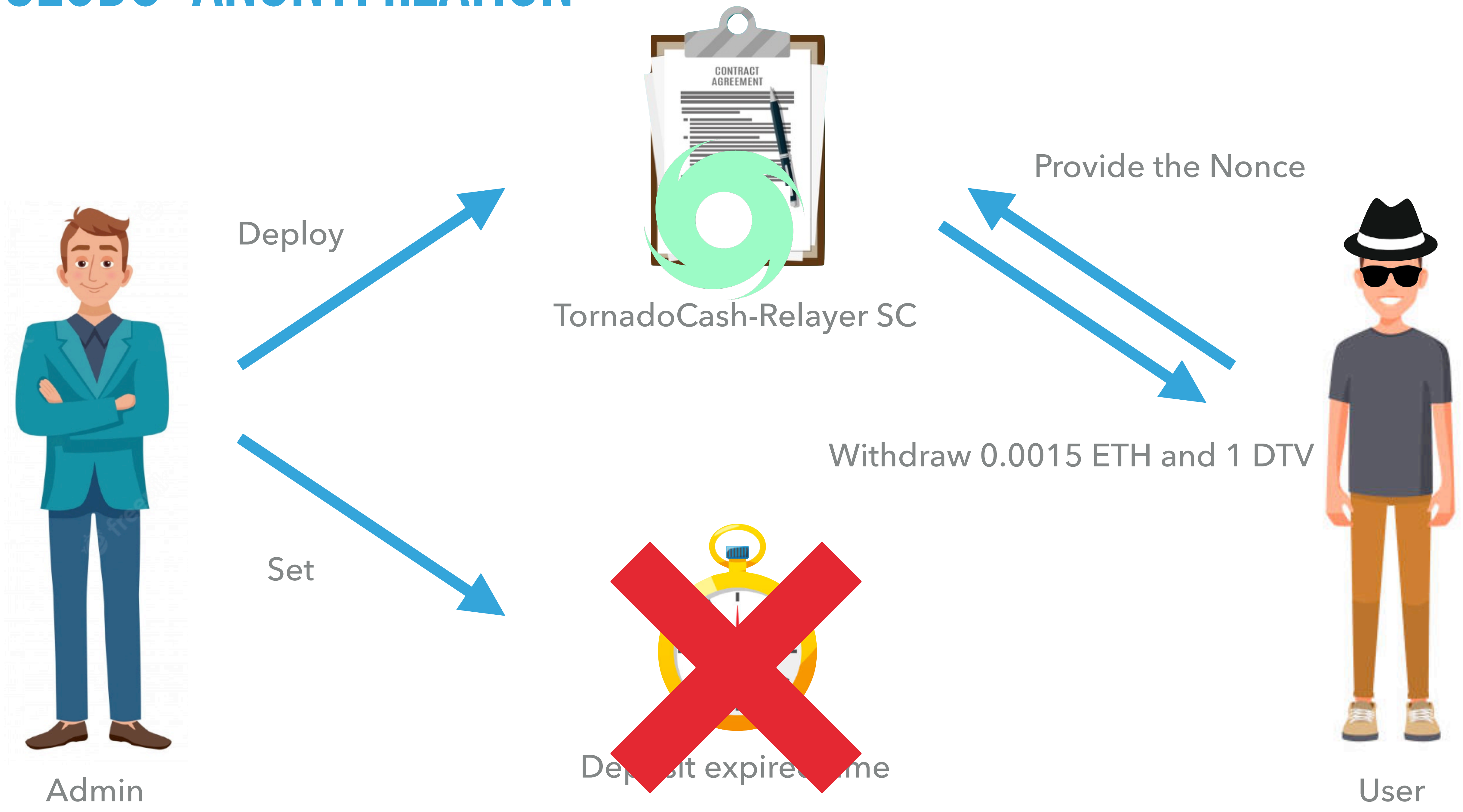
Set

Deposit expired time

Admin

User

PSEUDO-ANONYMIZATION



Deploy

TornadoCash-Relayer SC

Provide the Nonce

Withdraw 0.0015 ETH and 1 DTV

Set

Deposit expire time

Admin

User

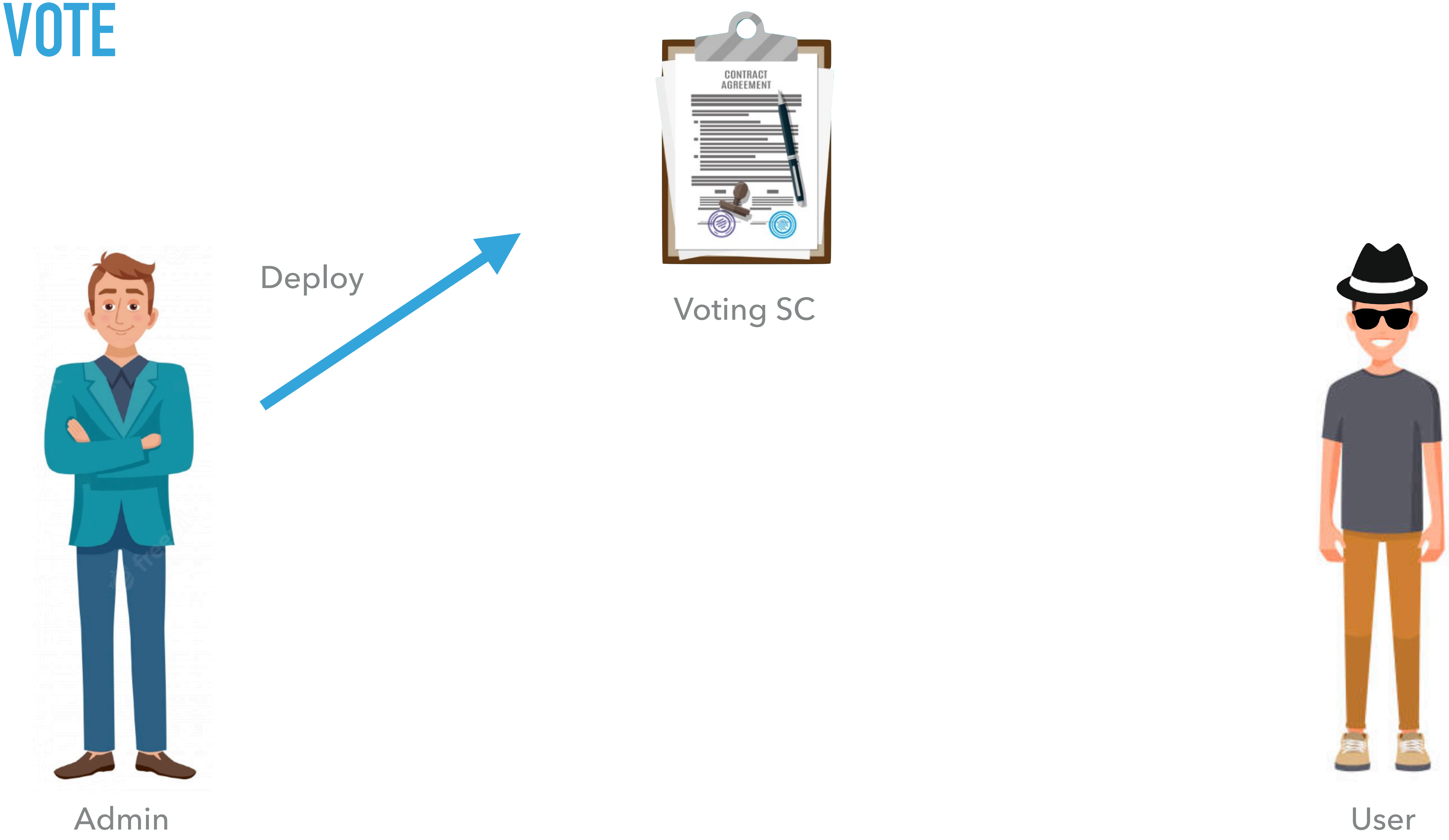
VOTE

Admin

User

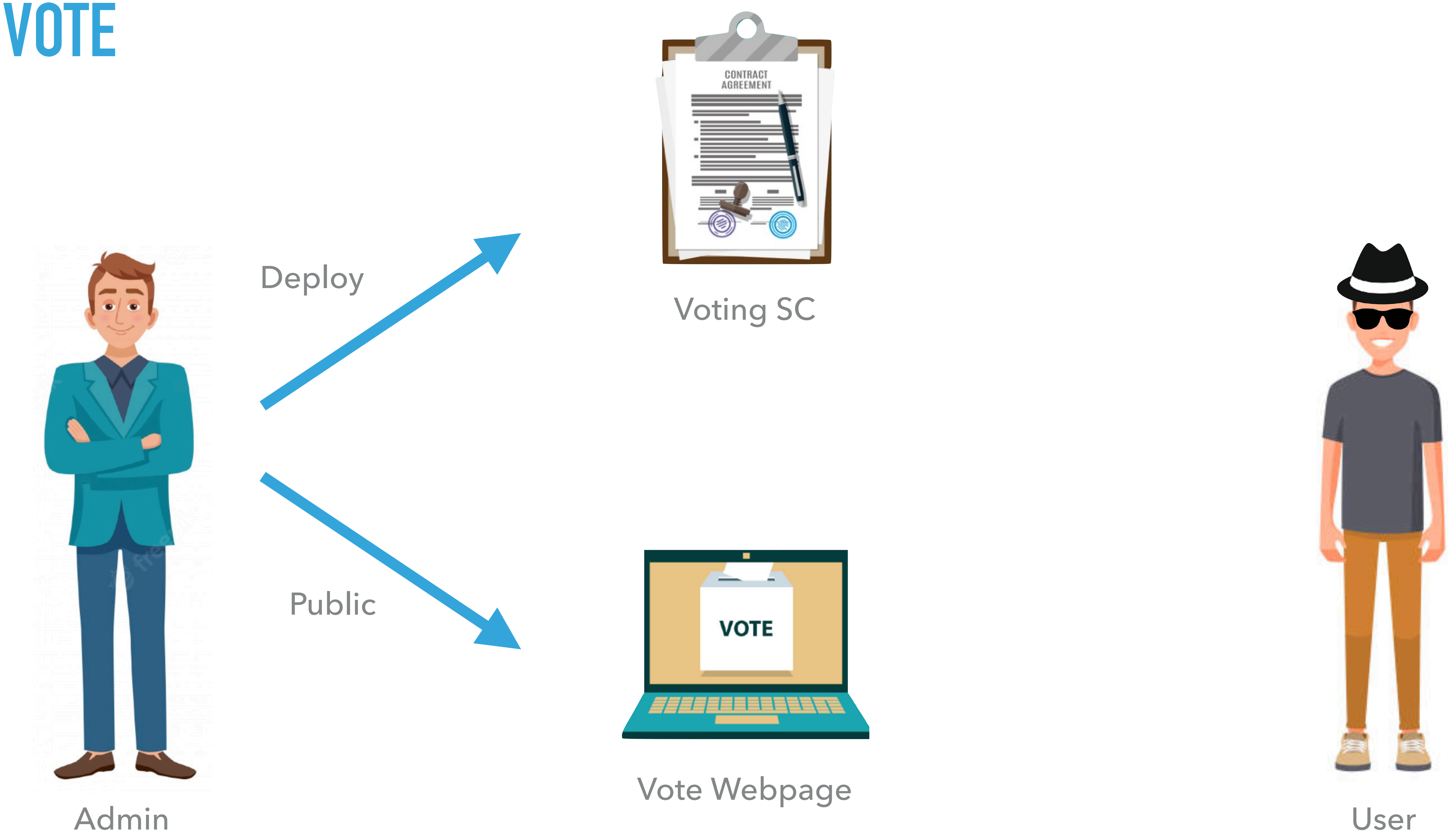
OUR MODEL

VOTE



OUR MODEL

VOTE



Deploy

Voting SC

Public

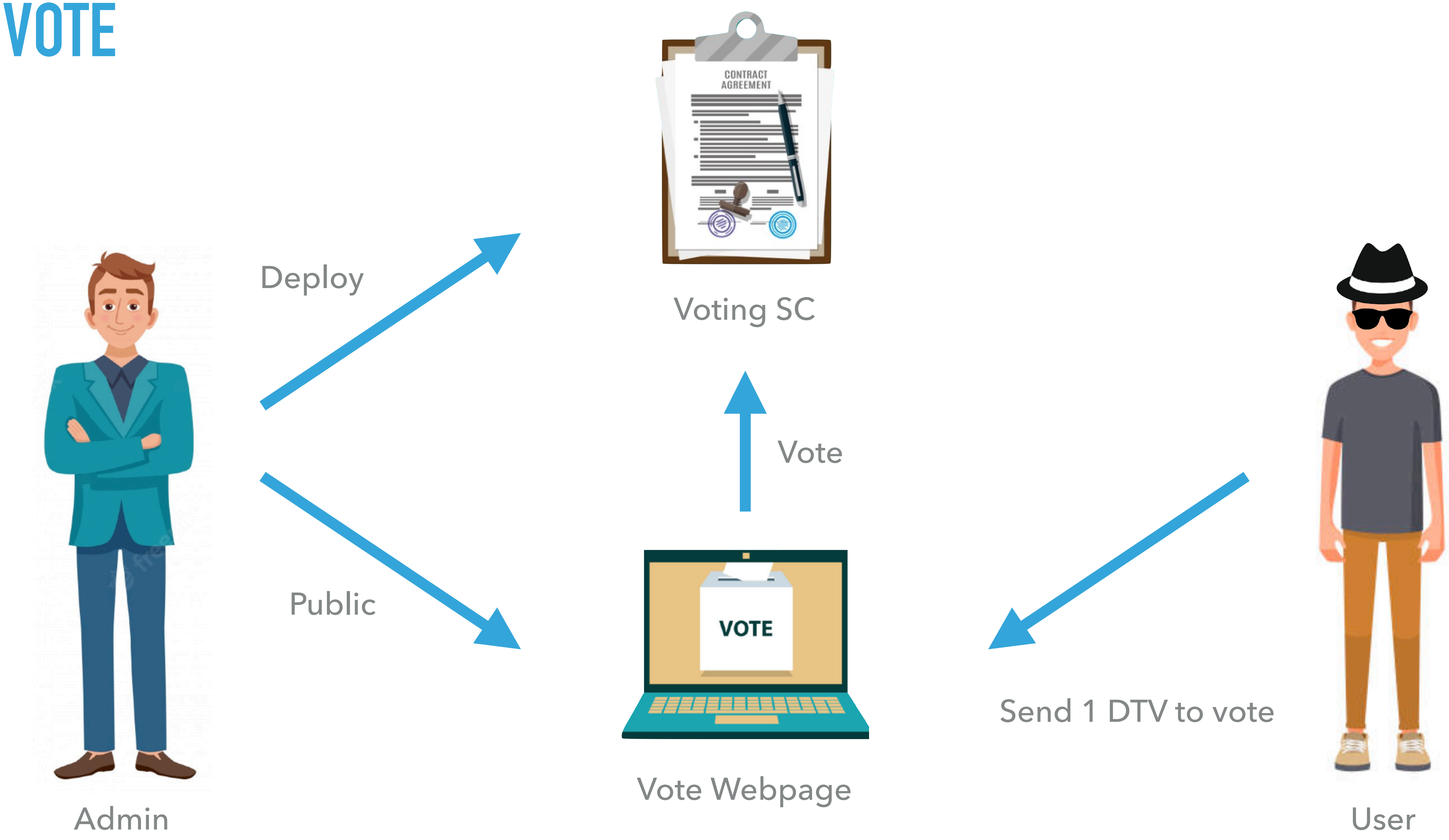
Vote Webpage

Admin

User

OUR MODEL

VOTE



Deploy

Voting SC

Vote

Public

Vote Webpage

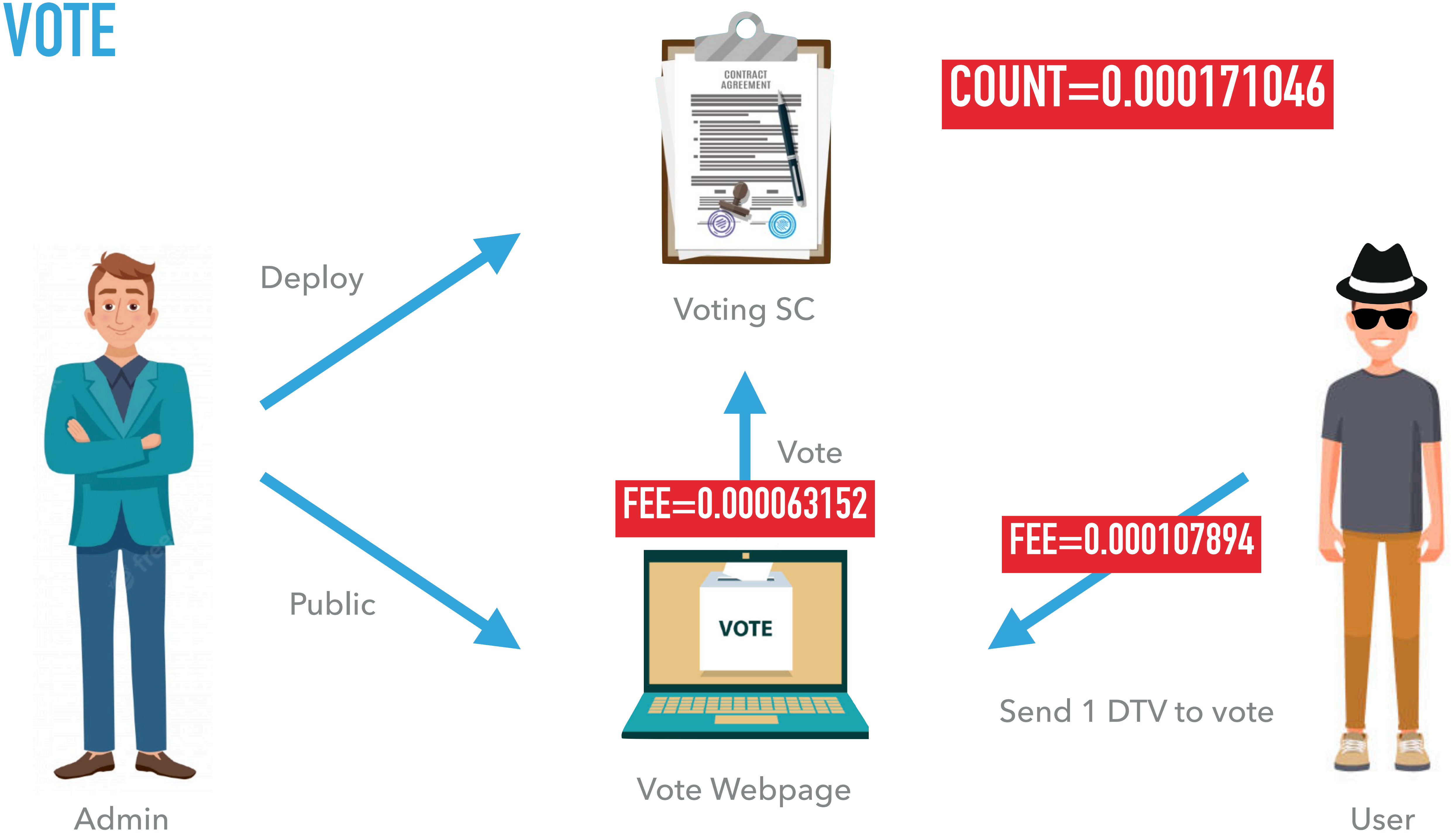
Send 1 DTV to vote

Admin

User

COST ESTIMATION

VOTE



COUNT=0.000171046

Deploy

Voting SC

Vote

FEE=0.000063152

Public

FEE=0.000107894

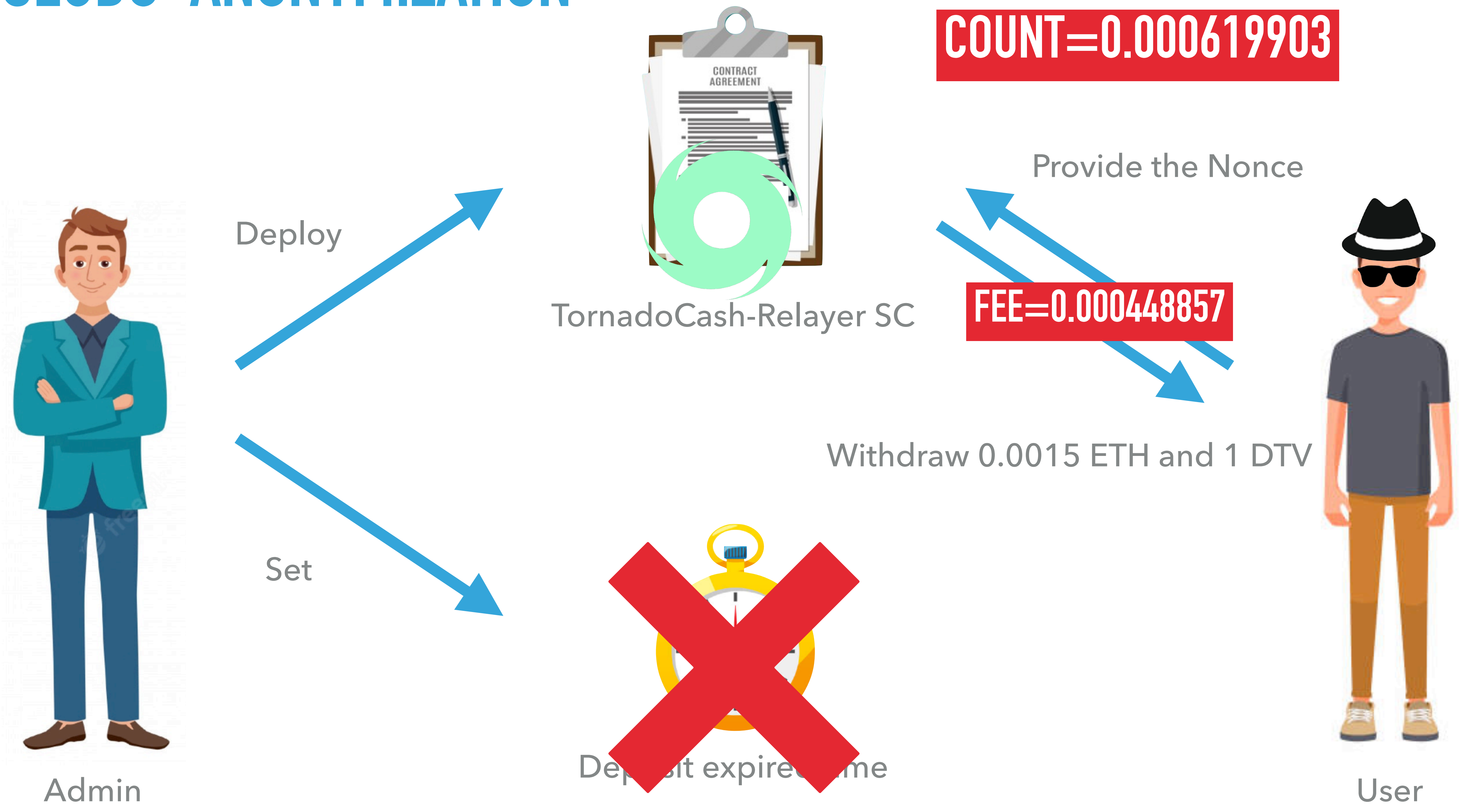
Send 1 DTV to vote

Vote Webpage

Admin

User

PSEUDO-ANONYMIZATION



COUNT=0.000619903

Deploy

TornadoCash-Relayer SC

Provide the Nonce

FEE=0.000448857

Withdraw 0.0015 ETH and 1 DTV

Set

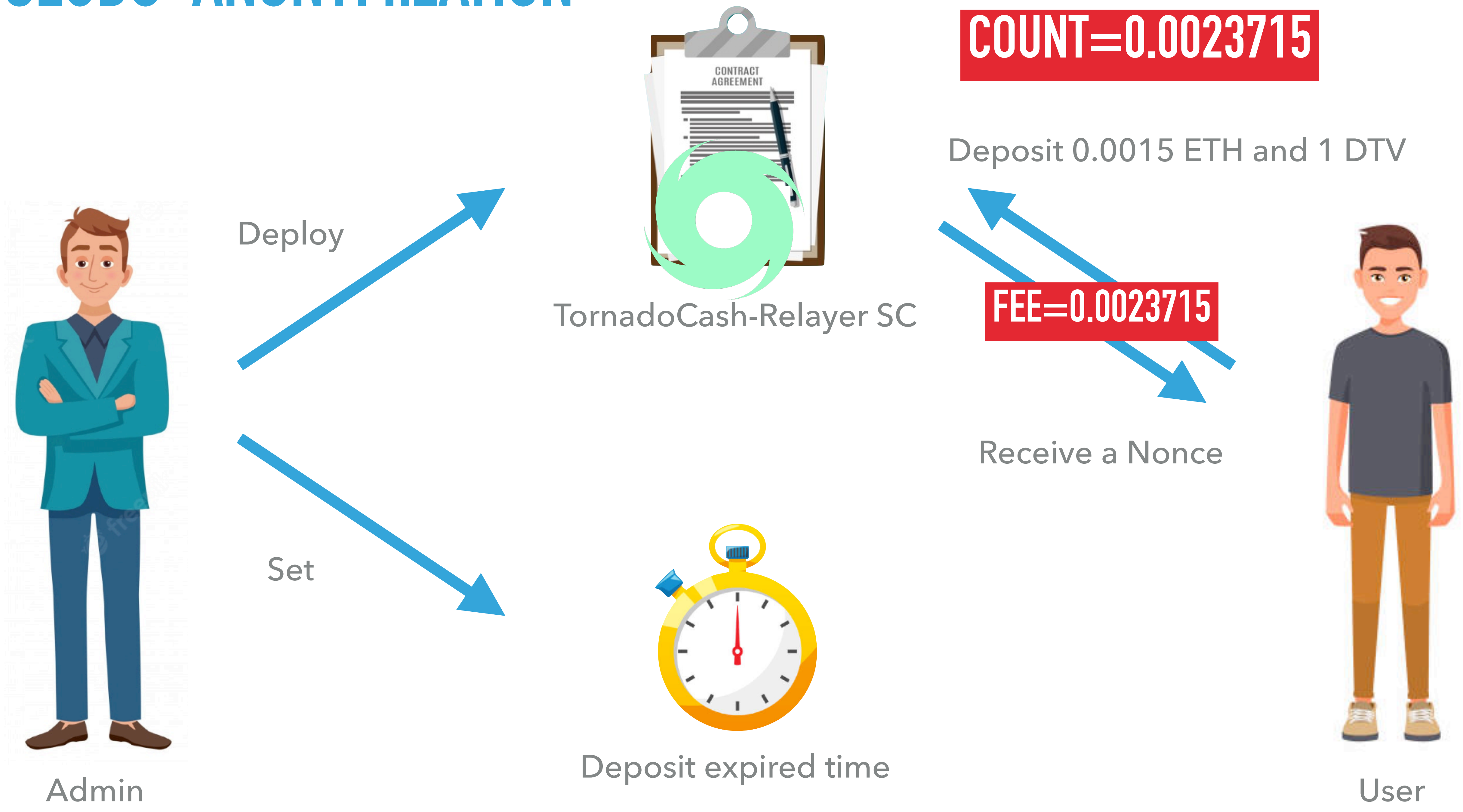
Deposit expire time

Admin

User

COST ESTIMATION

PSEUDO-ANONYMIZATION



COUNT=0.0023715

Deploy

TornadoCash-Relayer SC

Deposit 0.0015 ETH and 1 DTV

FEE=0.0023715

Receive a Nonce

Set

Deposit expired time

Admin

User

OUR COST

0.0023715 ETH ≈ 4.20€

Italian election

Year	Cost (€)	Voters	Cost p.v. (€)
2013	389 million	50,449,979	7.71
2018	400 million	50,161,844	7.97
2022	> 400 million	50,869,304	> 7.89

OUR PROPERTIES

- Verifiability
- Uniqueness
- Integrity
- Counting

✓

OUR PROPERTIES

Privacy	✓
Authentication	✓
Confidentiality	✗

Admin

OUR PROPERTIES

- Lack of evidence ✗
- Reliability ✓

CONCLUSION AND FUTURE WORK

CONCLUSION AND FUTURE WORK

- E-voting system Ethereum based, using Tornado Cash

CONCLUSION AND FUTURE WORK

- E-voting system Ethereum based, using Tornado Cash
- Implement a Web dApp

CONCLUSION AND FUTURE WORK

- E-voting system Ethereum based, using Tornado Cash
- Implement a Web dApp
- Enforce more properties: Confidentiality and Lack of evidence

CONCLUSION AND FUTURE WORK

- E-voting system Ethereum based, using Tornado Cash
- Implement a Web dApp
- Enforce more properties: Confidentiality and Lack of evidence
- Enforce authentication: OAuth and OpenID protocols

CONCLUSION AND FUTURE WORK

- E-voting system Ethereum based, using Tornado Cash
- Implement a Web dApp
- Enforce more properties: Confidentiality and Lack of evidence
- Enforce authentication: OAuth and OpenID protocols
- Increase privacy: Thor

An E-voting System Based on Tornado Cash

Stefano Bistarelli, Bruno Lazo La Torre Montalvo,
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 Firenze 2022 08/11/2022