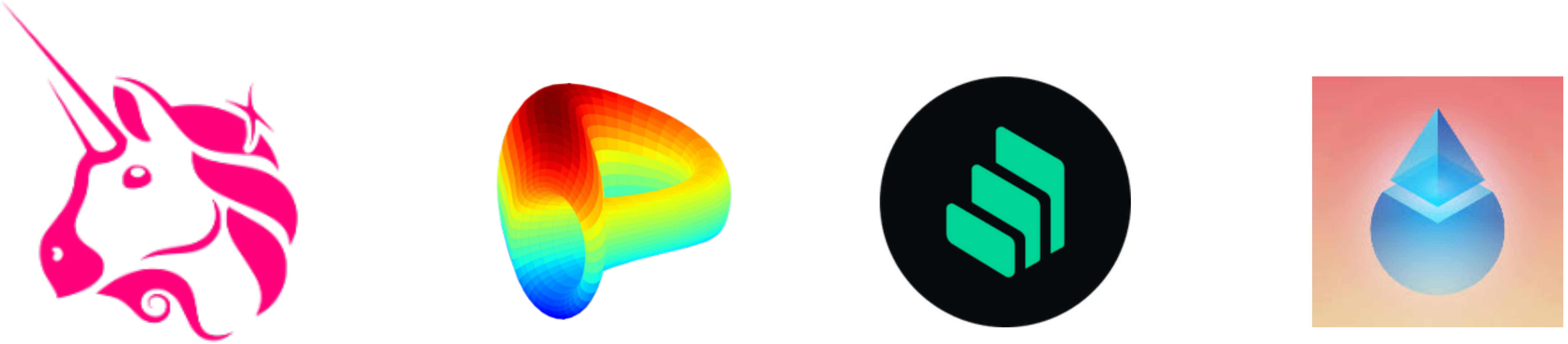
On the Governance of DAOs

The Centrality of Trustworthy and Transparent Governance

Vabuk Pahari, Bala Chandrasekaran, Abhisekh Dash, Krishna Gummadi, Johnnatan Messias

12 May 2025, TLDR, New York

DeFi Protocols and Governance Contracts



DeFi Protocols and Governance Contracts

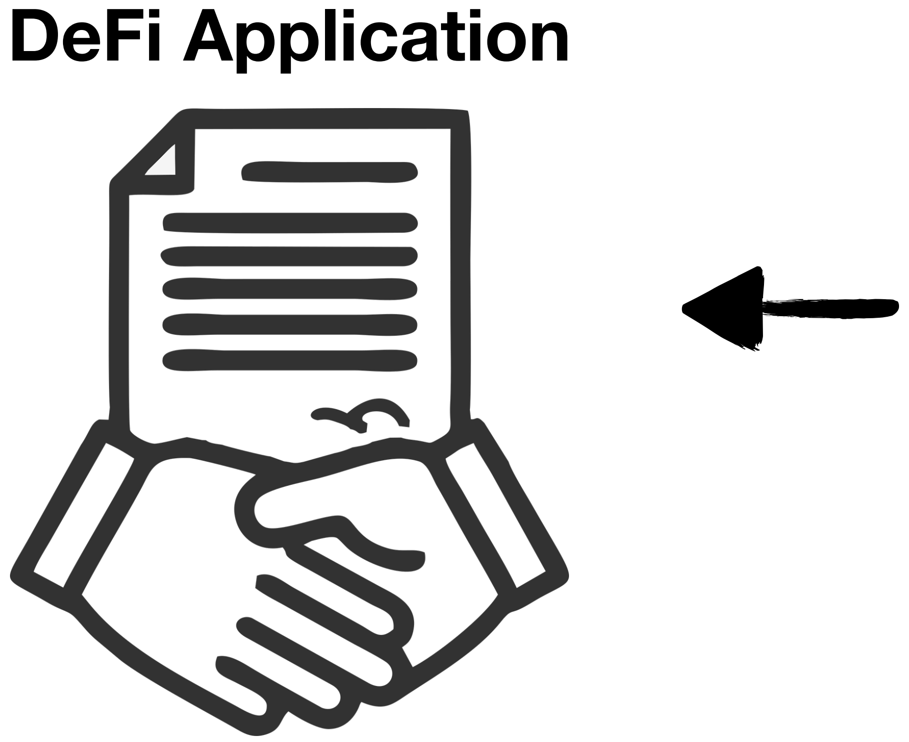
- **Decentralized Autonomous Organisations (DAOs)** own and govern DeFi Protocols

Governance Contracts and DAOs

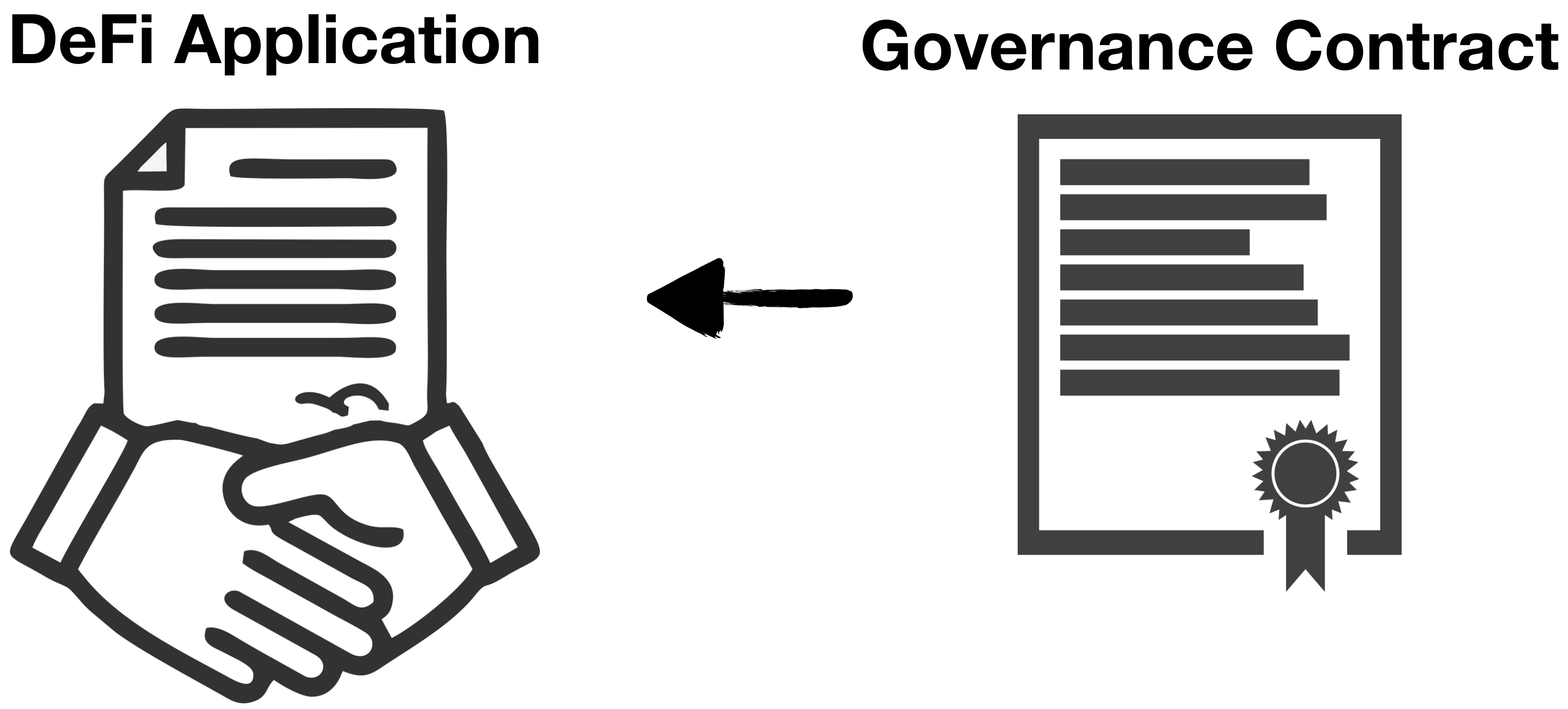
Governance Contracts and DAOs

DeFi Application

Governance Contracts and DAOs



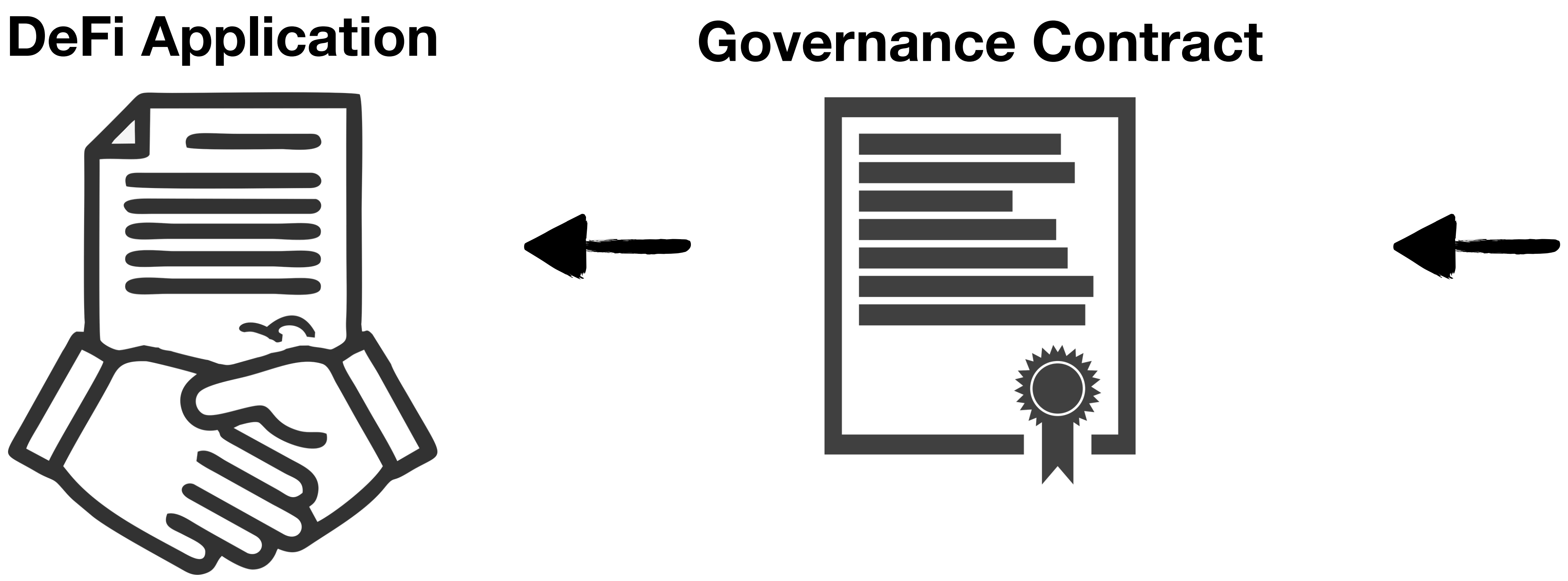
Governance Contracts and DAOs



DeFi Application

Governance Contract

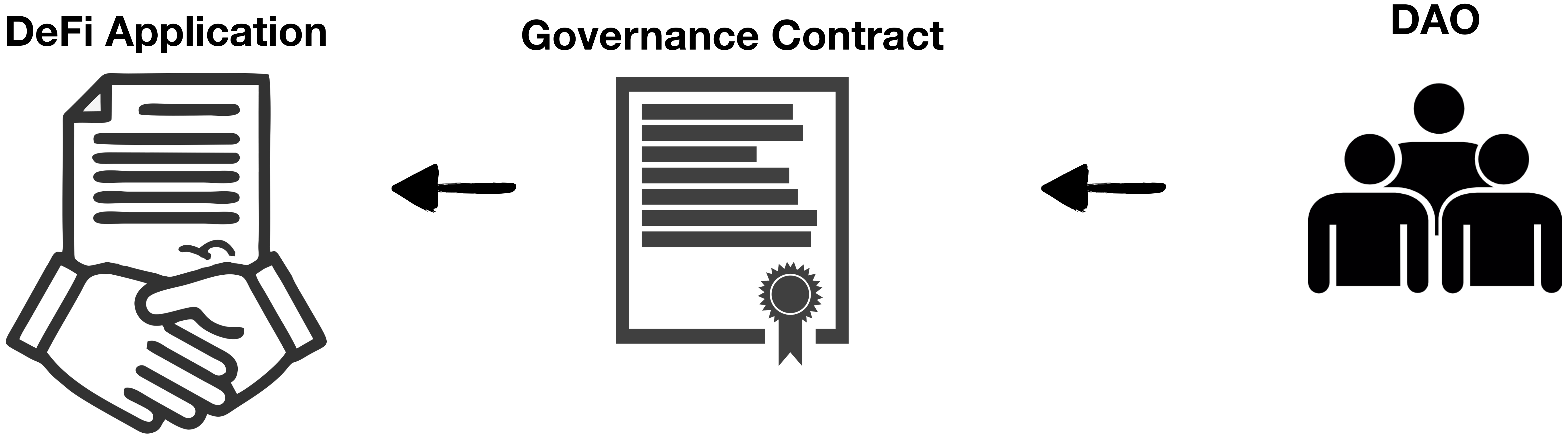
Governance Contracts and DAOs



DeFi Application

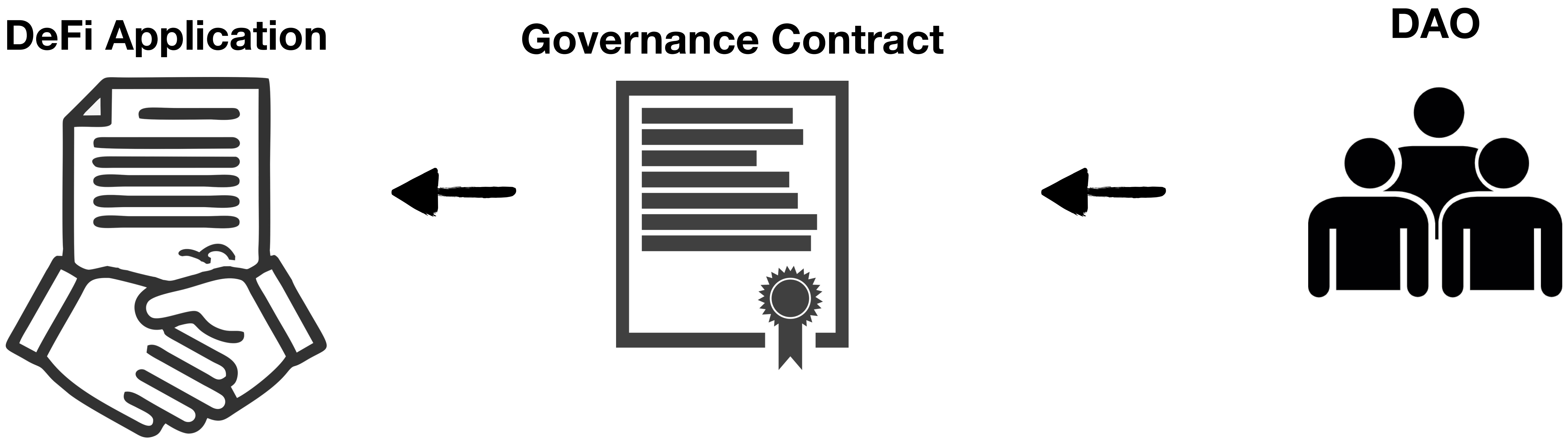
Governance Contract

Governance Contracts and DAOs



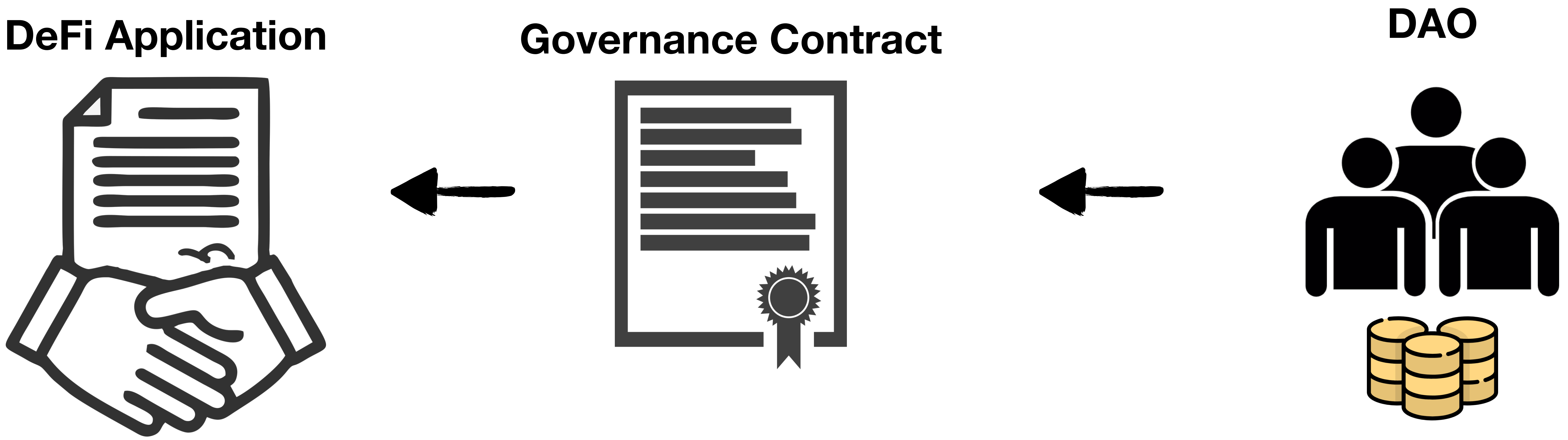
Governance Contracts and DAOs

- DAO consists of the group of holders of the **Governance Token**



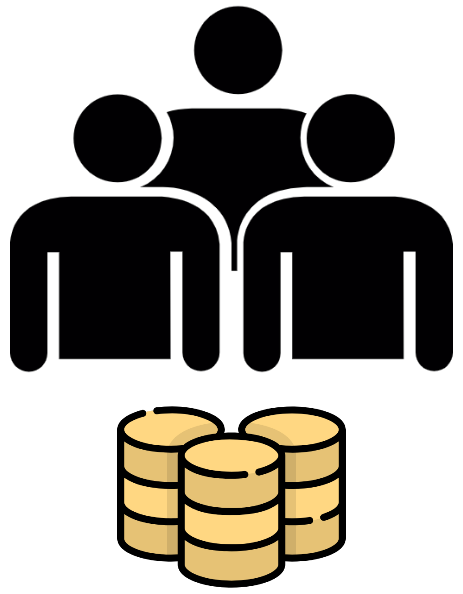
Governance Contracts and DAOs

- DAO consists of the group of holders of the **Governance Token**



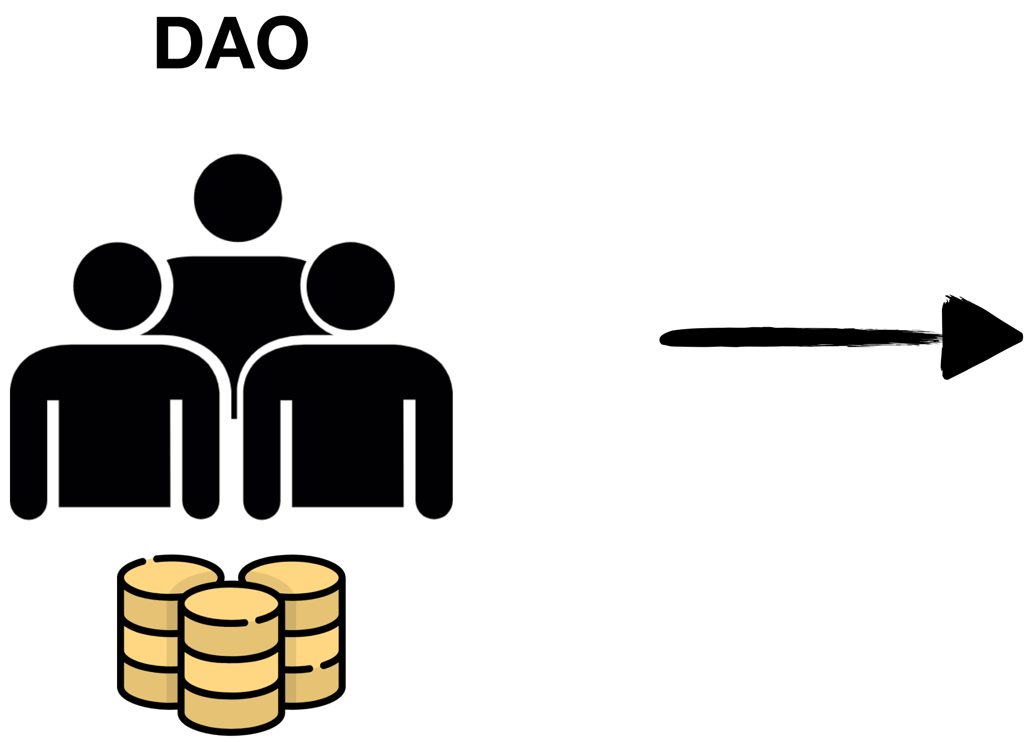
DAOs

DAOs



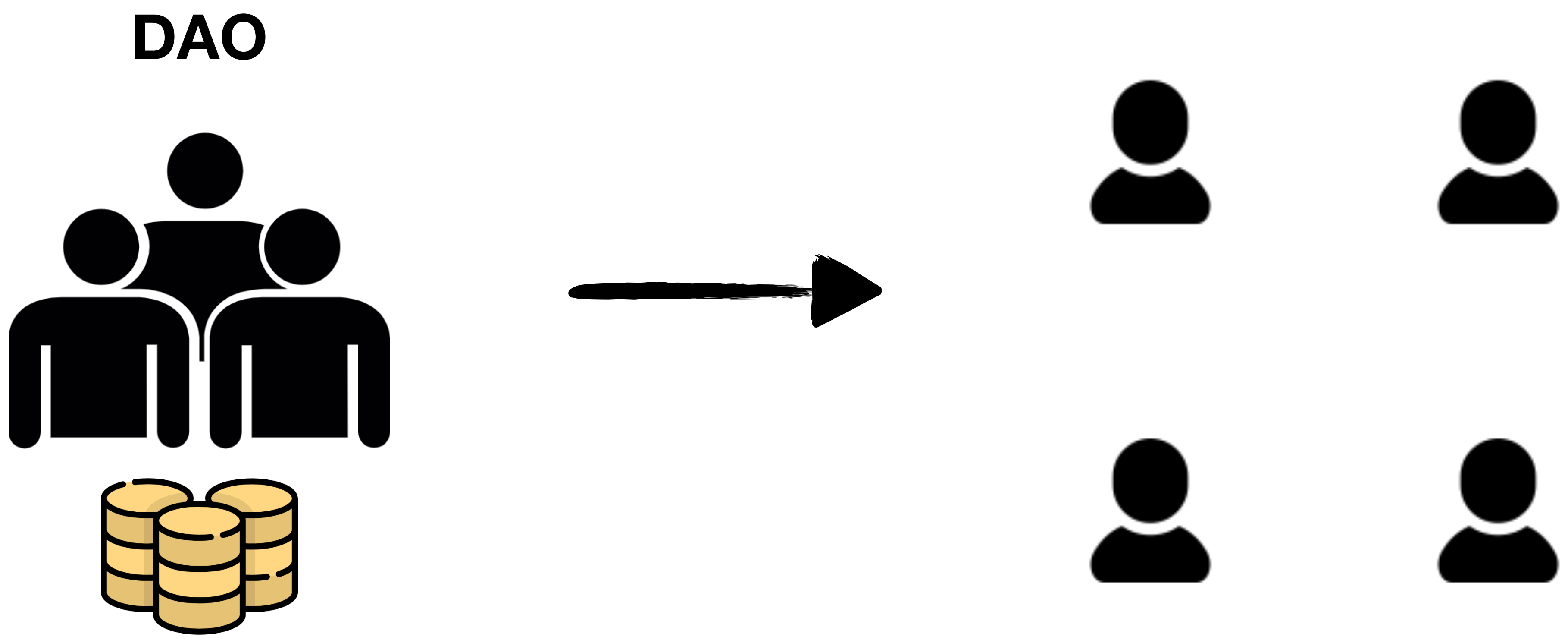
DAO

DAOs

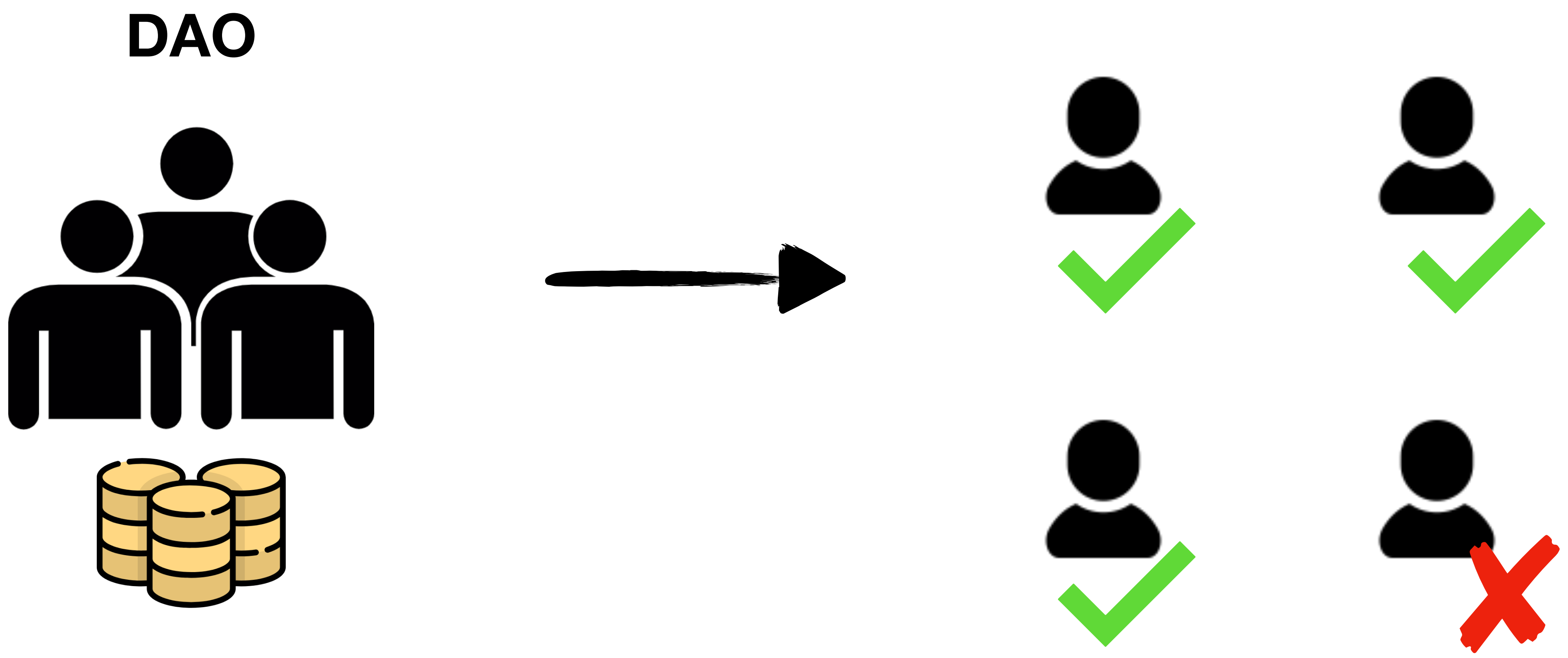


DAO

DAOs

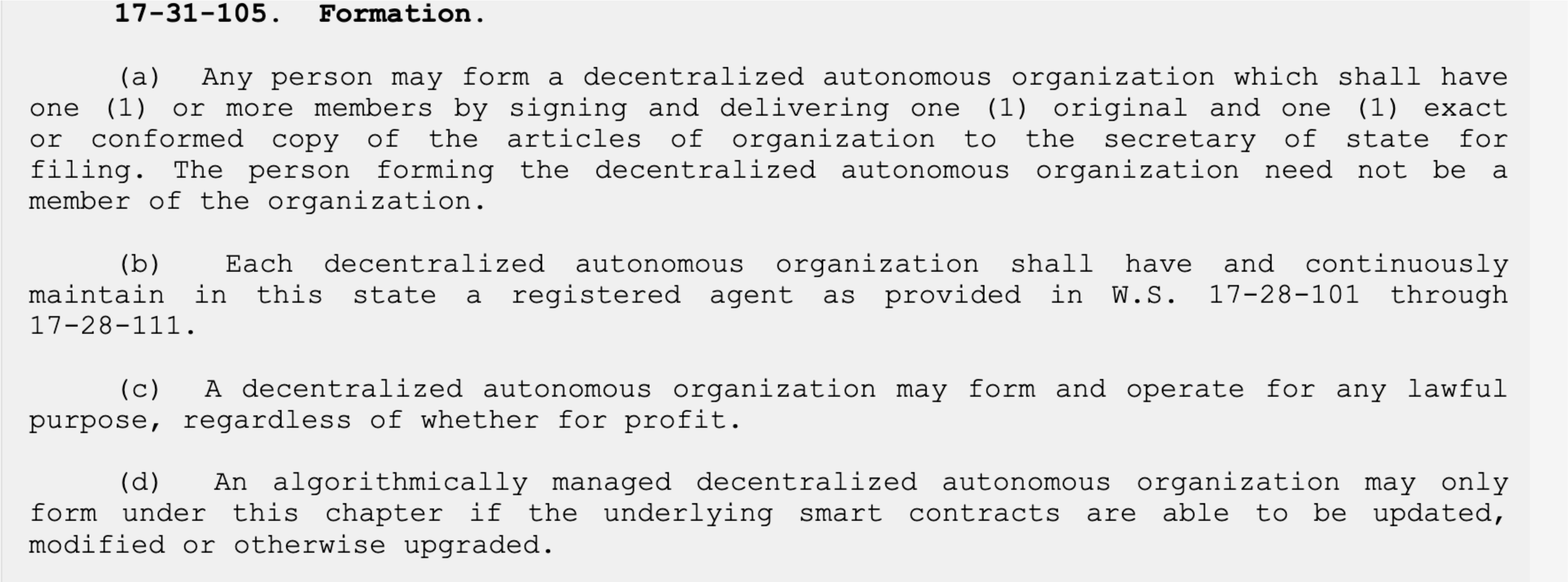


DAOs



DAOs

- *“An algorithmically managed decentralized autonomous organisation may only form under this chapter if the underlying smart contracts are able to be* ***updated, modified or otherwise upgraded****”*



17-31-105. Formation.

(a) Any person may form a decentralized autonomous organization which shall have one (1) or more members by signing and delivering one (1) original and one (1) exact or conformed copy of the articles of organization to the secretary of state for filing. The person forming the decentralized autonomous organization need not be a member of the organization.

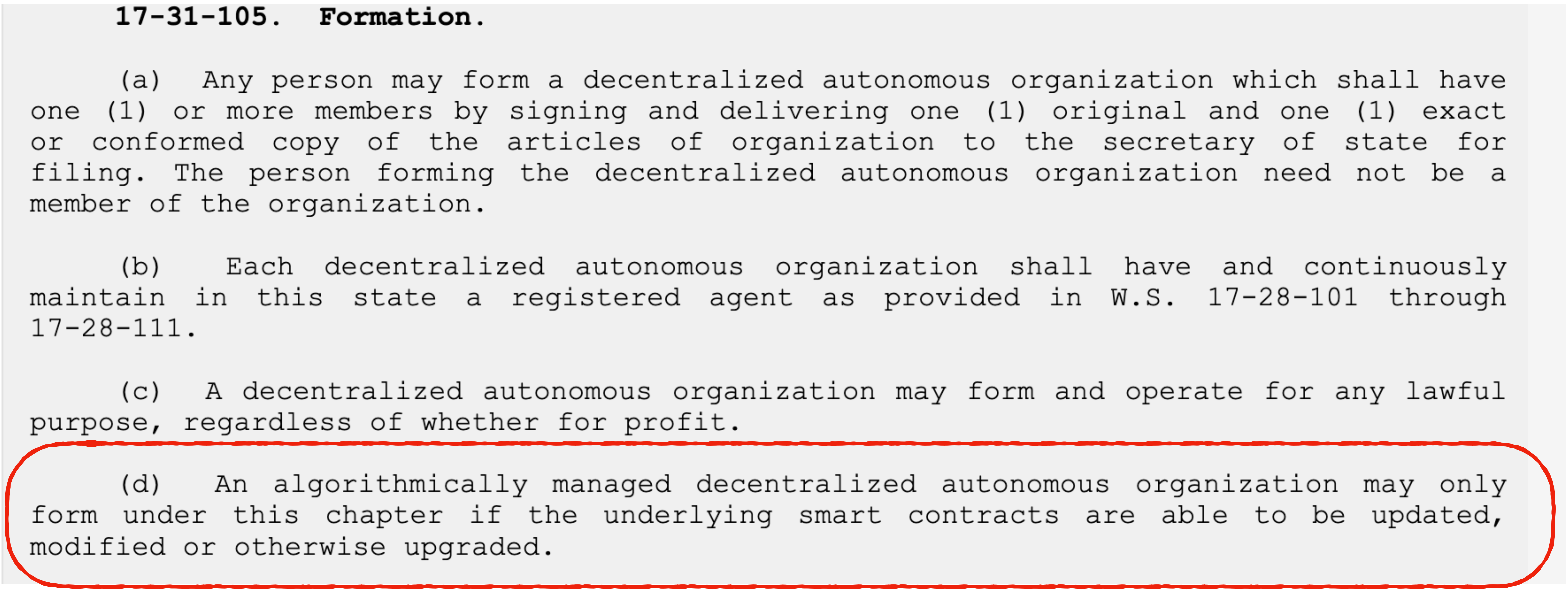
(b) Each decentralized autonomous organization shall have and continuously maintain in this state a registered agent as provided in W.S. 17-28-101 through 17-28-111.

(c) A decentralized autonomous organization may form and operate for any lawful purpose, regardless of whether for profit.

(d) An algorithmically managed decentralized autonomous organization may only form under this chapter if the underlying smart contracts are able to be updated, modified or otherwise upgraded.

DAOs

- *“An algorithmically managed decentralized autonomous organisation may only form under this chapter if the underlying smart contracts are able to be* ***updated, modified or otherwise upgraded****”*



17-31-105. Formation.

(a) Any person may form a decentralized autonomous organization which shall have one (1) or more members by signing and delivering one (1) original and one (1) exact or conformed copy of the articles of organization to the secretary of state for filing. The person forming the decentralized autonomous organization need not be a member of the organization.

(b) Each decentralized autonomous organization shall have and continuously maintain in this state a registered agent as provided in W.S. 17-28-101 through 17-28-111.

(c) A decentralized autonomous organization may form and operate for any lawful purpose, regardless of whether for profit.

(d) An algorithmically managed decentralized autonomous organization may only form under this chapter if the underlying smart contracts are able to be updated, modified or otherwise upgraded.

DAOs in practice

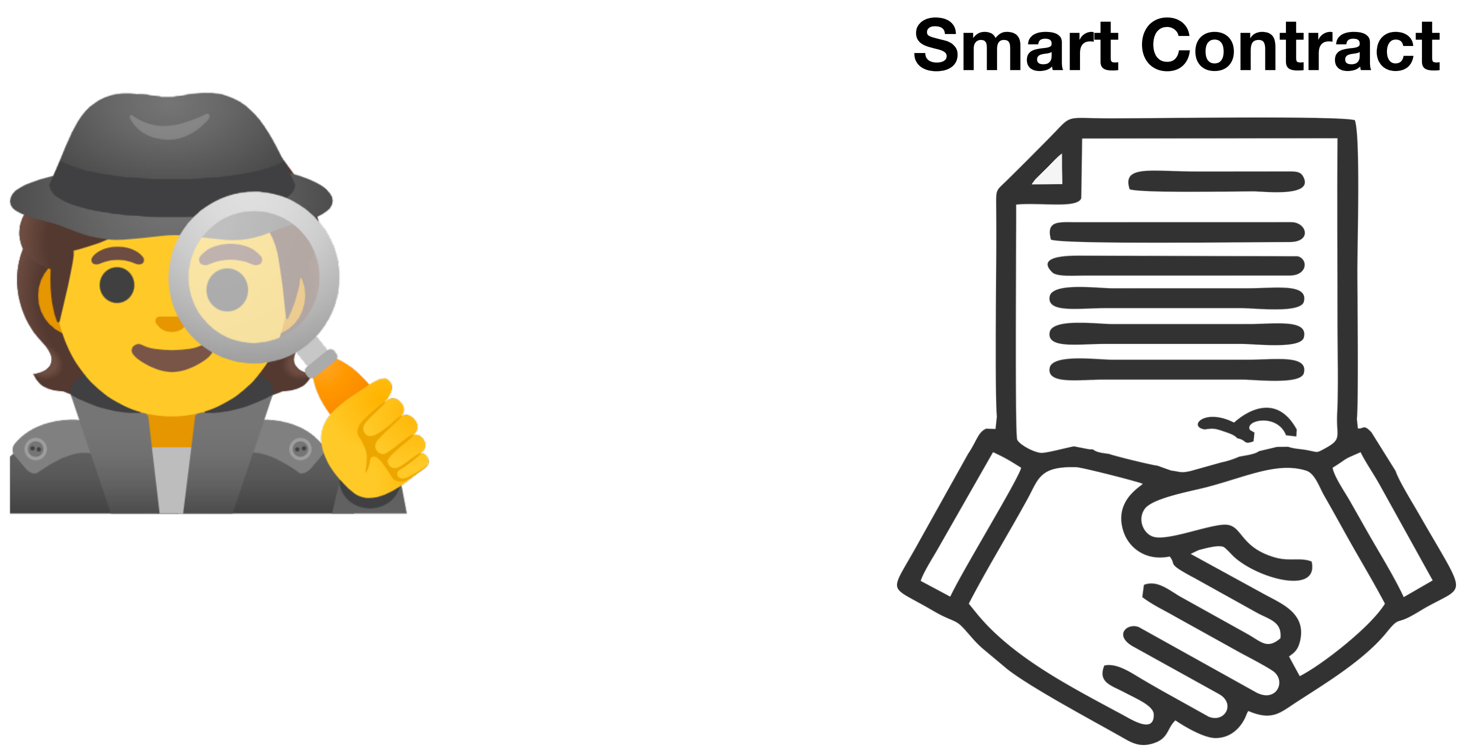
- We analysed the top **51** **DAOs** on Ethereum

DAOs in practice

- We analysed the top **51** **DAOs** on Ethereum

DAOs in practice

- We analysed the top **51** **DAOs** on Ethereum



DAOs in practice

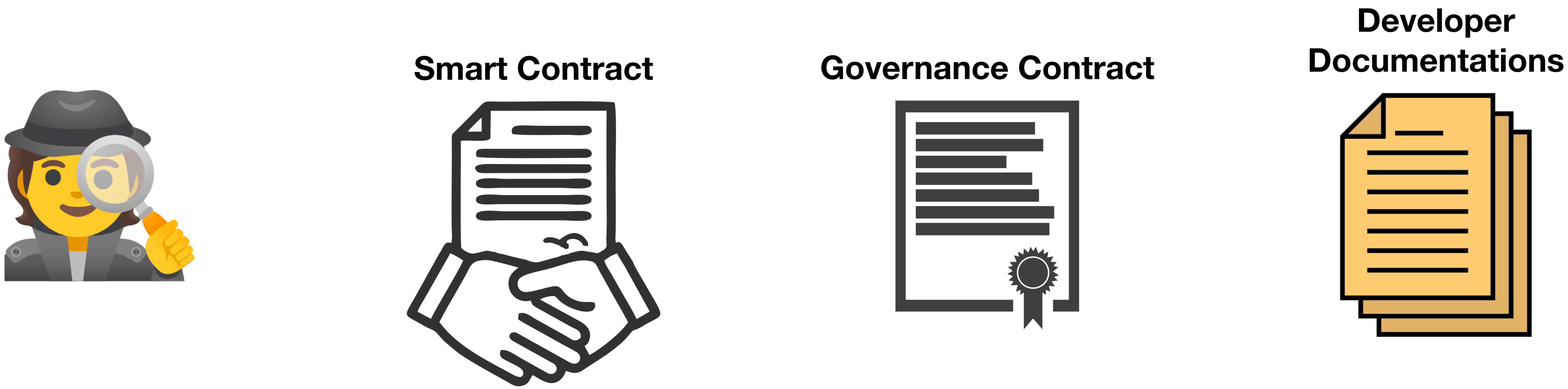
- We analysed the top **51** **DAOs** on Ethereum

Smart Contract

Governance Contract

DAOs in practice

- We analysed the top **51 DAOs** on Ethereum

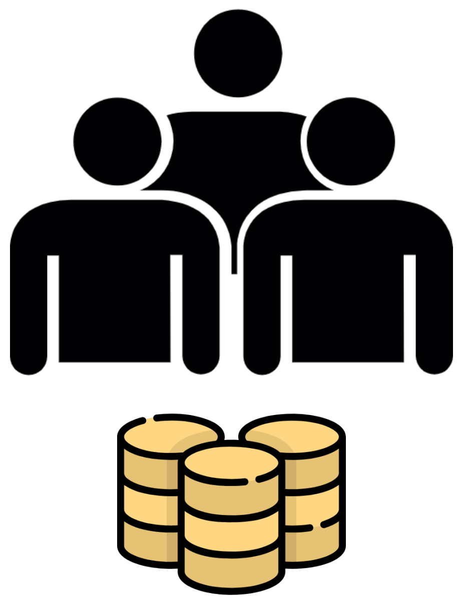


ID	*Protocol*	*RegReq*	*RegMeth*	*VM*	*Call*	*Vot. Plat.*	*Vot. Fmt.*	*Vot. Typ.*	*Vot. Agg*	*Cert.*	*Exec.*	*Veto.*
1	*Uniswap* [9]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	VI
2	*ENS* [10]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	VA
3	*Maker* [11]	👛	S	D	👤	🟢	♻	P	P	👤	👤	–
4	*Lido (Easy Track)* [12]	🏷	H	D	🛡	🟢	🕓	R	M	👤	👤	VI, VA
4	*Lido Governance* [13]	🏷	H	D	◉	🟢	🕓	P	M	👤	👤	–
5	*Frax Finance Omega* [14]	👛	S	D, D•	🛡	🟢	🕓	R	M	👤	👤	VA
5	*Frax Finance Alpha* [14]	👛	S	D, D•	◉	🟢	🕓	R	M	👤	👤	-
6	*AAVE* [15]	🏷	H, S	D, D•	◉	🟢	🕓	P	V	👤	👤	VA
7	*Compound* [16]	👛	H	D, D•	🛡◉	🟢	🕓	P	M	👤	👤	VI, VA
8	*Radicle* [17]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	–
9	*0x Protocol* [18]	👛	S	D, D•	◉	🟢	🕓	P	M	👤	👤	–
10	*Gitcoin* [19]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	–
11	*Silo Finance* [20]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	–
12	*Lyra* [21]	👛	S	D, D•	◉	🟢	🕓	P	M	👤	👤	VA
13	*API3* [22]	👛	S	D, D•	◉	🟢	🕓	P	M	👤	👤	–
14	*Ampleforth* [23]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	VI
15	*Instadapp* [24]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	VI, VA
16	*Rari* [25]	👛	S	D, D•	◉	🟢	🕓	P	M	👤	👤	VI, VA
17	*NounsDAO* [26]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	VI, VA
18	*Curve* [27]	👛	S	D	◉	🟢	🕓	P	T	👤	👤	–
19	*Origin* [28]	👛	S	D, D•	◉	🟢	🕓	P	M	👤	👤	VI
20	*Hop DAO* [29]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	–
21	*Cryptex* [30]	👛	H	D, D•	◉	🟢	🕓	P	M	👤	👤	–
22	*Angle Protocol* [31]	👛	S	D, D•	◉	🟢	🕓	P	M	👤	👤	VI, VA
23	*DxDao* [32]	👛	H	D	👤	🟢	🕓	P	T	👤	👤	–
24	*Nexus Mutual* [33]	👤✓	H	D	🛡	🟢	🕓	P	M	👤, C	👤	VA
25	*Goldfinch* [34]	👤✓	H	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
26	*ParagonsDAO* [35]	🏷	H, S	R	🛡	○	🕓	P	T	C	C	VI, VA
27	*Illuvium* [36]	👛	S	R	🛡	○	🕓	P	T	C	C	VI, VA
28	*SuperRare* [37]	🏷	H	D, D•	🛡	○	🕓	P	M	C, OC	C	VI, VA
29	*Mantle* [38]	👛	H	D, D•	🛡	○	🕓	P	M	C	C	VI, VA
30	*Res. Hub Fdn.* [39]	🏷	H	D	🛡◉	○	🕓	P	M	C	C	VI, VA
31	*Stargate Finance* [40]	👛	S	D, D•	🛡,◉	○	🕓	P	M	C	C	VI, VA
32	*Uma* [41]	👛	S	D, D•	🛡	○	🕓	P	M	C	C	VI, VA
33	*Cowswap* [42]	🏷	H, S	D, D•	🛡◉	○	🕓	P	M	C, OC	C	VI, VA
34	*Sturdy Finance* [43]	🏷	H	D	🛡◉	○	🕓	P	M	C	C	VI, VA
35	*Euler* [44]	👛	H	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
36	*SAFE* [45]	🏷	H, S	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
37	*Tokenlon* [46]	🏷	H, S	D	🛡	○	🕓	P	M	C	C	VI, VA
38	*Botto* [47]	👛	S	D	🛡	○	🕓	P	M	C	C	VI, VA
39	*Balancer* [48]	👛	S	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
40	*Sushiswap* [49]	👛	S	D, D•	🛡	○	🕓	P	M	C	C	VI, VA
41	*Gearbox* [50]	👛	S	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
42	*Paraswap* [51]	👛	S	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
43	*Alchemix* [52]	🏷	H, S	D, D•	🛡	○	🕓	P	M	C	C	VI, VA
44	*1Inch* [53]	👛	S	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
45	*Shutter DAO 0x36* [54]	👛	H	D, D•	🛡,◉	○	🕓	P	M	C	C	VI, VA
46	*Yearn Finance* [55]	👛	S	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
47	*Shapeshift* [56]	🏷	H, S	D, D•	🛡◉	○	🕓	P	M	C	C	VI, VA
48	*Decentraland* [57]	🏷	H	D, D•	🛡	○	🕓	P	M	C	C	VI, VA
49	*Optimism* [58]	👛	H	D, D•	🛡	🟢	🕓	P	M	👤	👤	VA
50	*Arbitrum* [59]	👛	H	D, D•	🛡◉	🟢	🕓	P	M	👤, C	👤	VA
51	*Synthetix* [60]	👛	H	R	🛡	○	🕓	P	T	C	C	VA

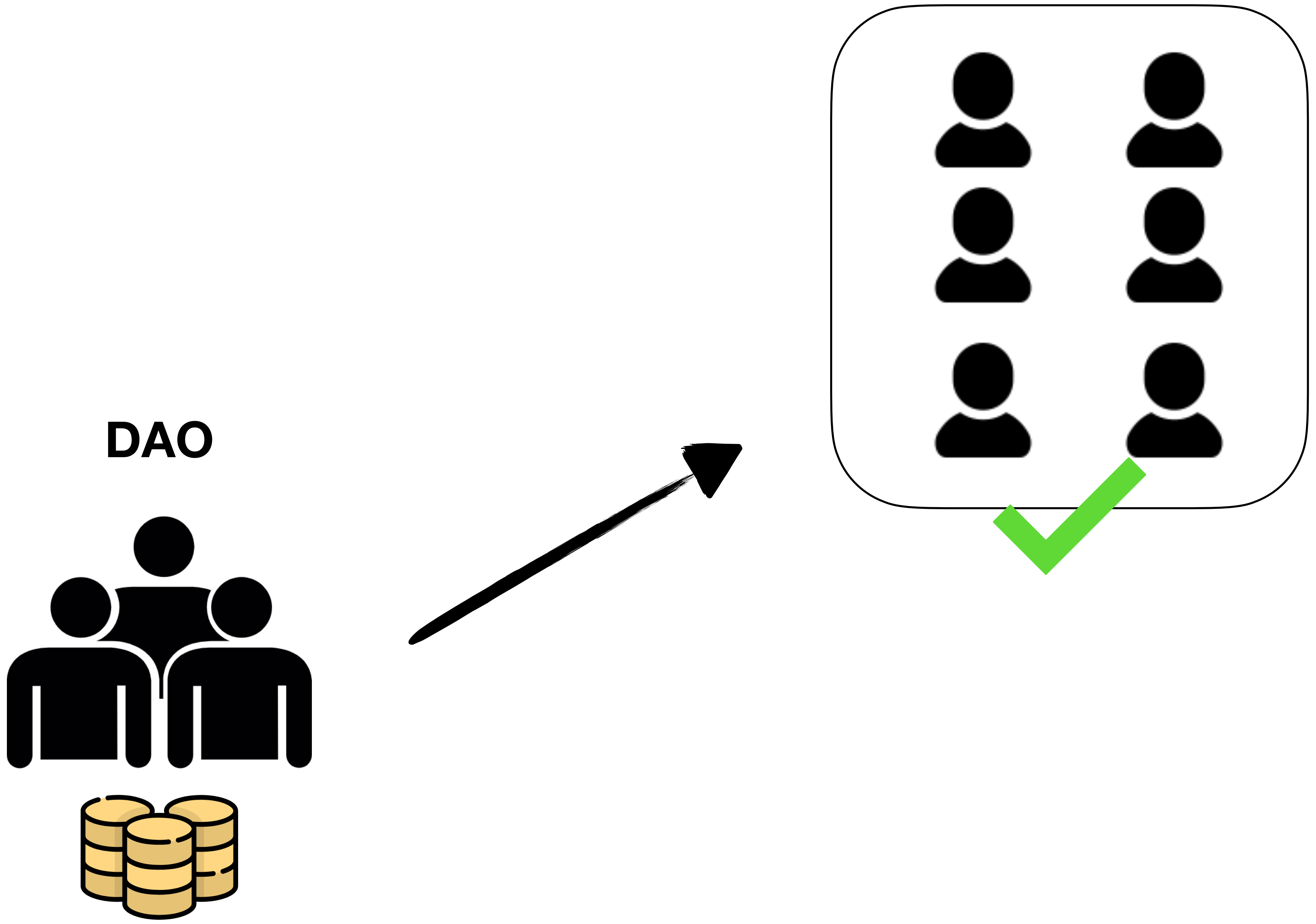
DAOs in practice

DAOs in practice

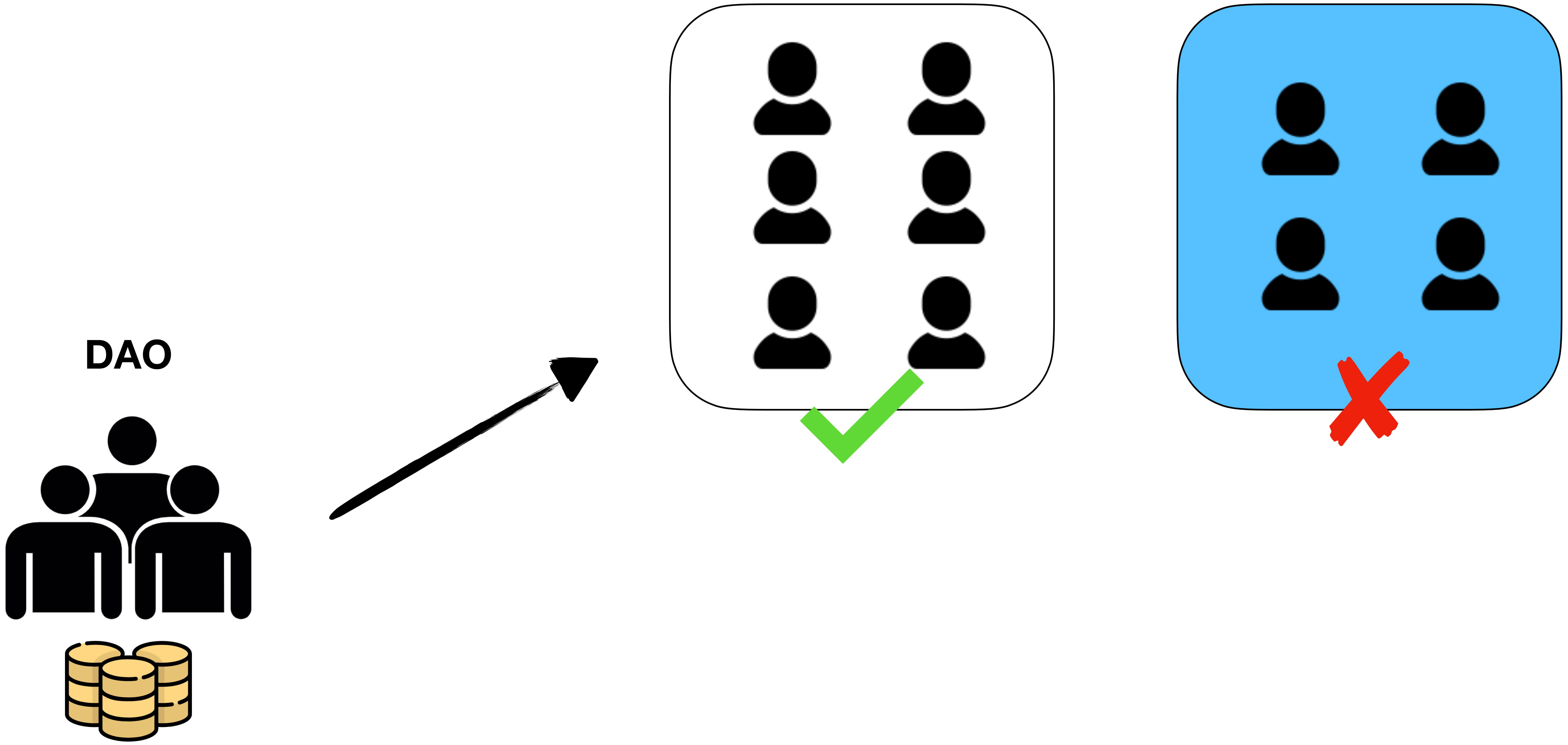
DAO



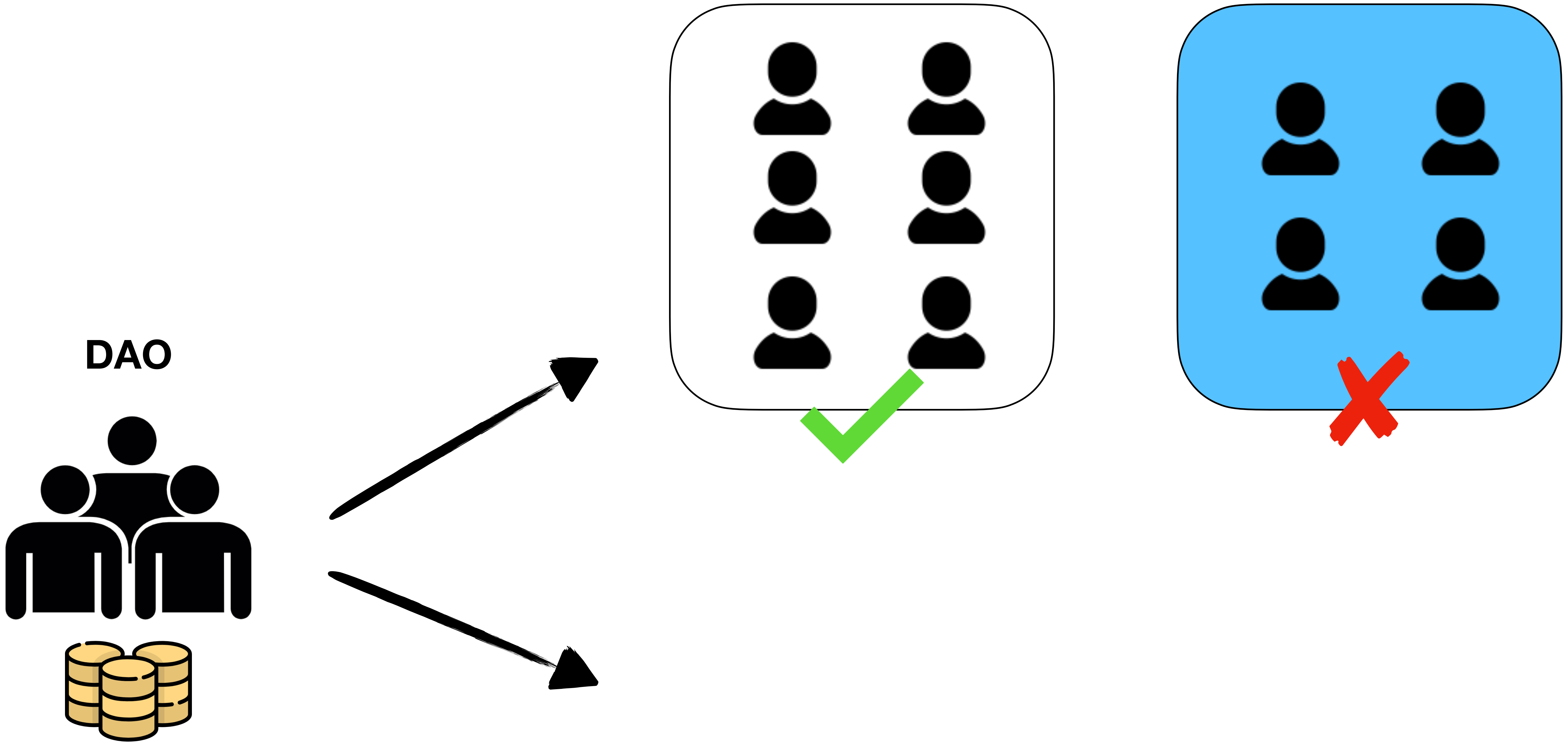
DAOs in practice



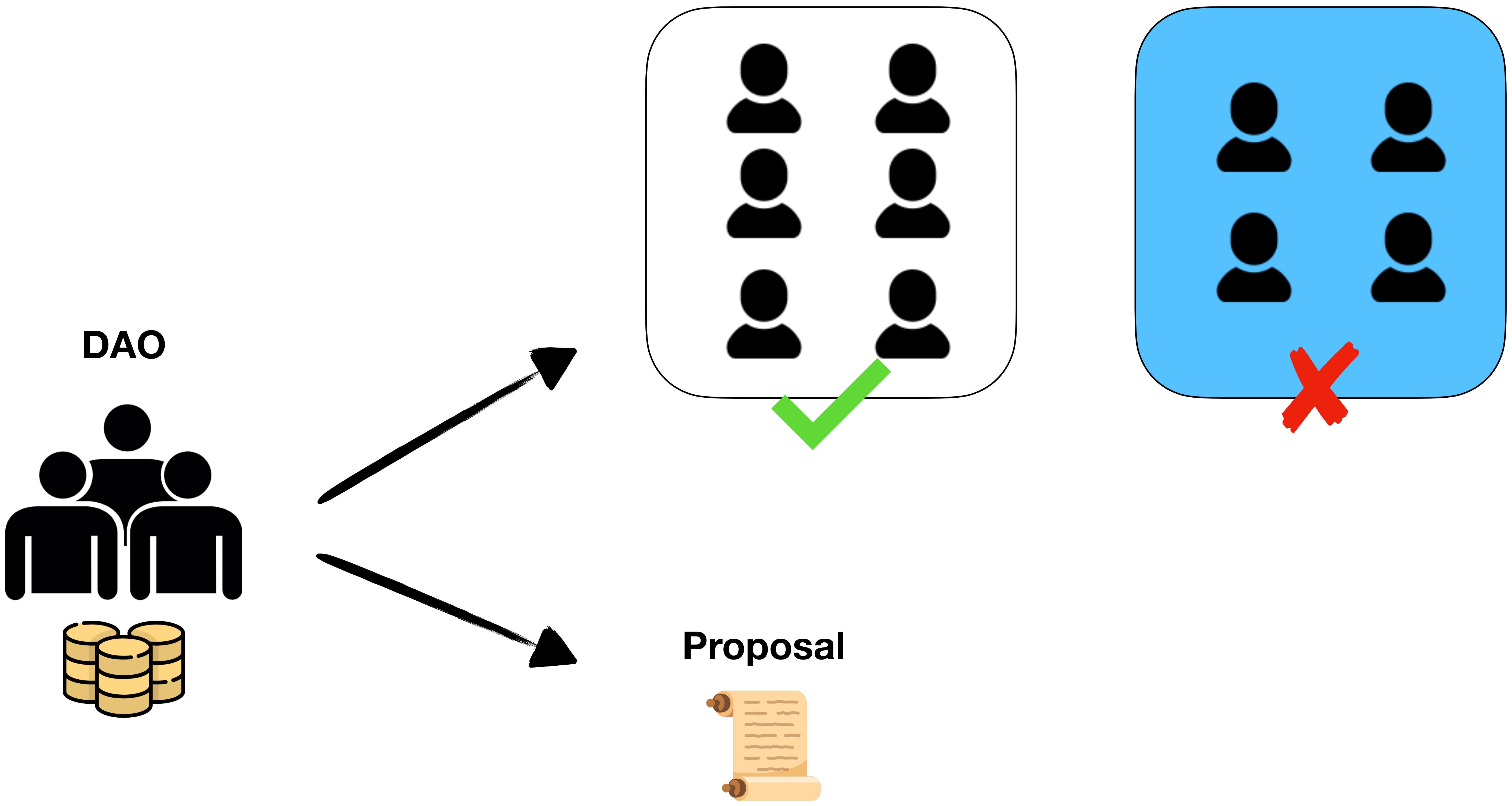
DAOs in practice



DAOs in practice



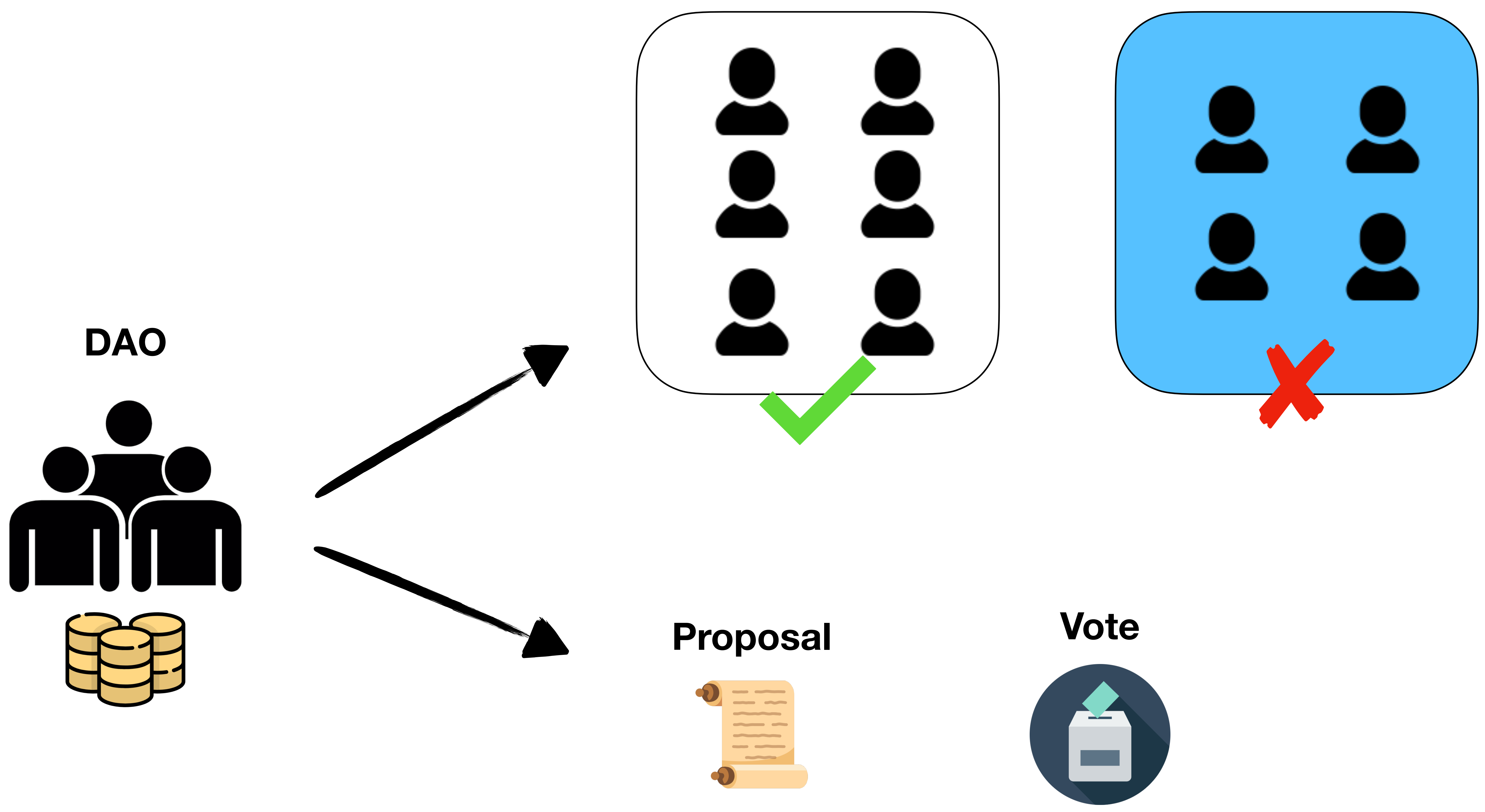
DAOs in practice



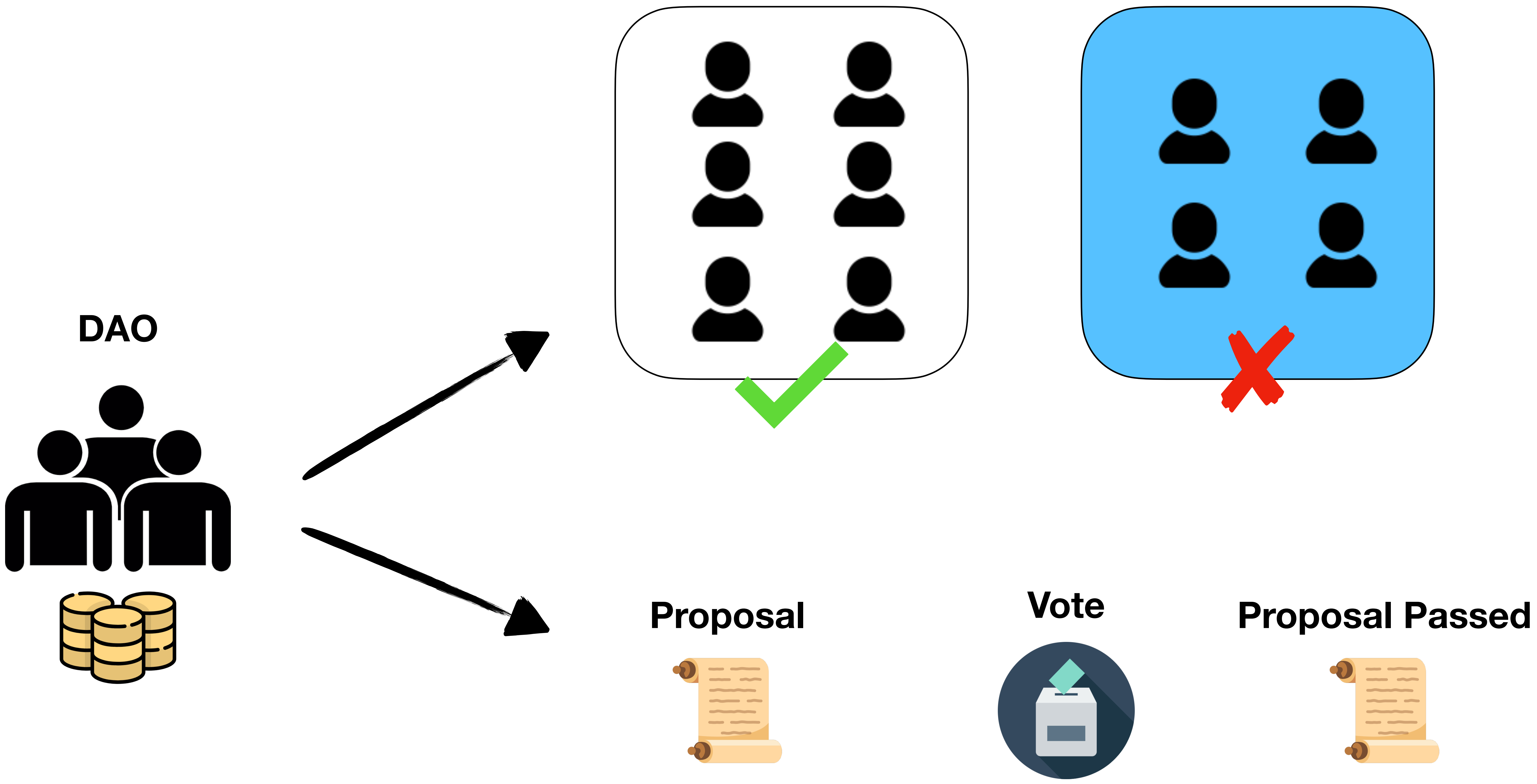
DAO

Proposal

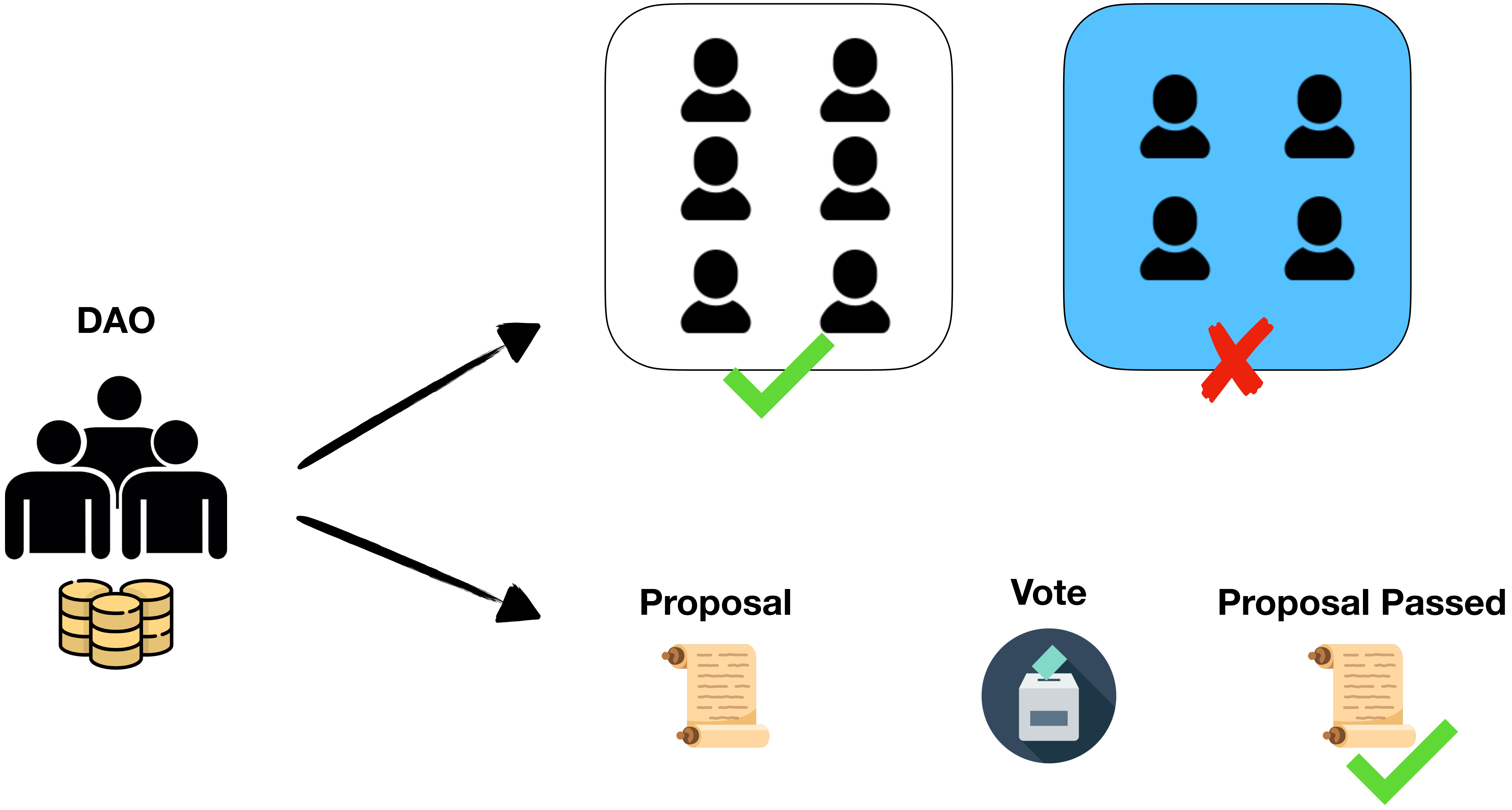
DAOs in practice



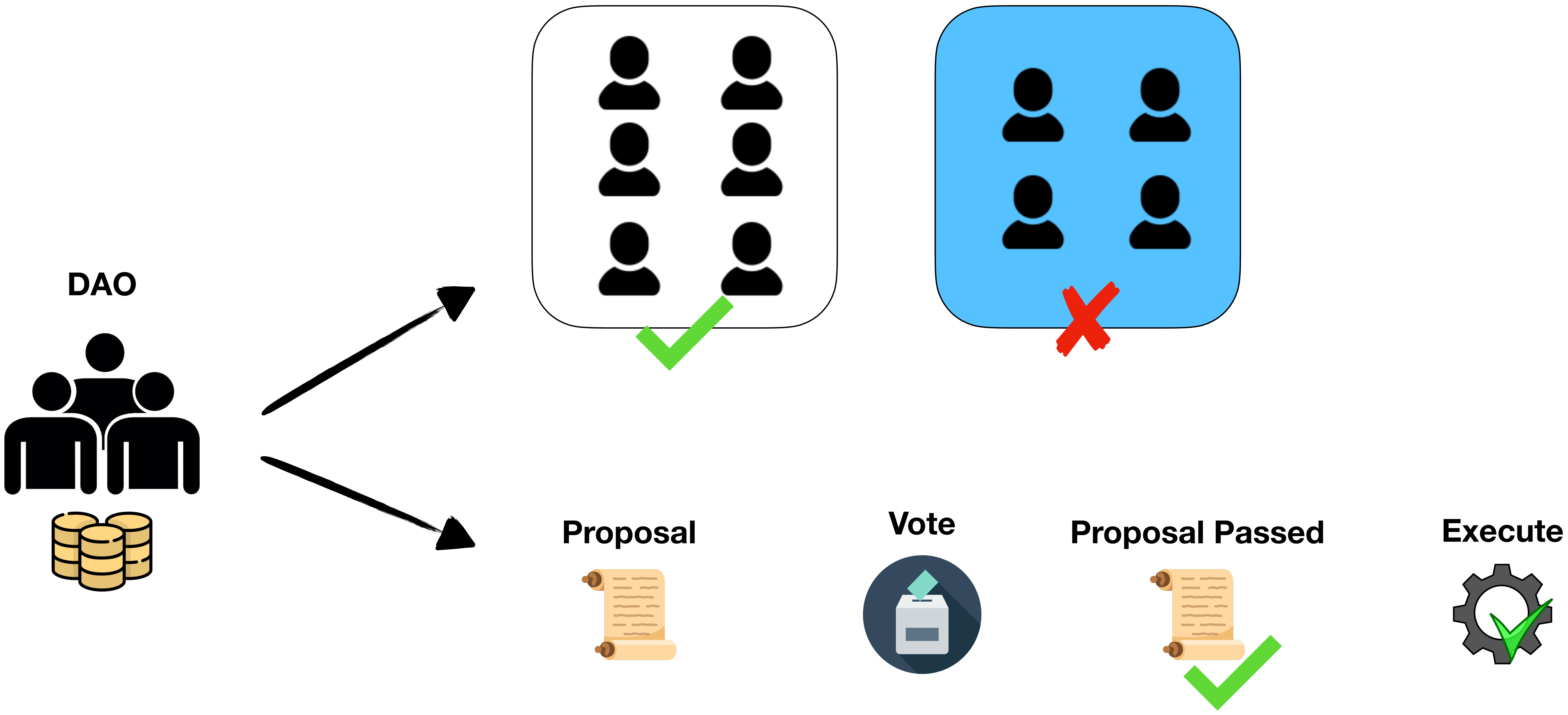
DAOs in practice



DAOs in practice



DAOs in practice



Who can participate in governance?

Registration

- Owning Governance Tokens is not enough!!!
- **39** (**76%**) DAOs require registration

Registration

- Why require Registration?
  - Gatekeeping

Registration

- Why require Registration?
    - Gatekeeping 👤

Registration

- Why require Registration?
  - Gatekeeping

Registration

- Why require Registration?
  - Gatekeeping

Registration

- Why require Registration?
    - Gatekeeping 👤✓ 👤✗

Registration

- Why require Registration?
  - Gatekeeping

Registration

- Why require Registration?
  - Gatekeeping 👤✓ ~~BINANCE~~

Registration: Verified vs Anonymous

Registration: Verified vs Anonymous

Verified

2 total

Registration: Verified vs Anonymous

Verified

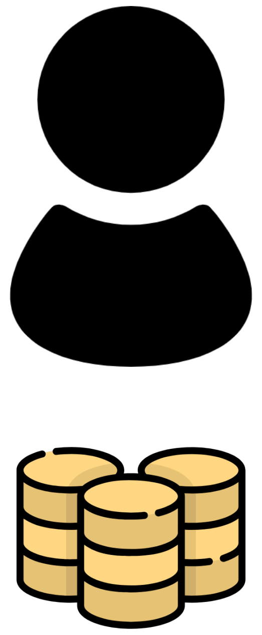
2 total

Anonymous

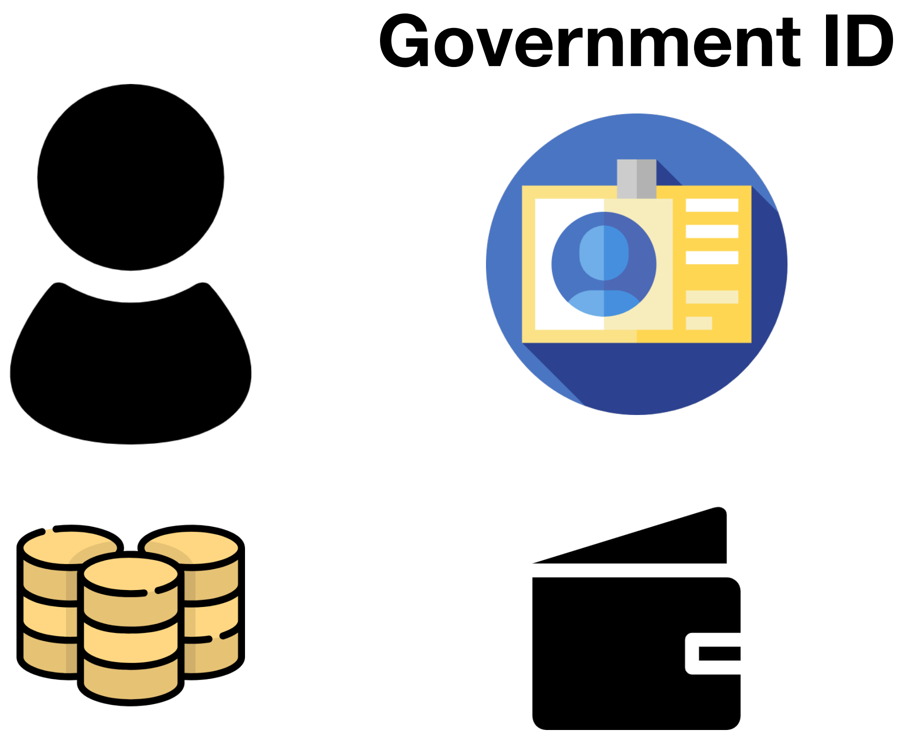
37 total

Verified Registration

Verified Registration

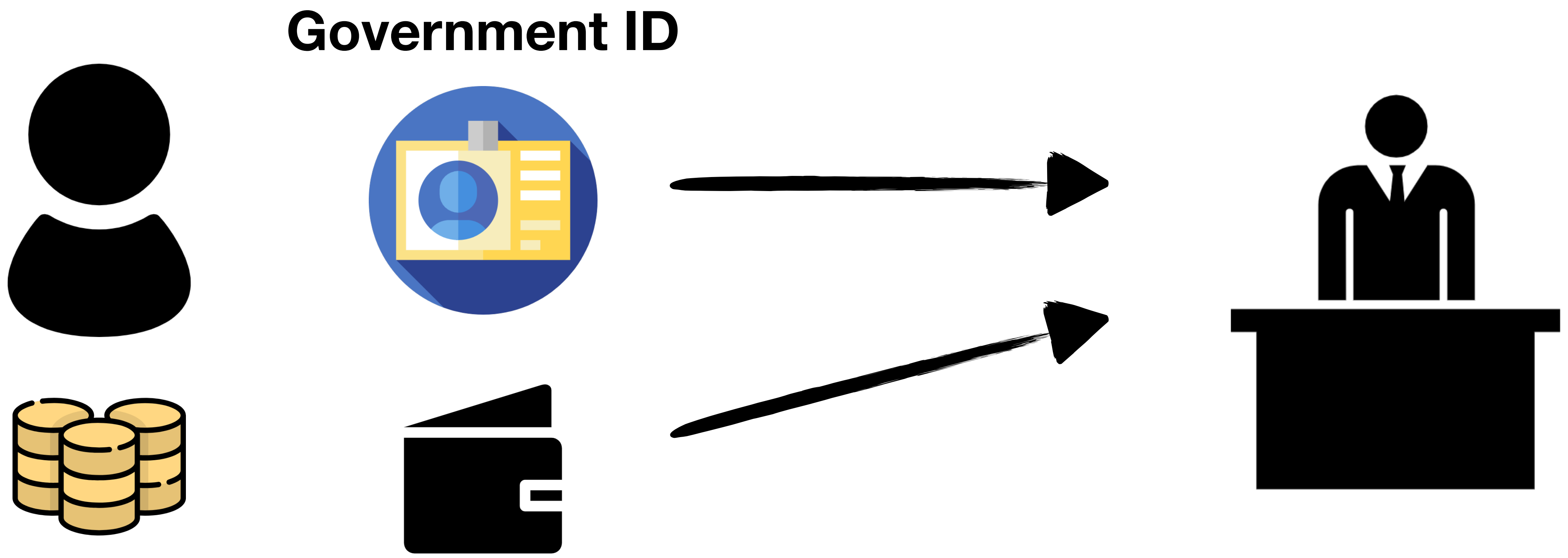


Verified Registration

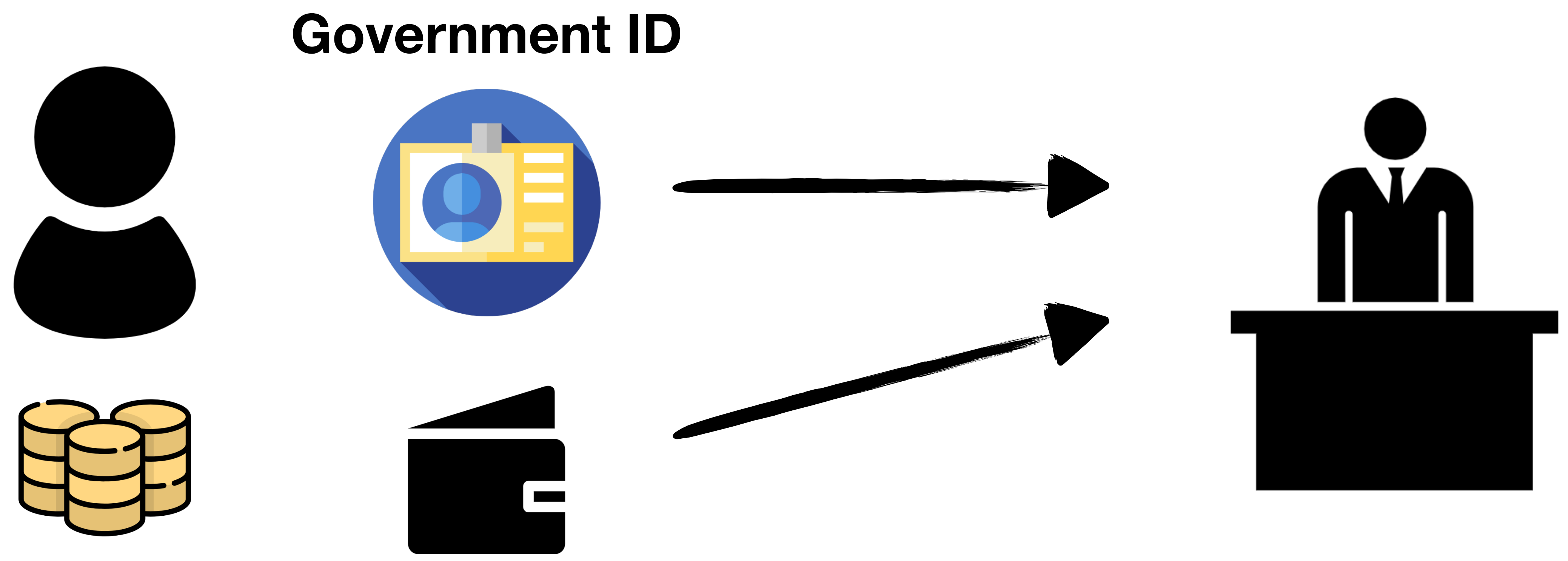


Government ID

Verified Registration



Verified Registration

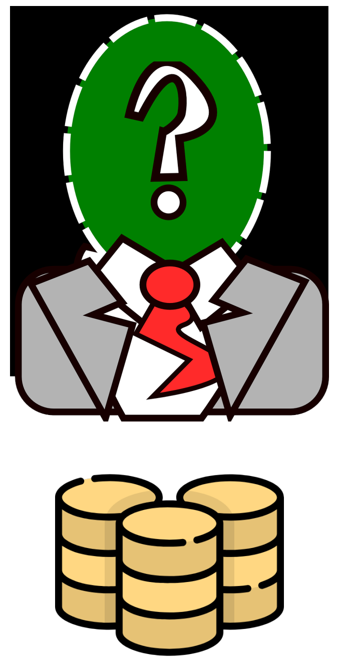


Government ID

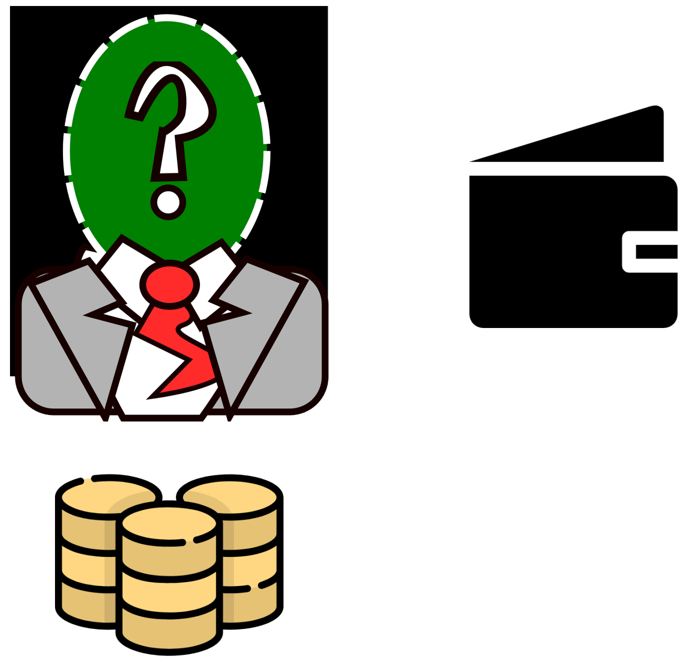
CENTRALIZED

Anonymous Registration

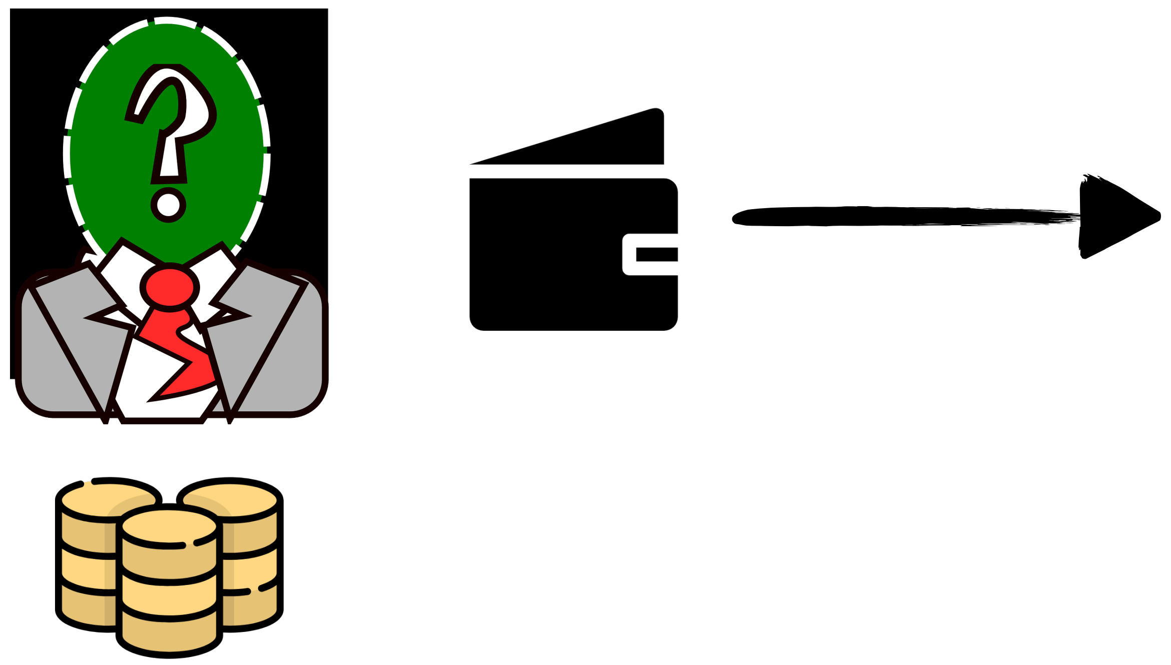
Anonymous Registration



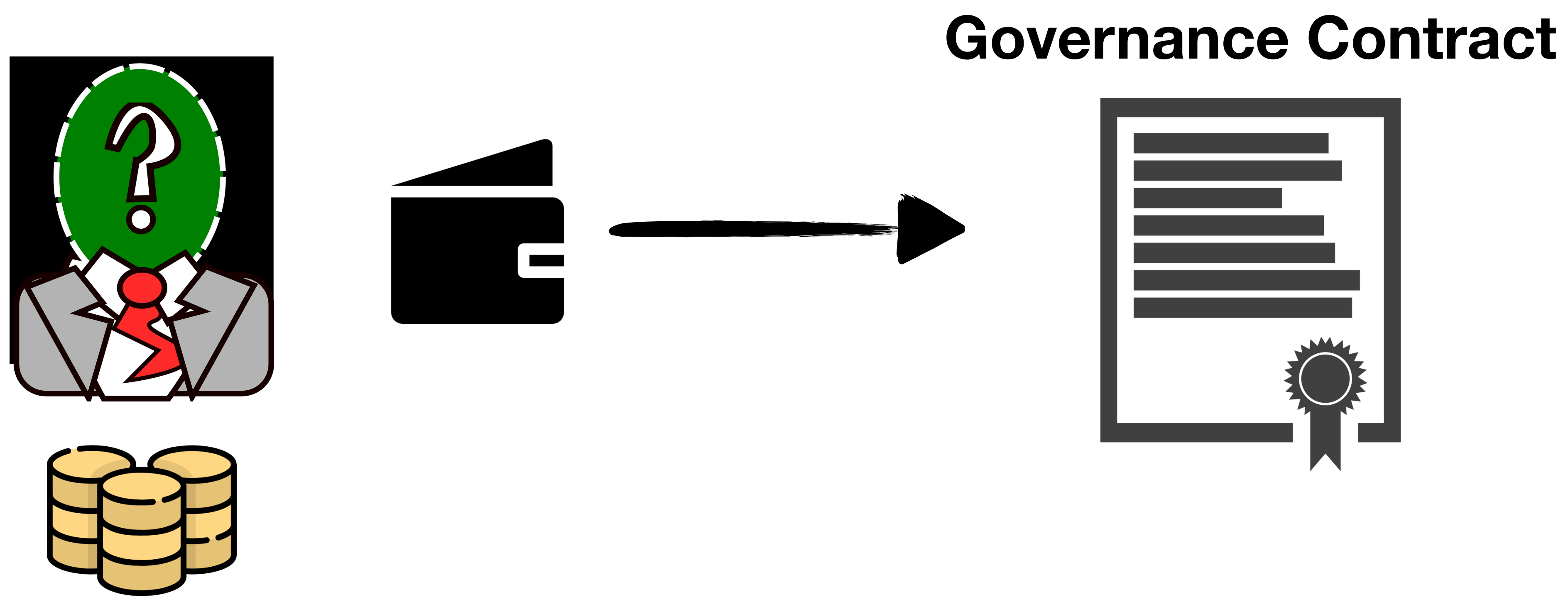
Anonymous Registration



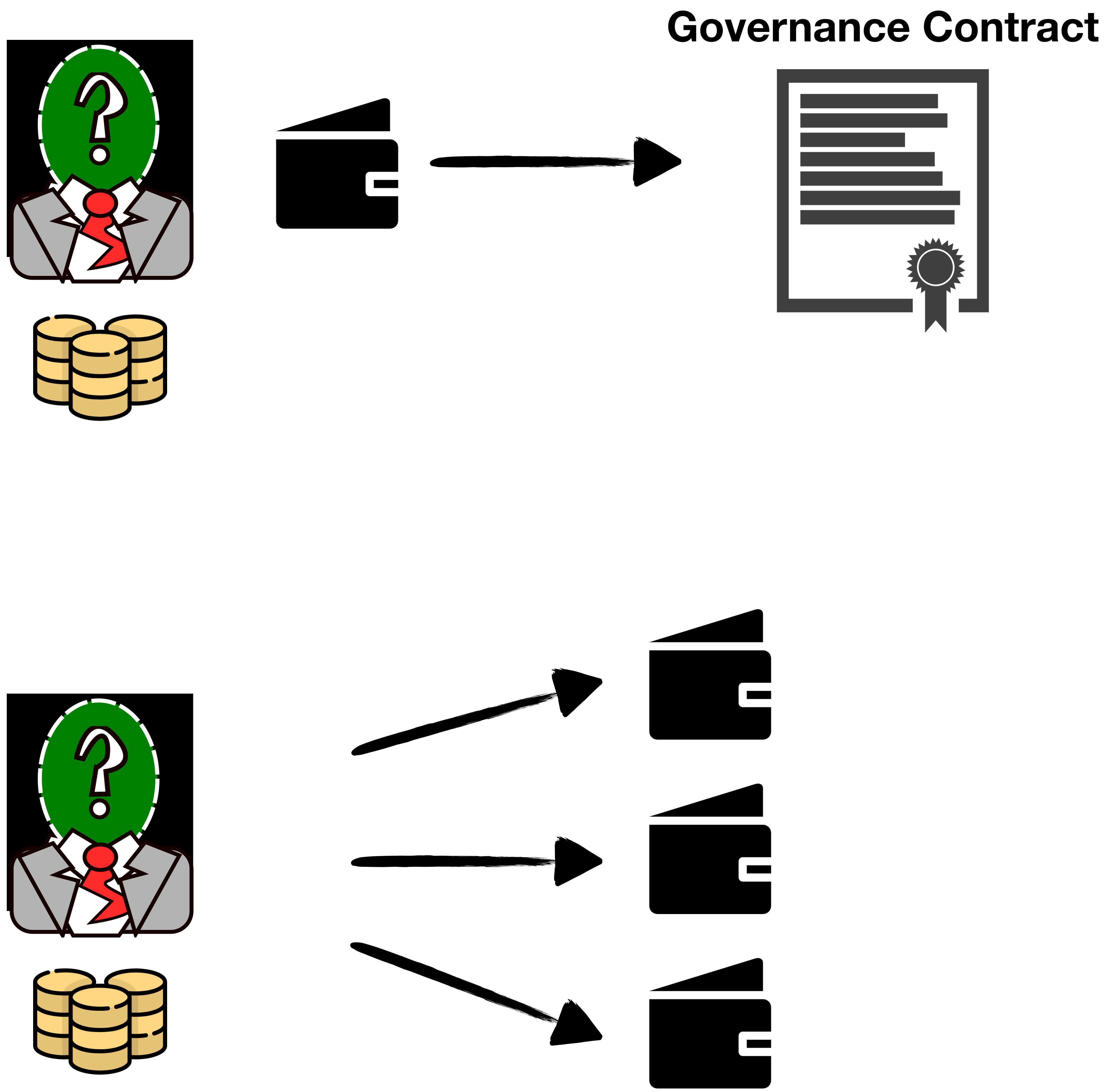
Anonymous Registration



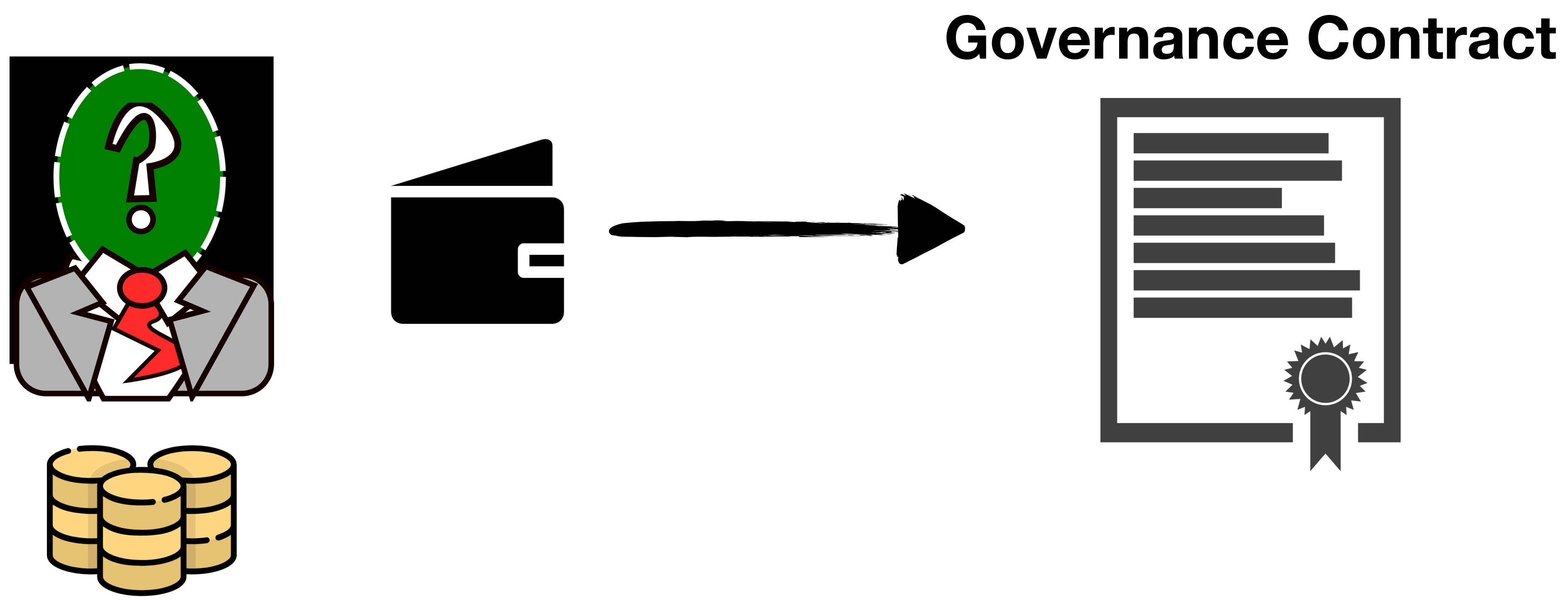
Anonymous Registration

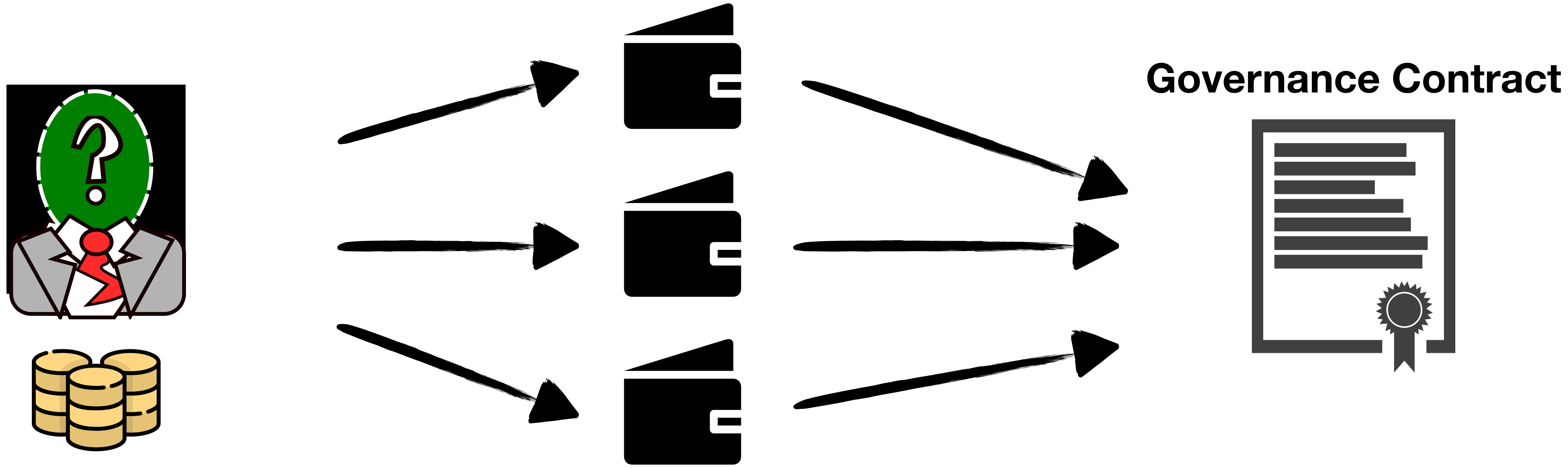


Anonymous Registration



Anonymous Registration





Registration: Token Holding vs. Staking

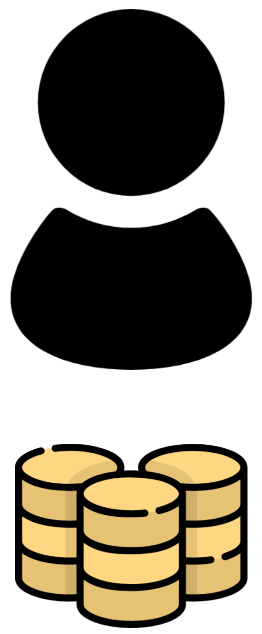
- Token Holding

Registration: Token Holding vs. Staking

- Token Holding

Registration: Token Holding vs. Staking

- Token Holding



Registration: Token Holding vs. Staking

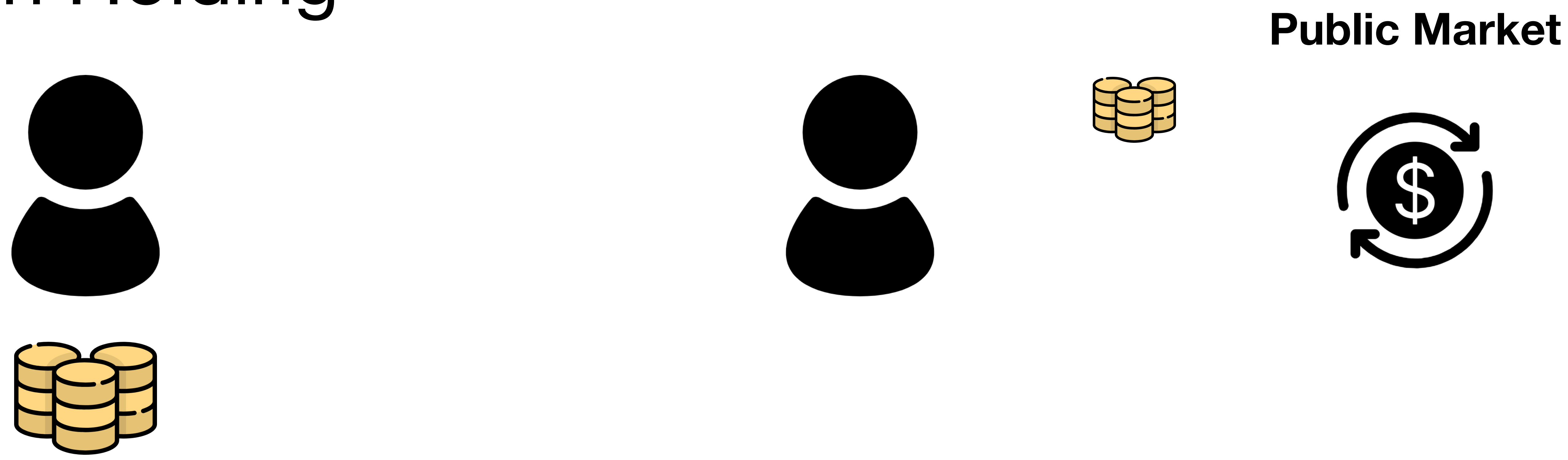
- Token Holding

Registration: Token Holding vs. Staking

- Token Holding

Registration: Token Holding vs. Staking

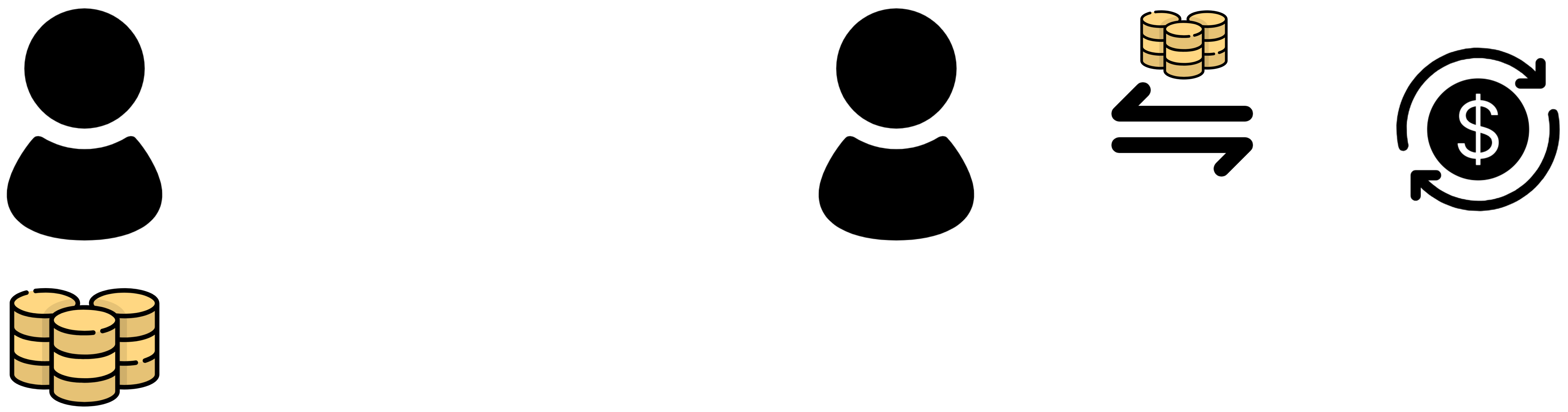
- Token Holding



Public Market

Registration: Token Holding vs. Staking

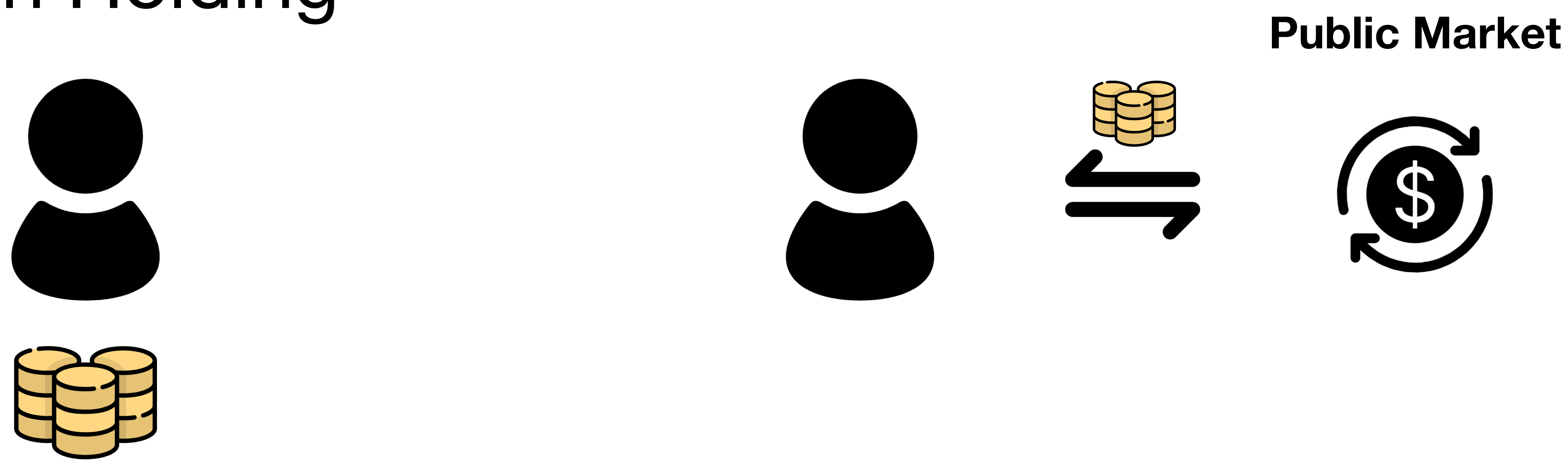
- Token Holding



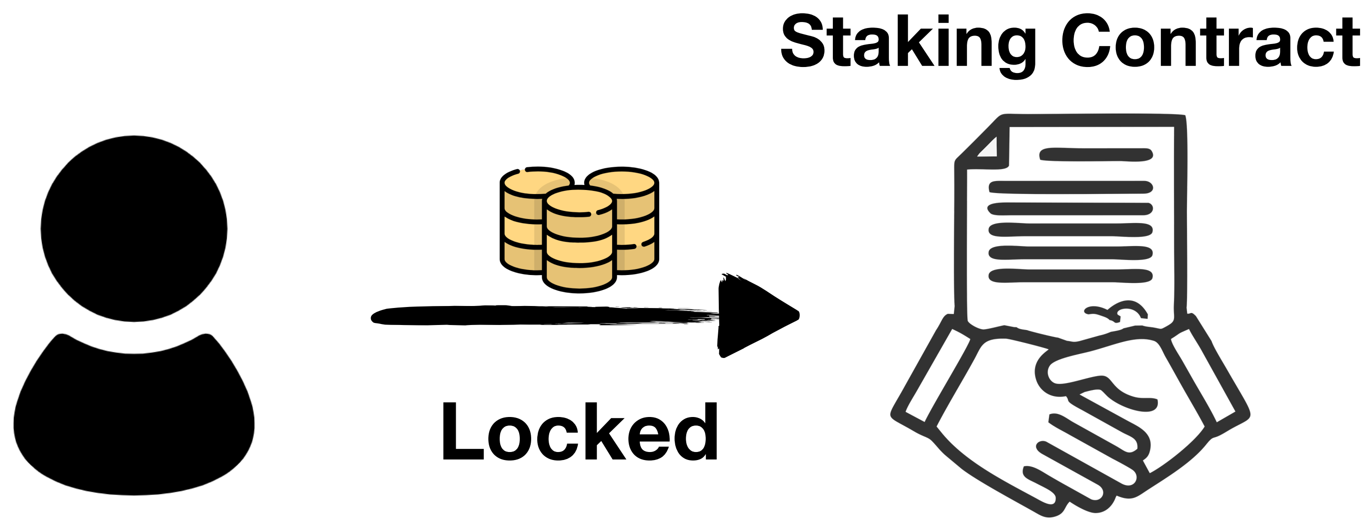
Public Market

Registration: Token Holding vs. Staking

- Token Holding

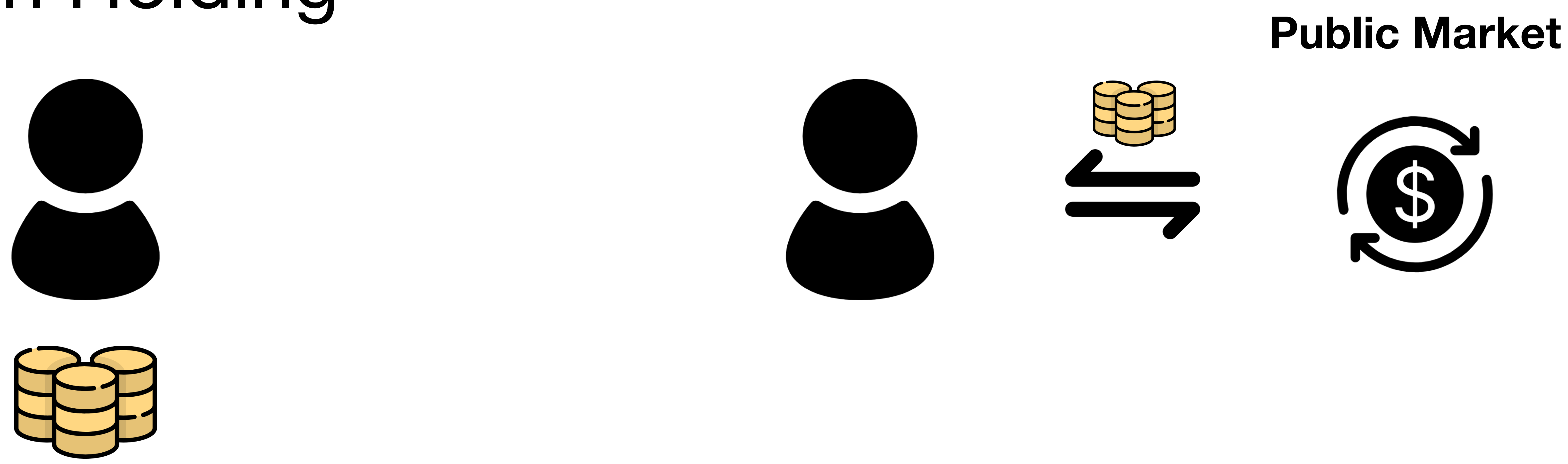


- Token Staking

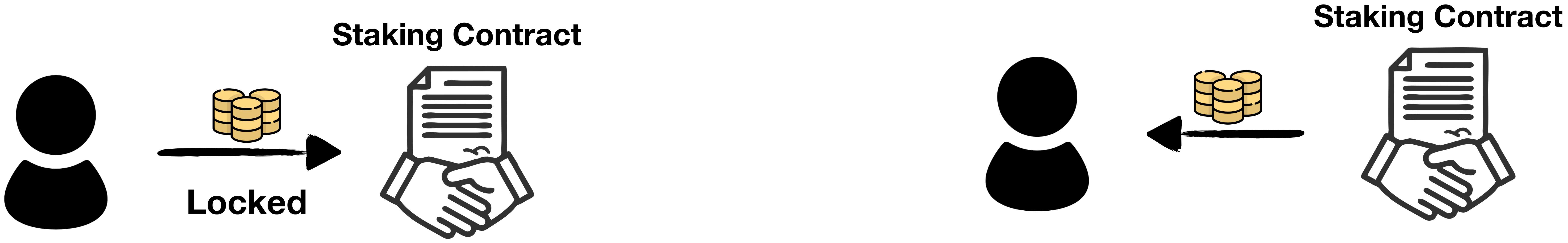


Registration: Token Holding vs. Staking

- Token Holding

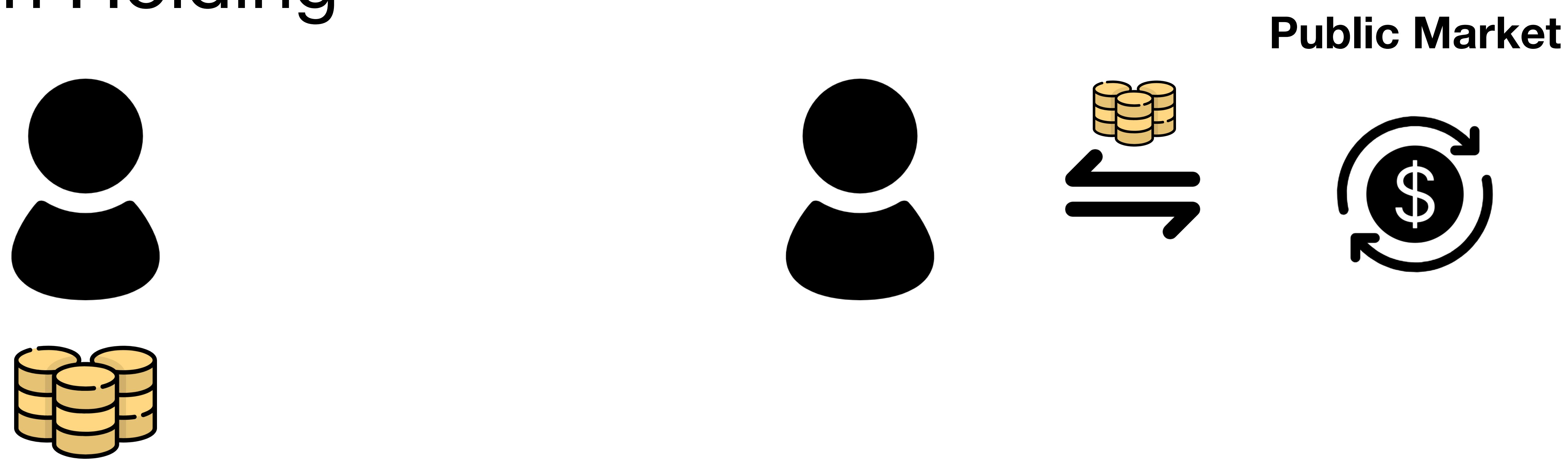


- Token Staking



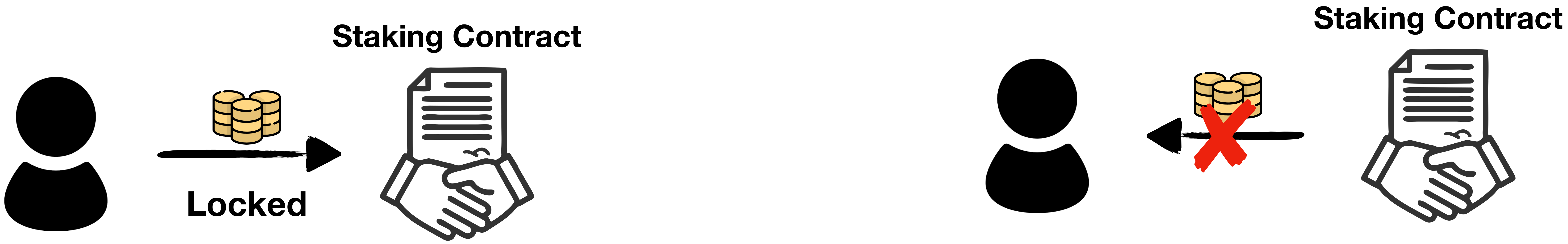
Registration: Token Holding vs. Staking

- Token Holding



Public Market

- Token Staking



Staking Contract

Locked

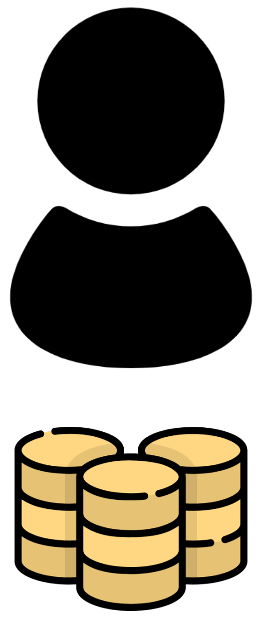
Staking Contract

Governance and Monetary Rights

- Governance Tokens have both **governance** and **monetary** rights !!!

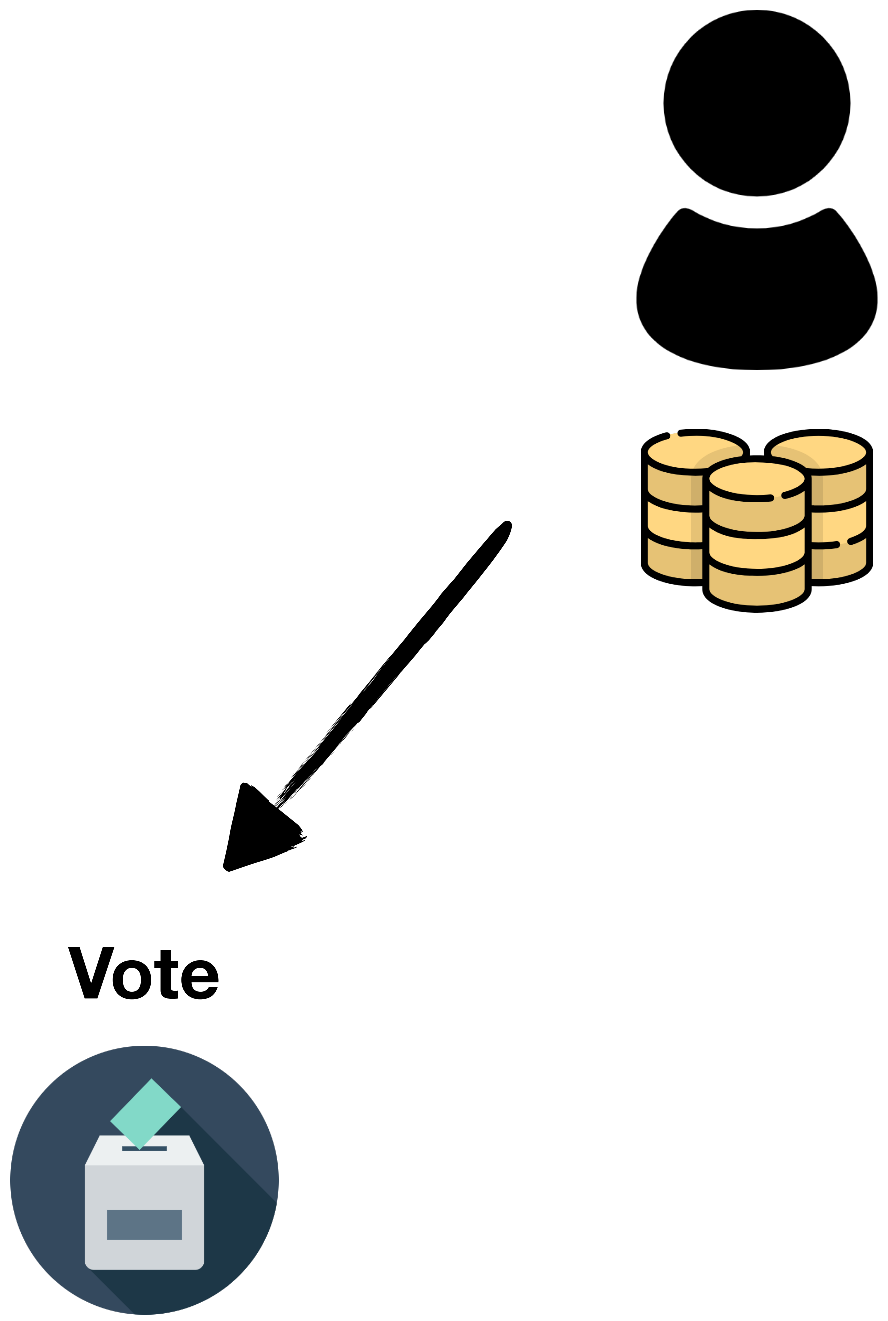
Governance and Monetary Rights

- Governance Tokens have both **governance** and **monetary** rights !!!



Governance and Monetary Rights

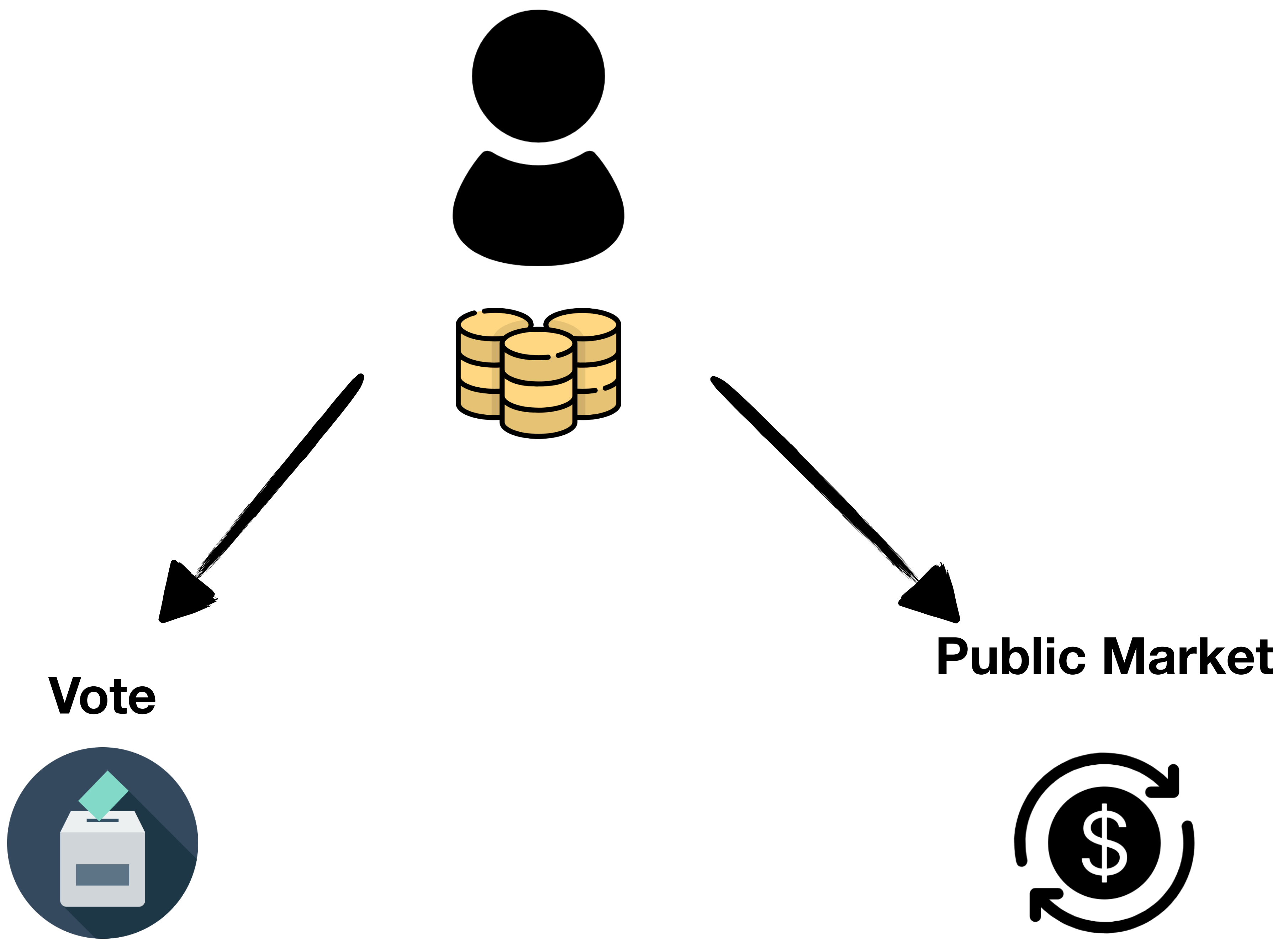
- Governance Tokens have both **governance** and **monetary** rights !!!



Vote

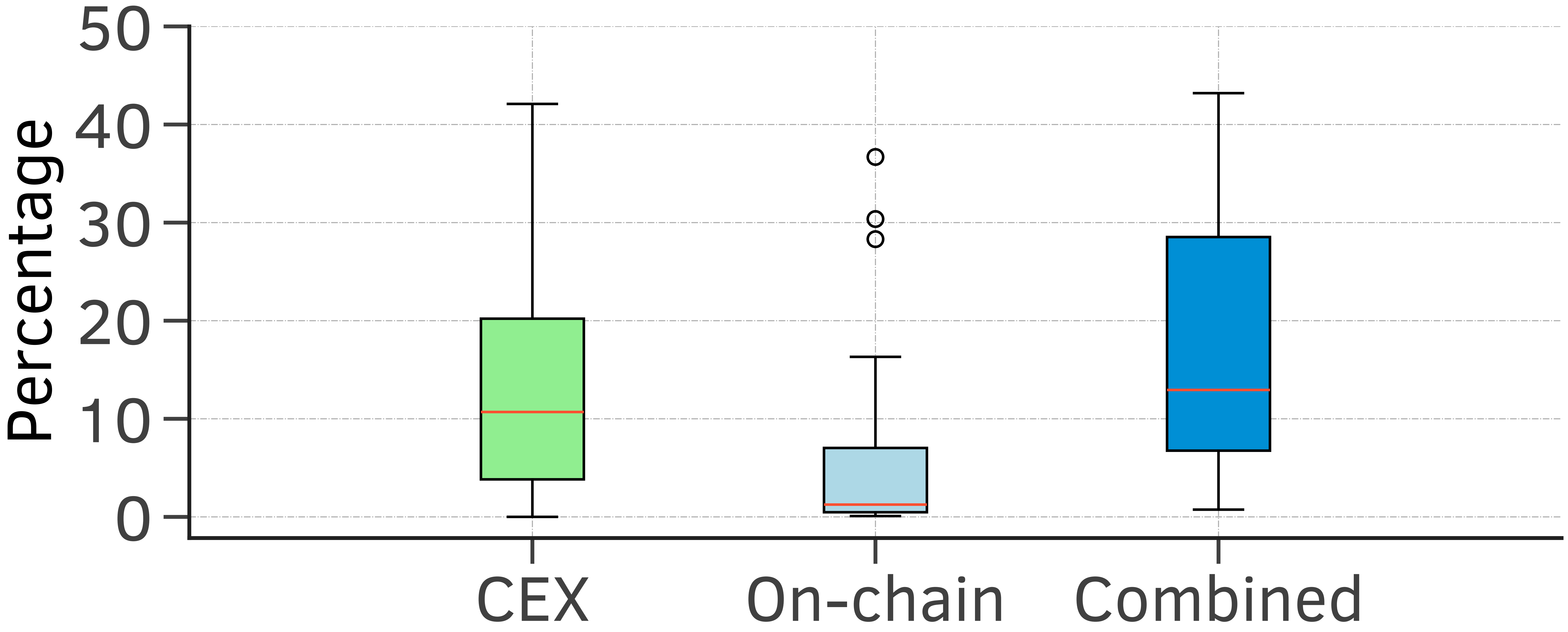
Governance and Monetary Rights

- Governance Tokens have both **governance** and **monetary** rights !!!



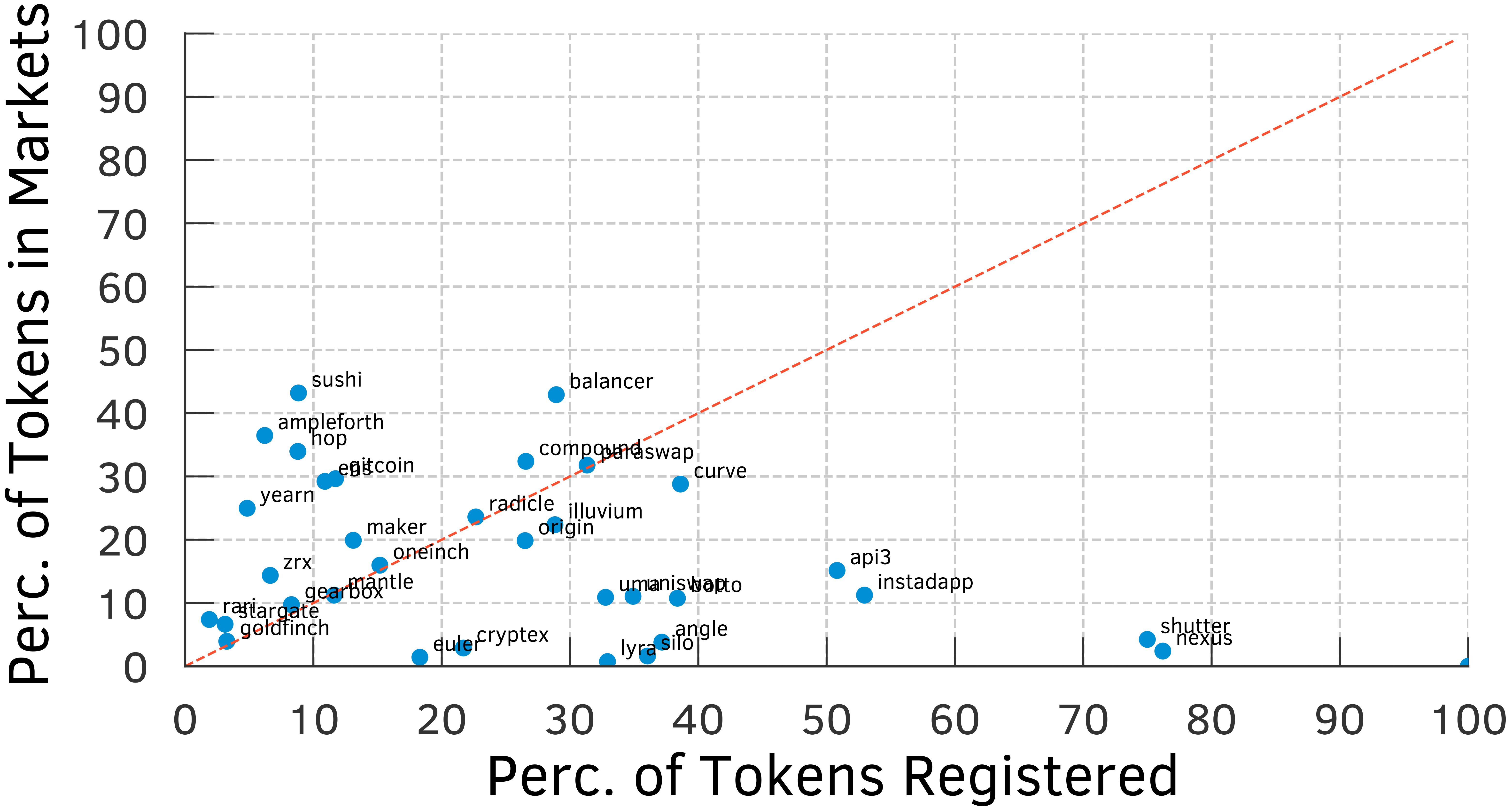
Public Markets

- Custodians own a lot of tokens



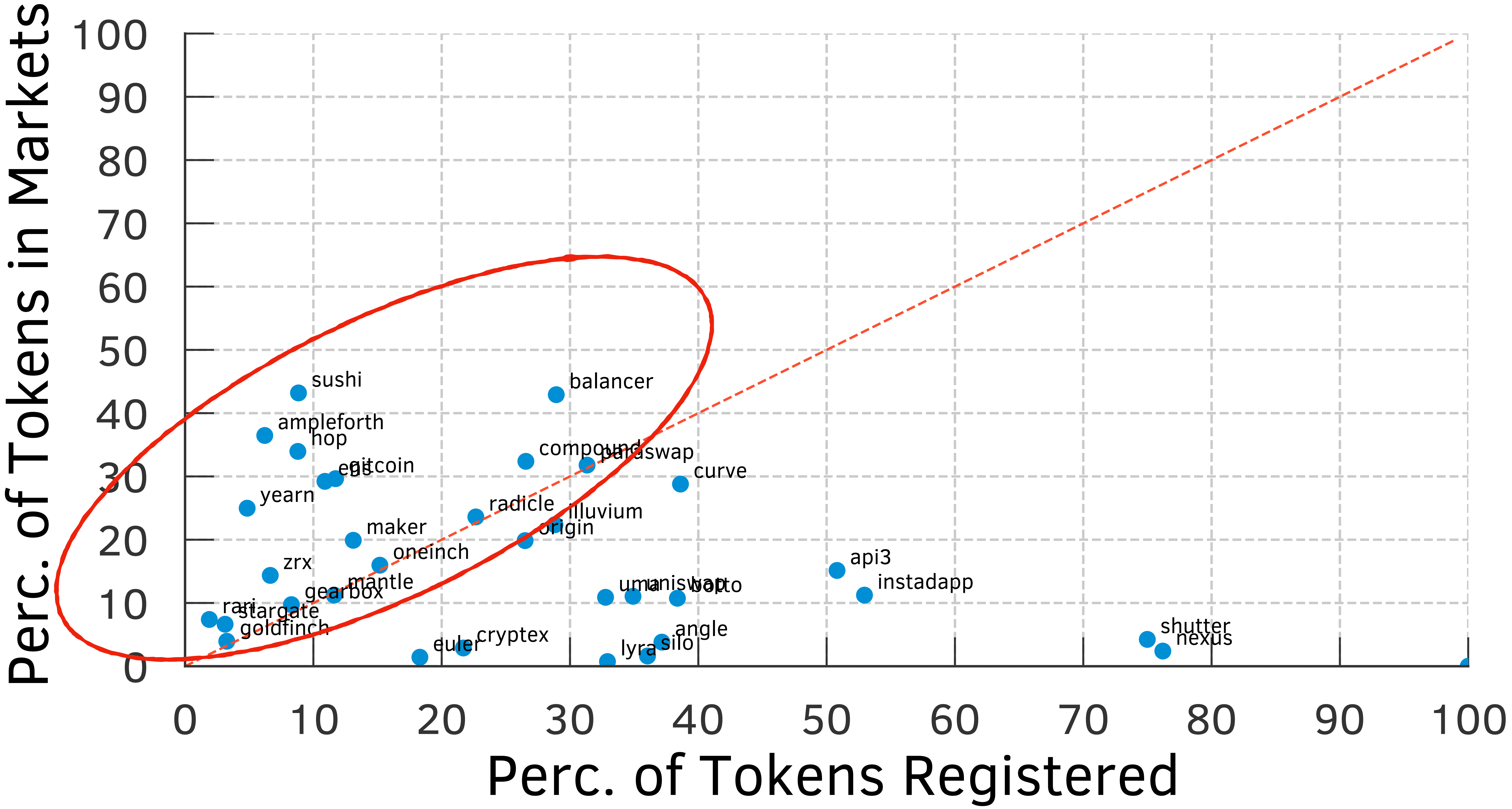
Public Markets

- For **44%** of DAOs, there are more tokens in Markets than are registered to vote



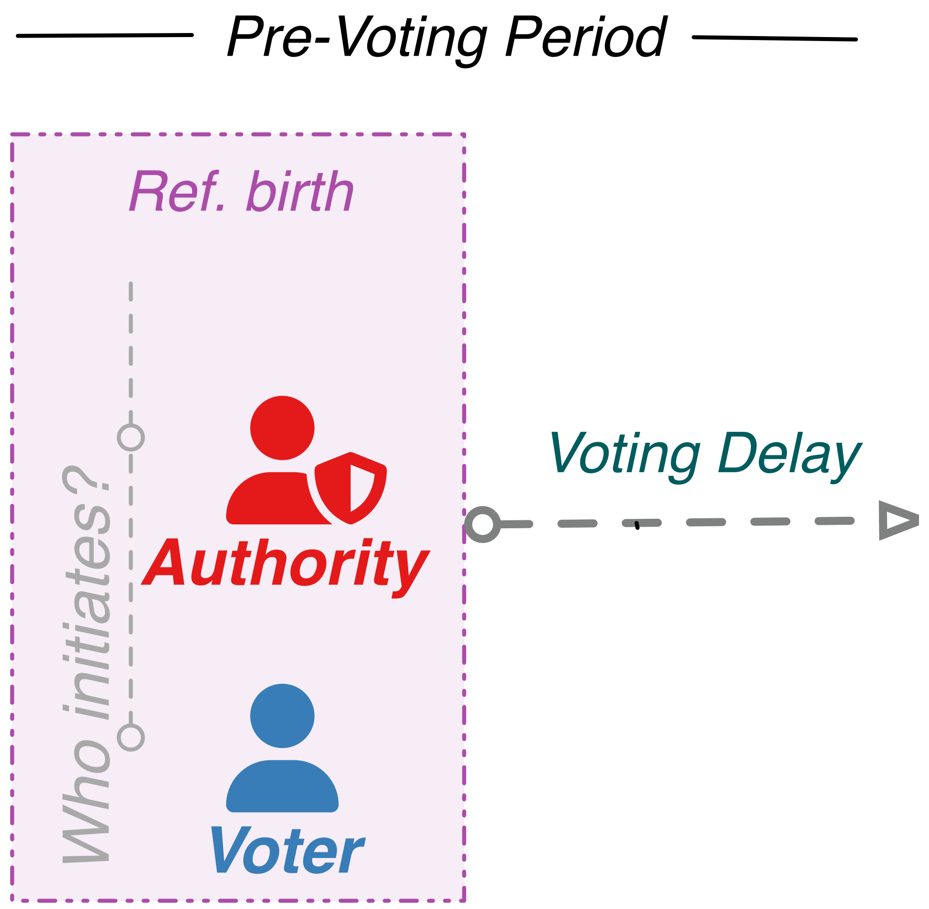
Public Markets

- For **44%** of DAOs, there are more tokens in Markets than are registered to vote

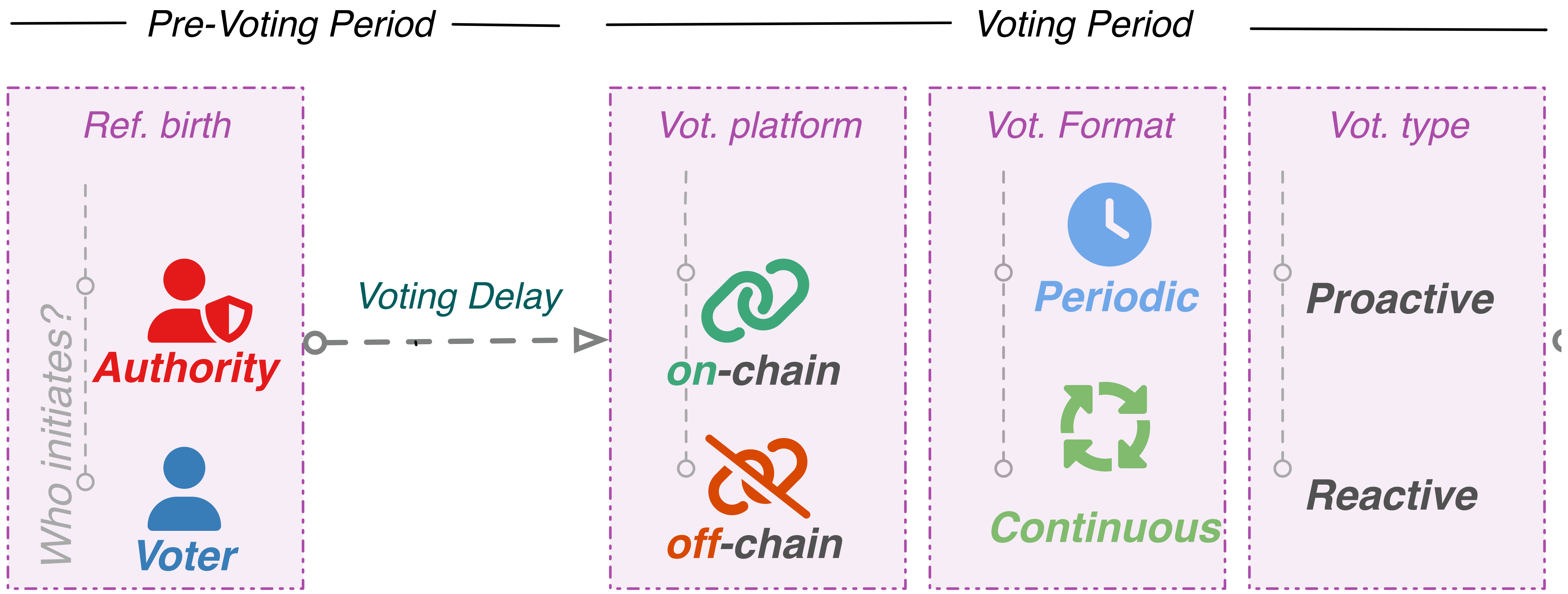


How is governance power exercised?

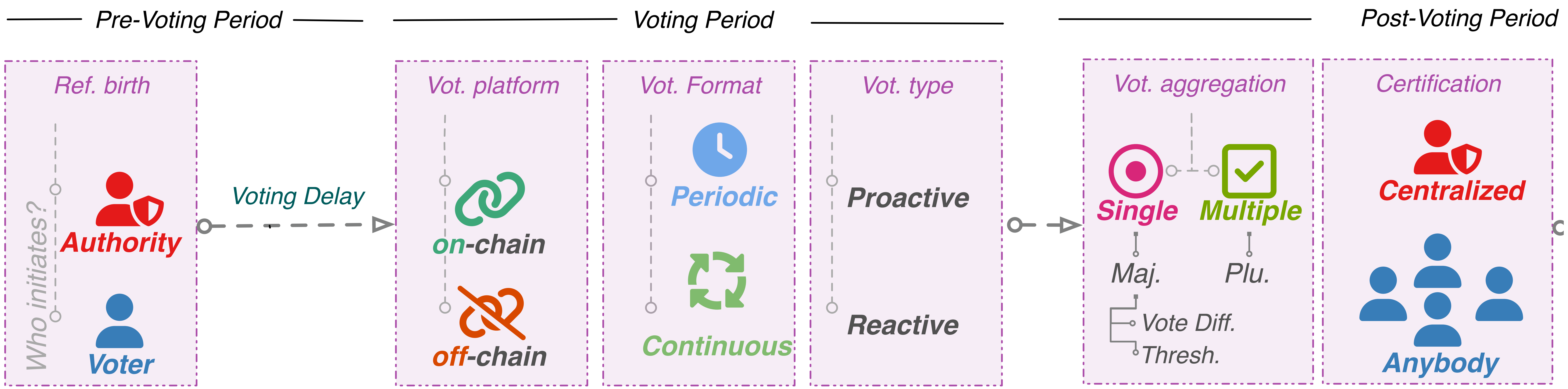
Lifecycle of a proposal



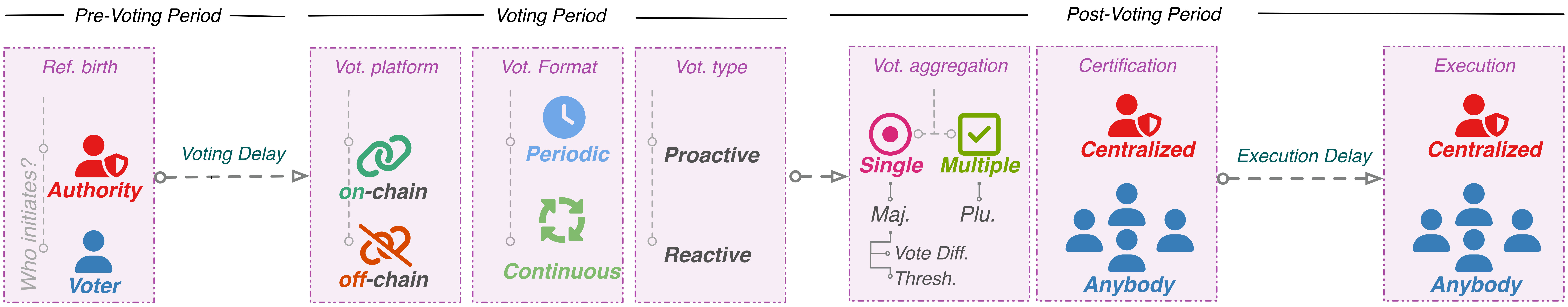
Lifecycle of a proposal



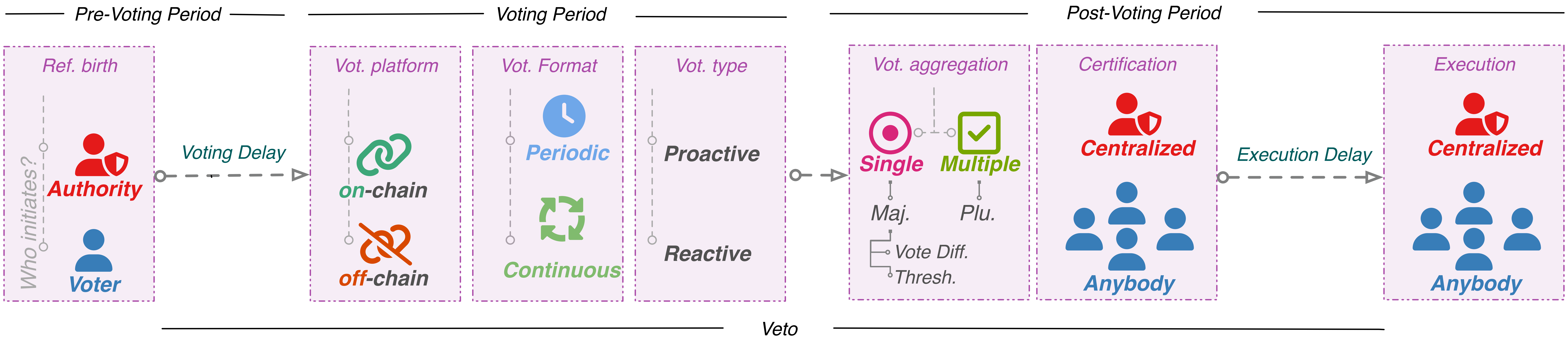
Lifecycle of a proposal



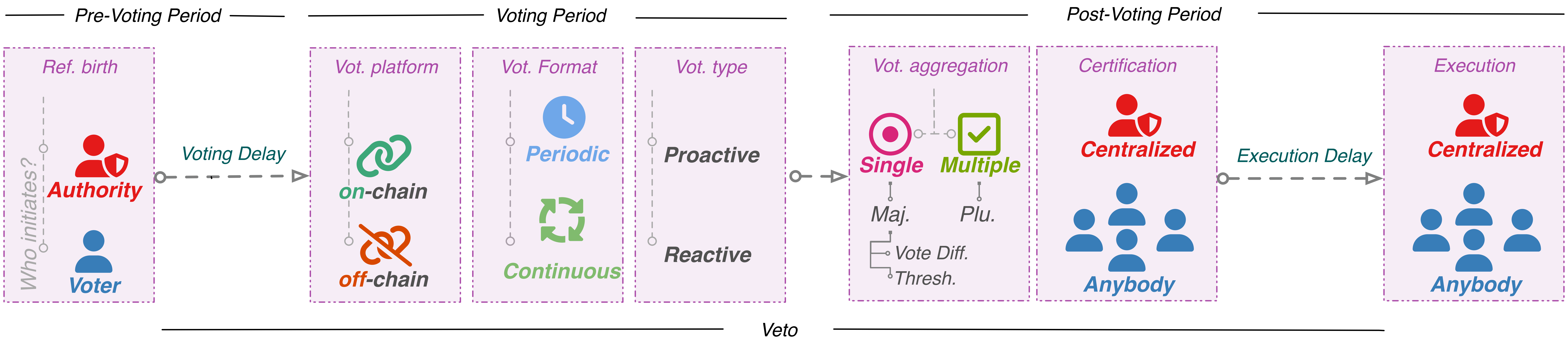
Lifecycle of a proposal



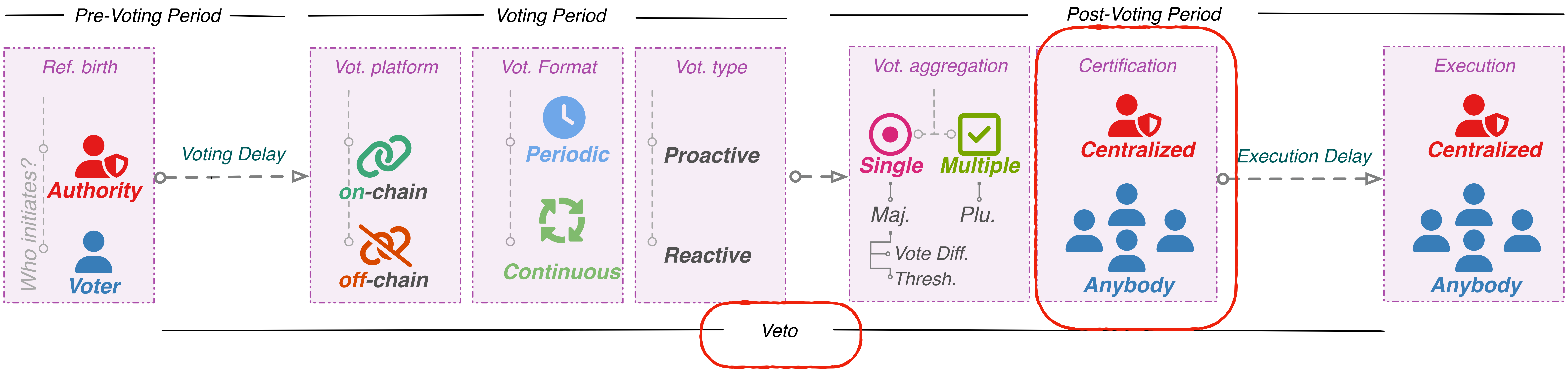
Lifecycle of a proposal



Lifecycle of a proposal

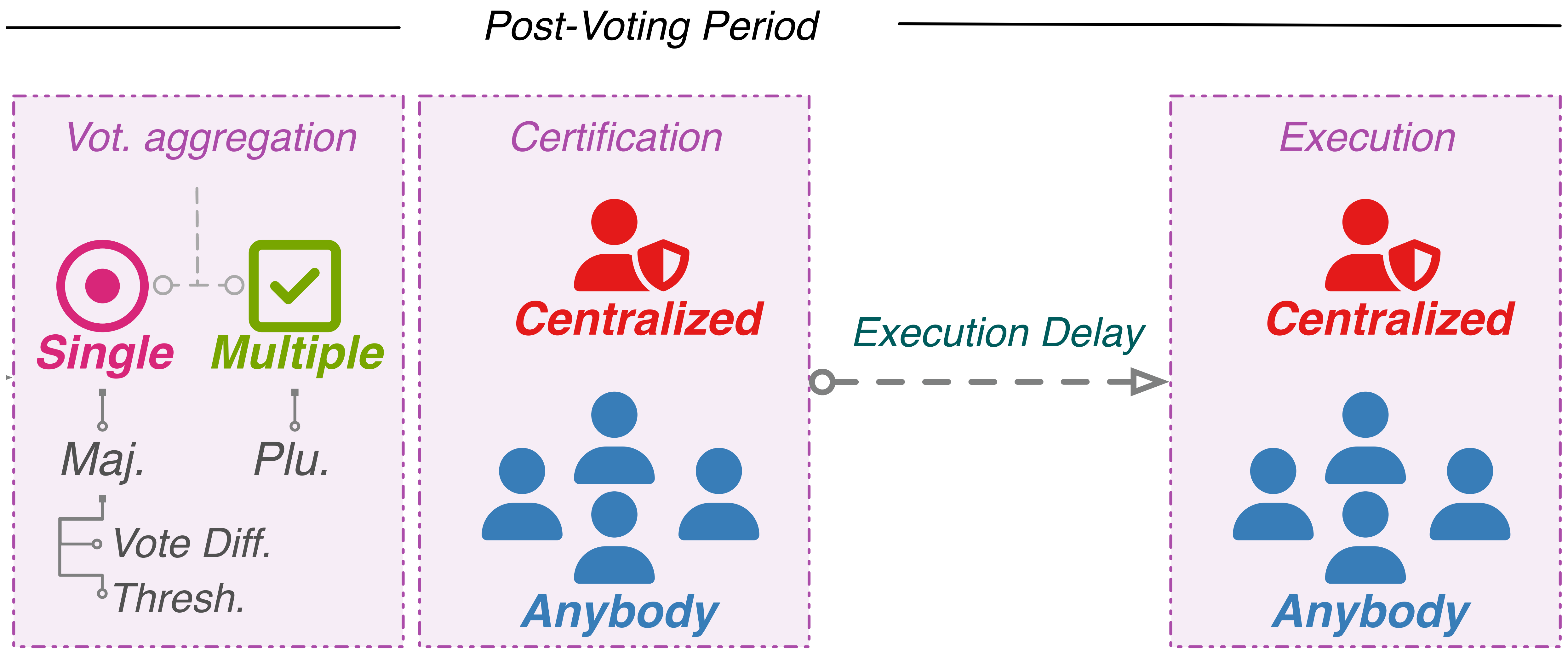


Lifecycle of a proposal



Post-Voting Period

- Voting Aggregation
- **Certification**
- Execution

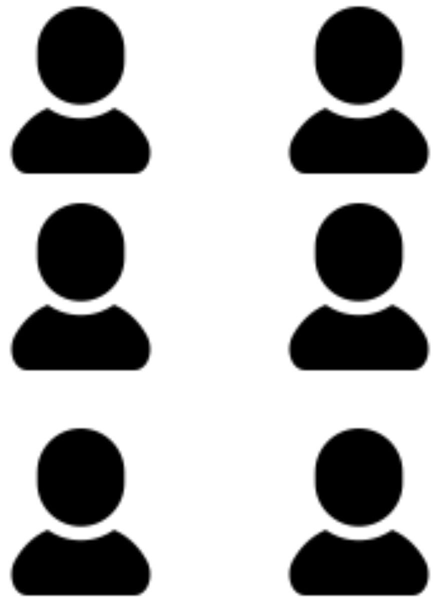


Post-Voting Period

- **Certification**
  - **Decentralized**
    - Generally for DAOs with on-chain voting

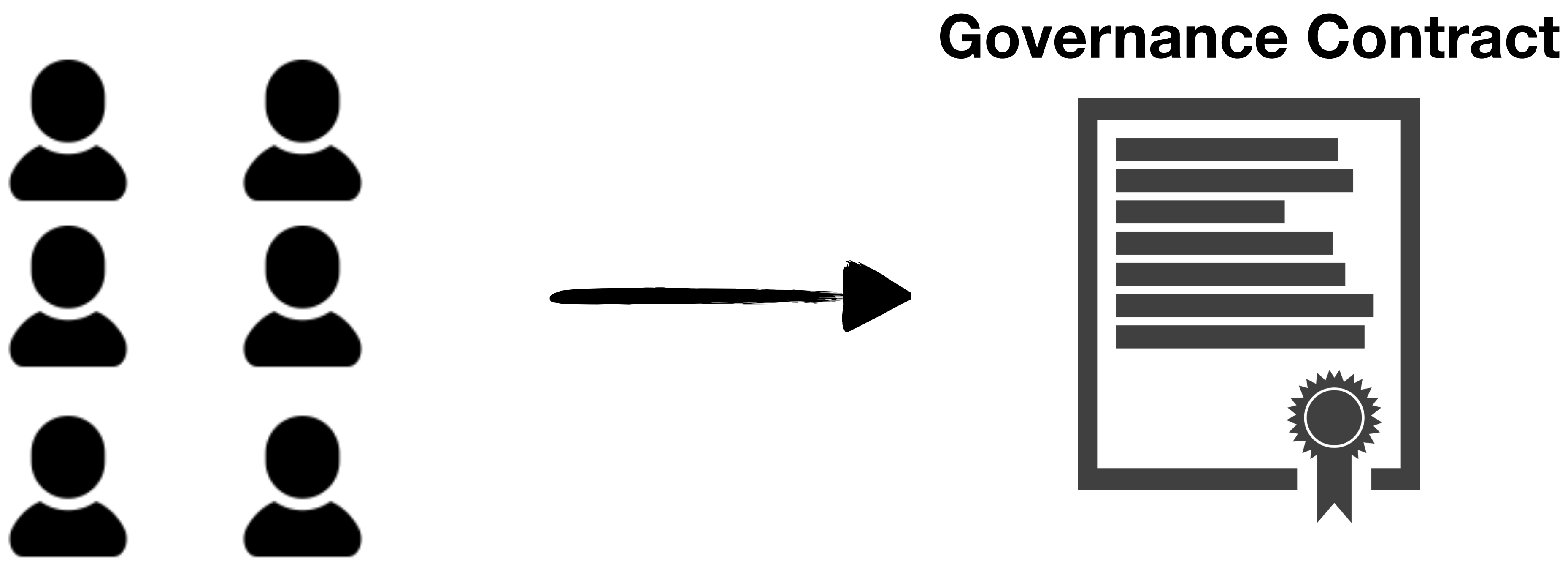
Post-Voting Period

- **Certification**
    - **Decentralized**
        - Generally for DAOs with on-chain voting



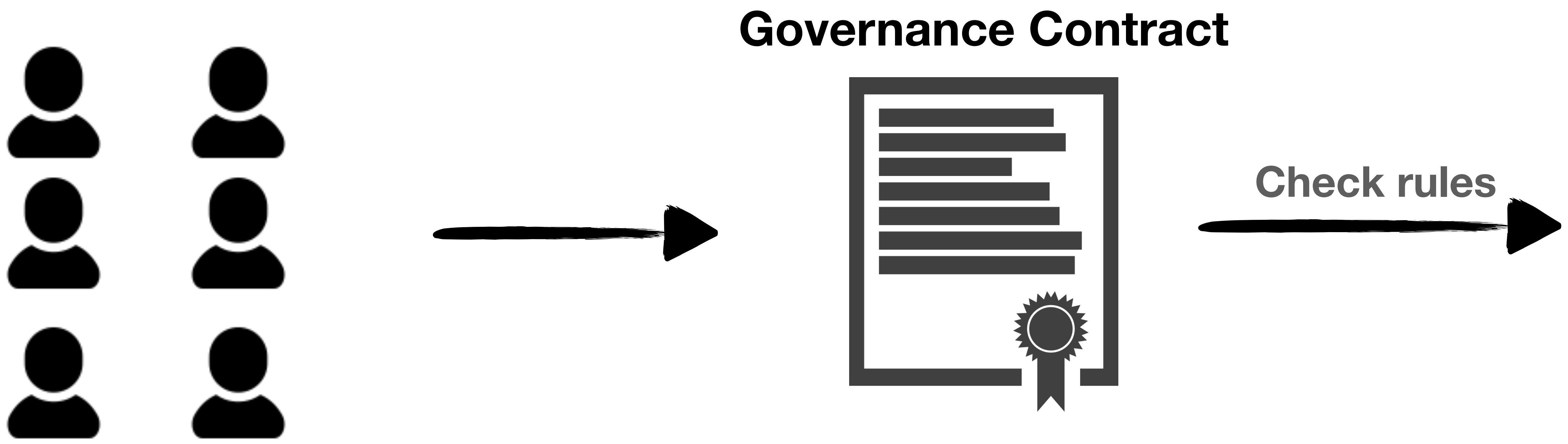
Post-Voting Period

- **Certification**
  - **Decentralized**
    - Generally for DAOs with on-chain voting



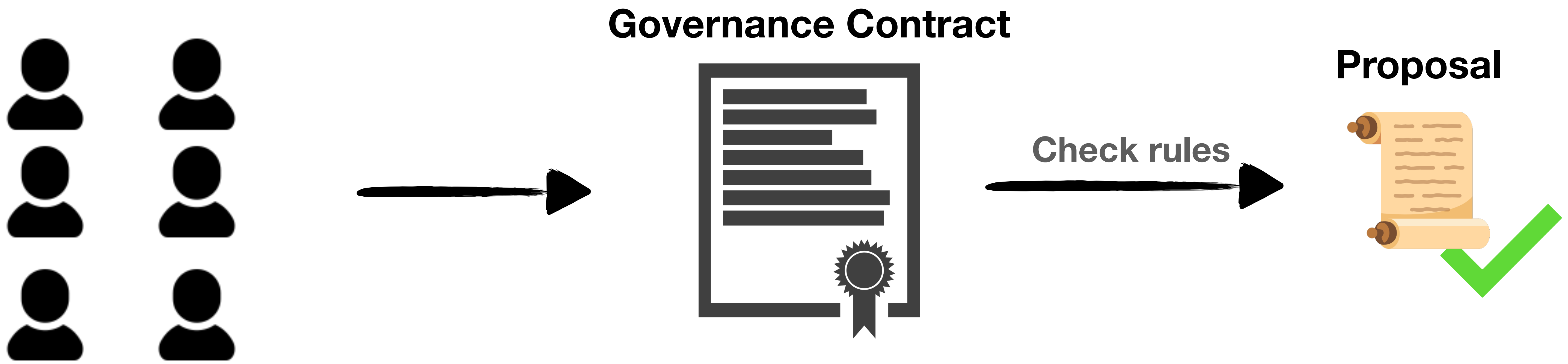
Post-Voting Period

- **Certification**
    - **Decentralized**
        - Generally for DAOs with on-chain voting



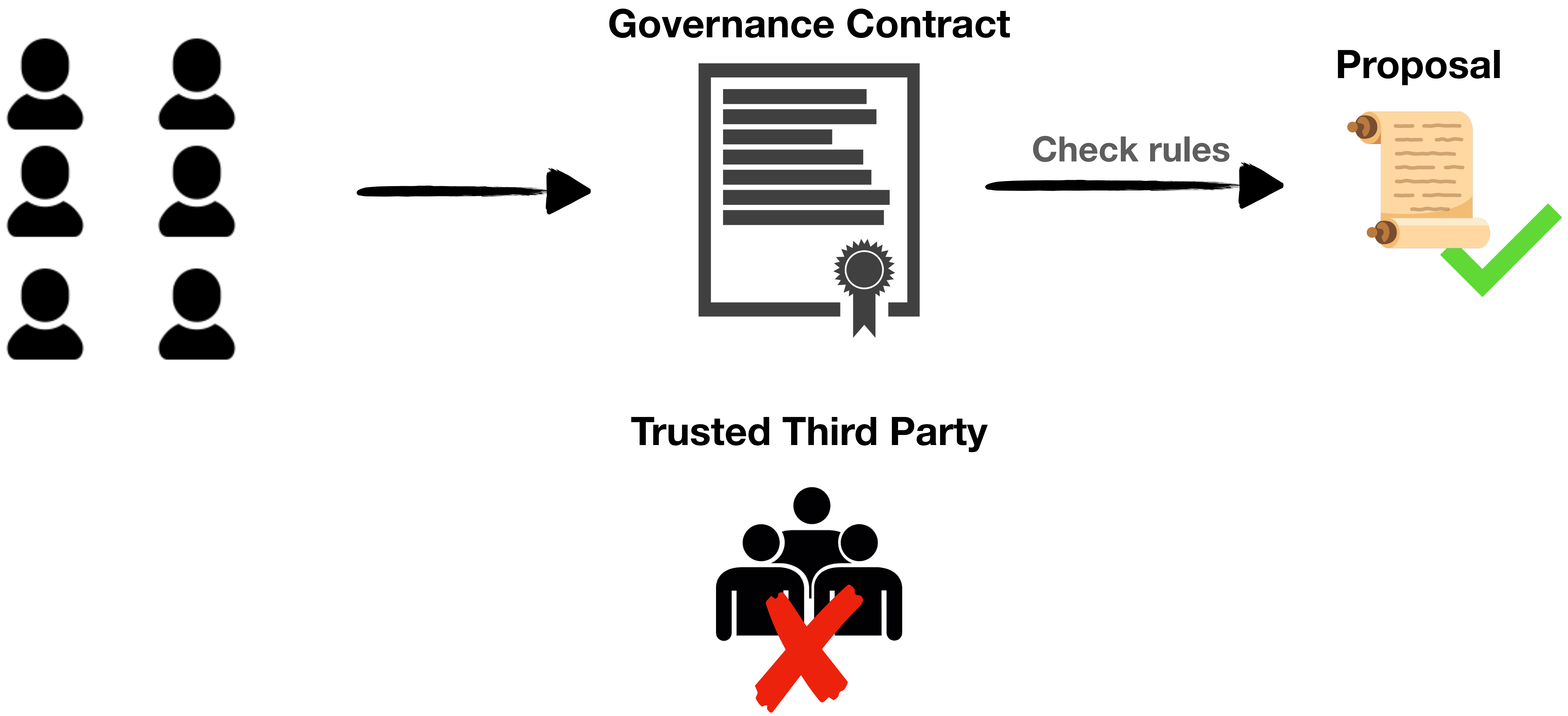
Post-Voting Period

- **Certification**
  - **Decentralized**
    - Generally for DAOs with on-chain voting



Post-Voting Period

- **Certification**
  - **Decentralized**
    - Generally for DAOs with on-chain voting



Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting, but also Layer 2s

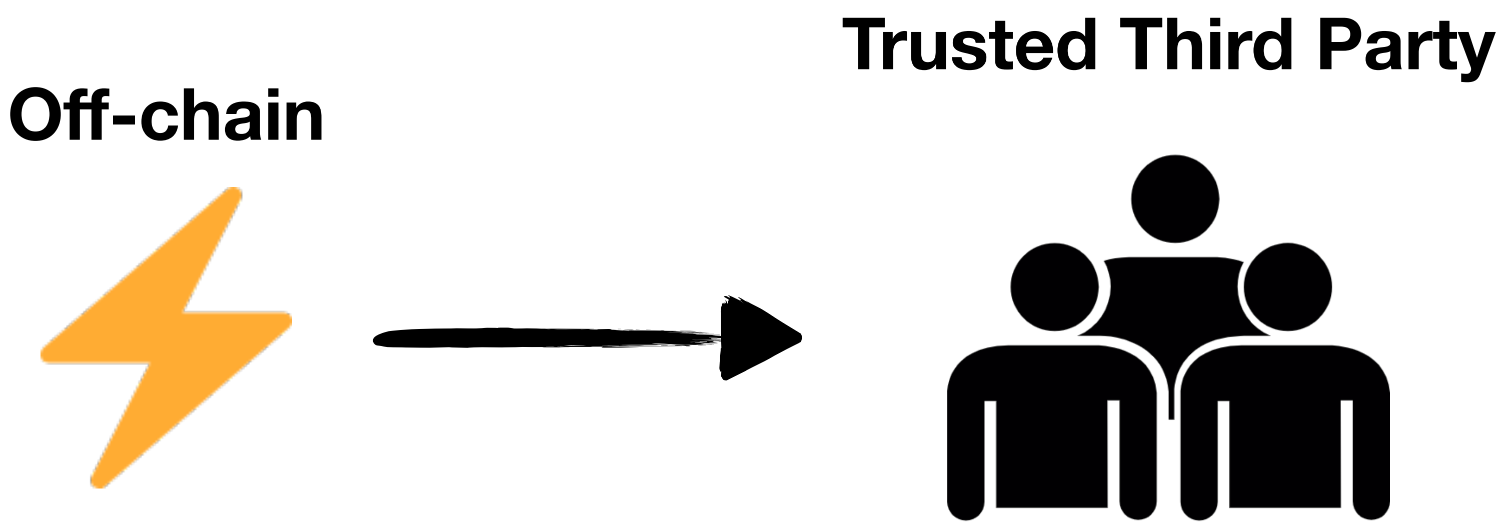
Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting, but also Layer 2s

Trusted Third Party

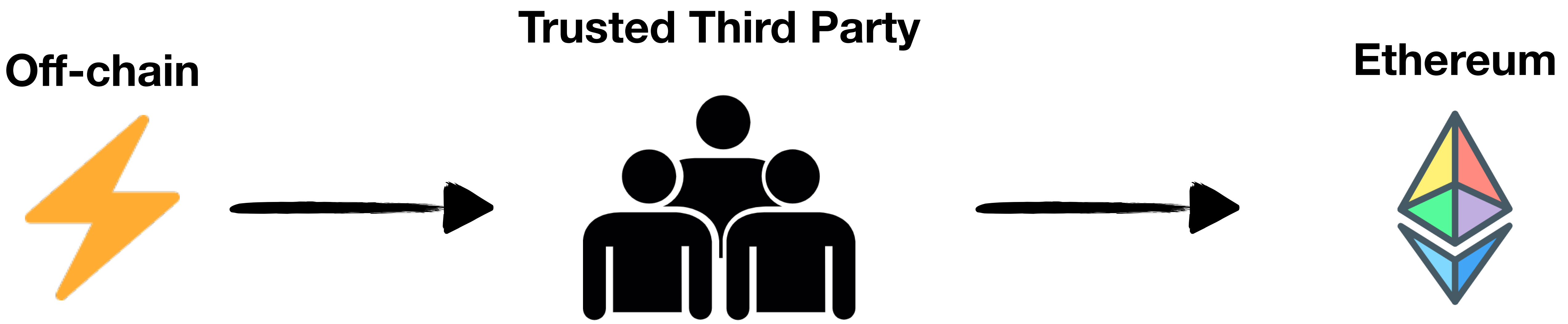
Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting, but also Layer 2s



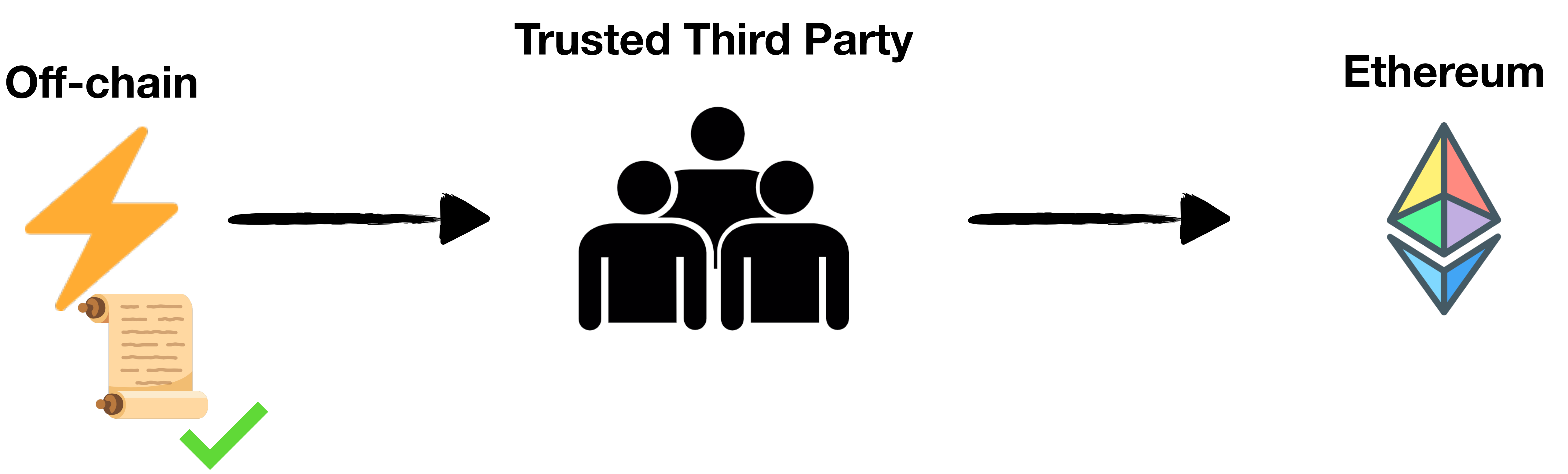
Post-Voting Period

- **Certification**
    - **Centralised**
        - Generally for DAOs with off-chain voting, but also Layer 2s



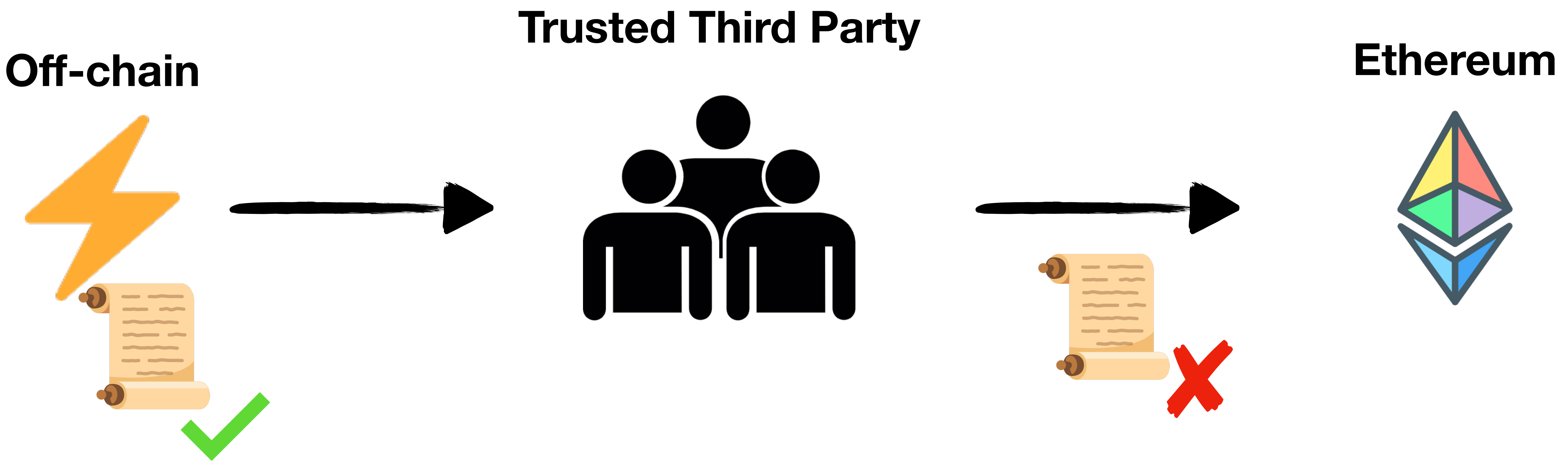
Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting, but also Layer 2s



Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting, but also Layer 2s

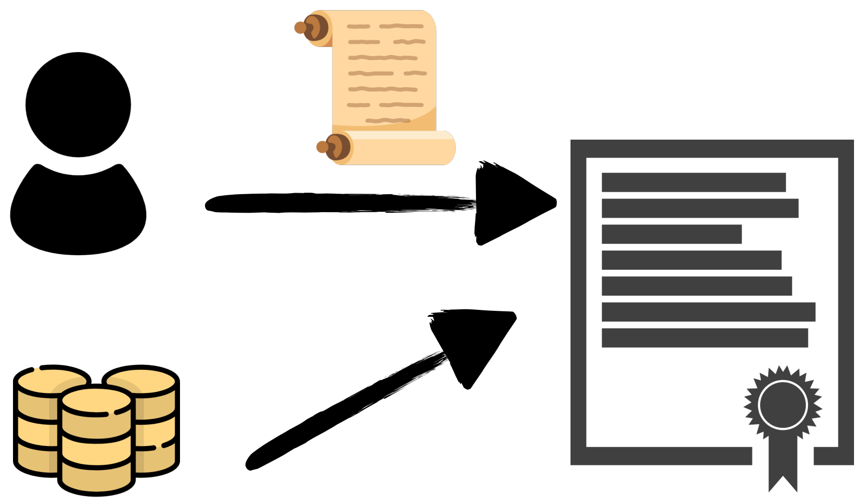


Post-Voting Period

- **Certification**
  - **Optimistic Certification**: Allow anybody to certify a proposal by putting down some collateral (money)

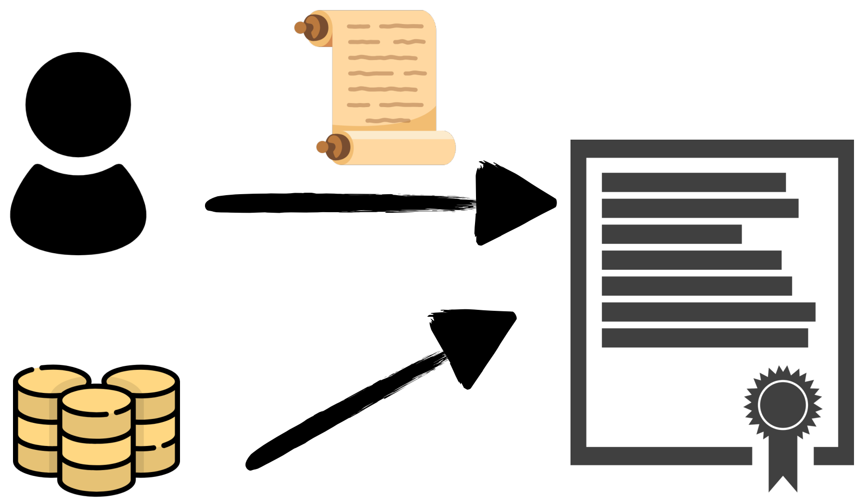
Post-Voting Period

- **Certification**
  - **Optimistic Certification**: Allow anybody to certify a proposal by putting down some collateral (money)



Post-Voting Period

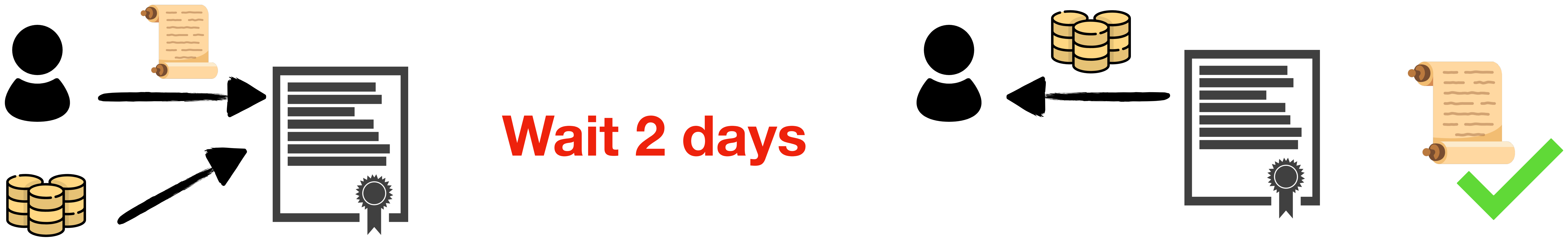
- **Certification**
  - **Optimistic Certification**: Allow anybody to certify a proposal by putting down some collateral (money)



Wait 2 days

Post-Voting Period

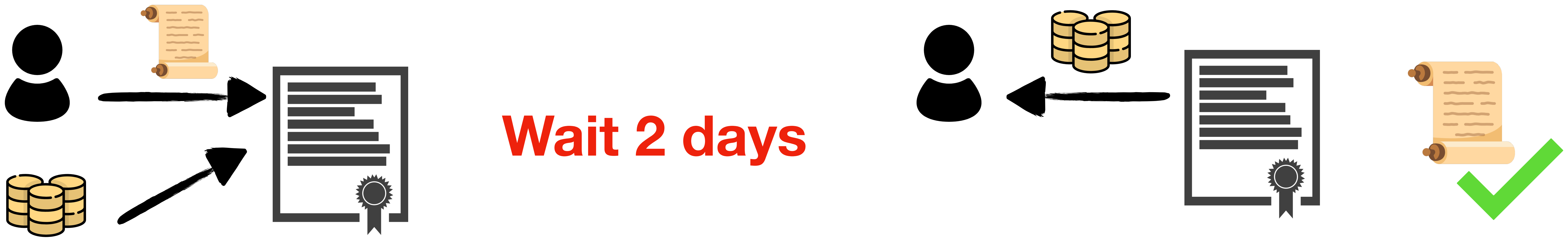
- **Certification**
  - **Optimistic Certification**: Allow anybody to certify a proposal by putting down some collateral (money)



Wait 2 days

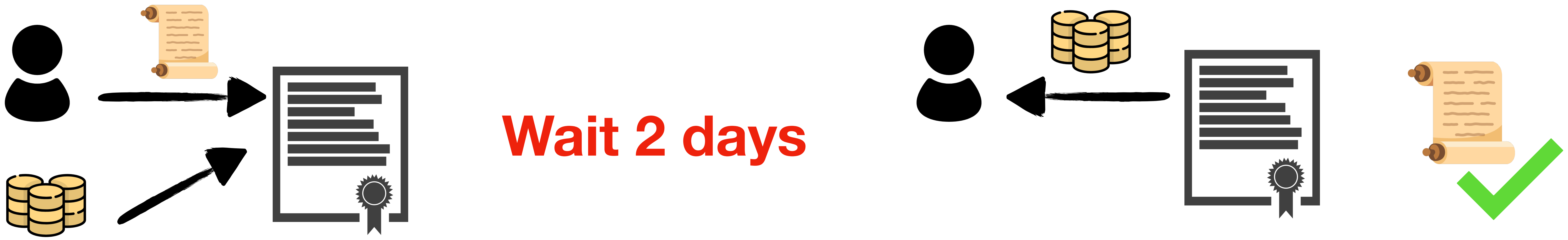
Post-Voting Period

- **Certification**
  - **Optimistic Certification:** Allow anybody to certify a proposal by putting down some collateral (money)

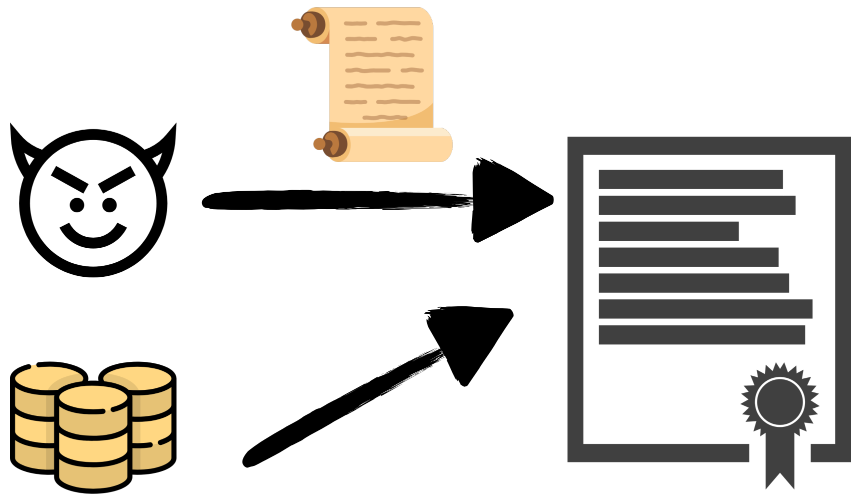


Post-Voting Period

- **Certification**
  - **Optimistic Certification:** Allow anybody to certify a proposal by putting down some collateral (money)

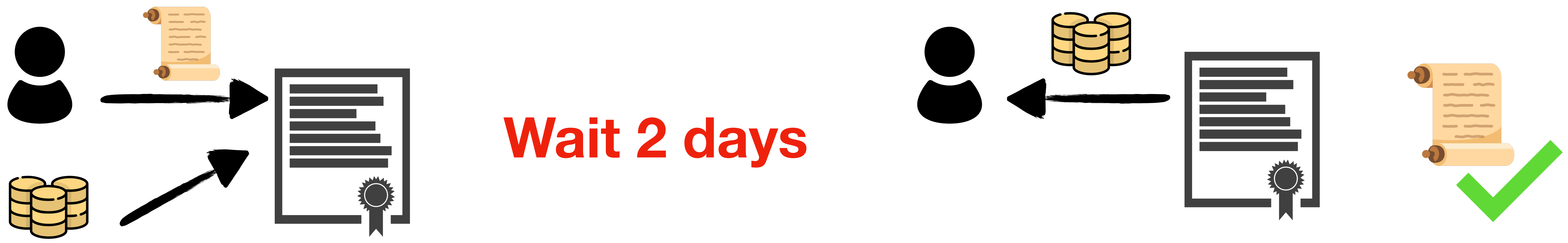


Proposal 1

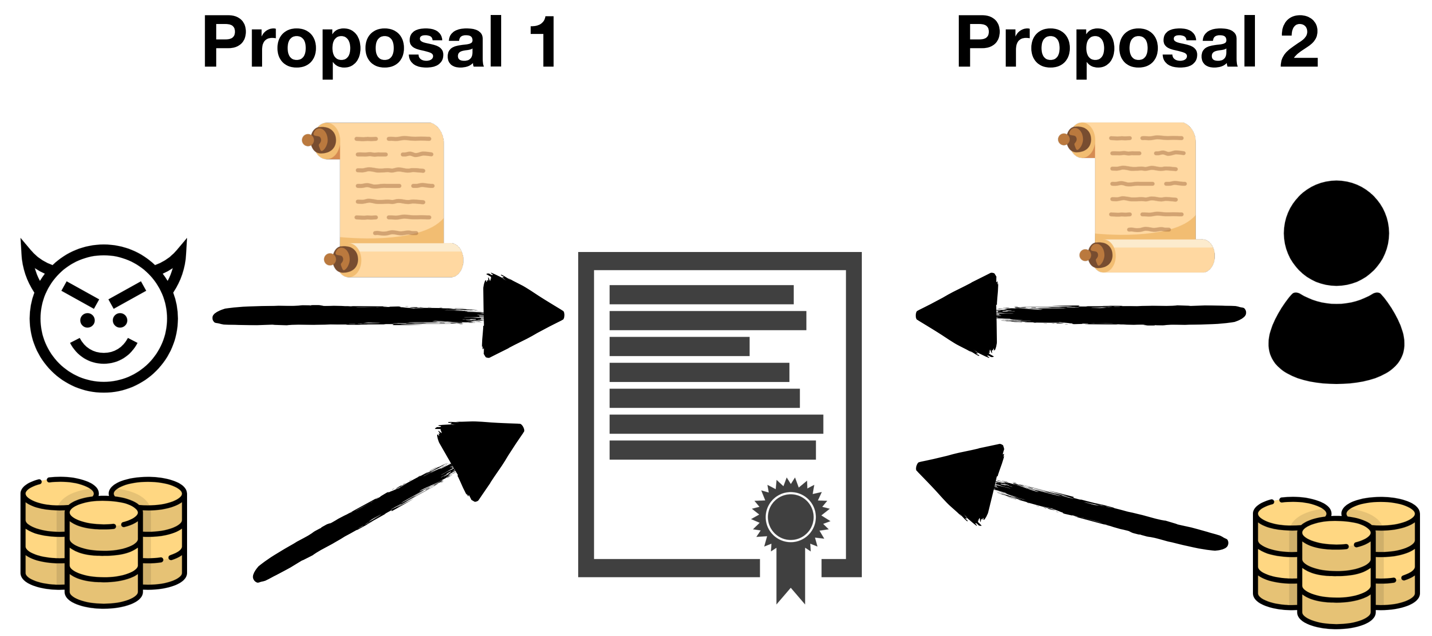


Post-Voting Period

- **Certification**
  - **Optimistic Certification:** Allow anybody to certify a proposal by putting down some collateral (money)

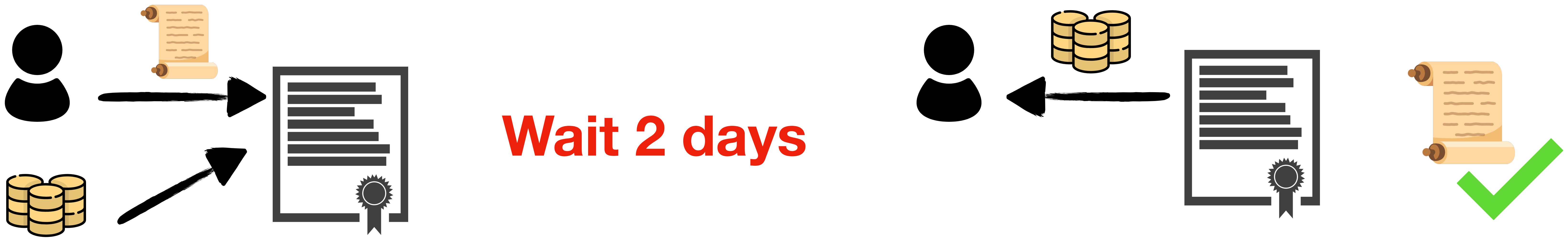


Wait 2 days

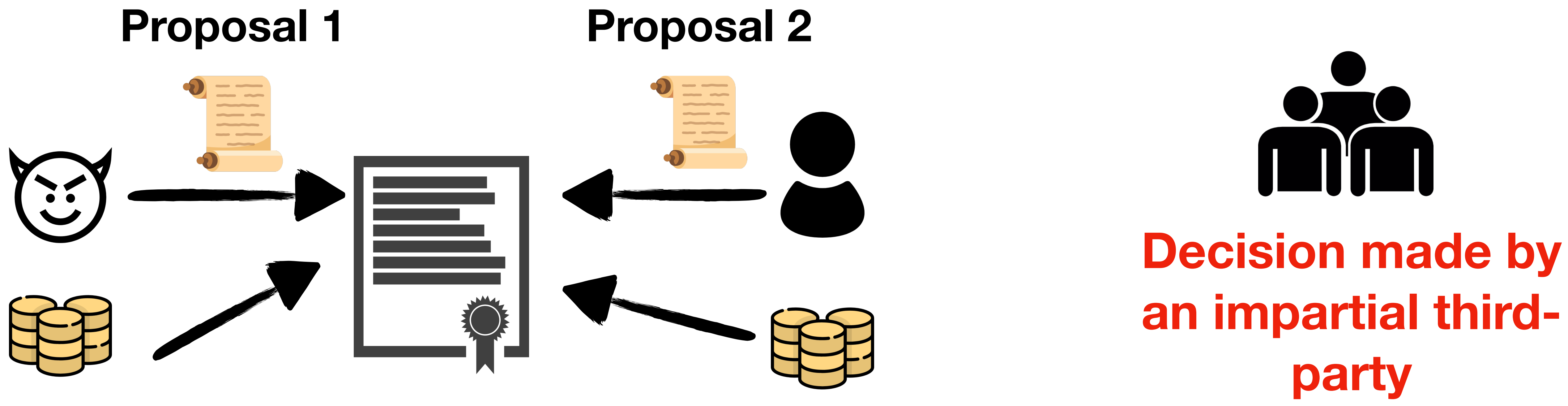


Post-Voting Period

- **Certification**
  - **Optimistic Certification**: Allow anybody to certify a proposal by putting down some collateral (money)



Wait 2 days



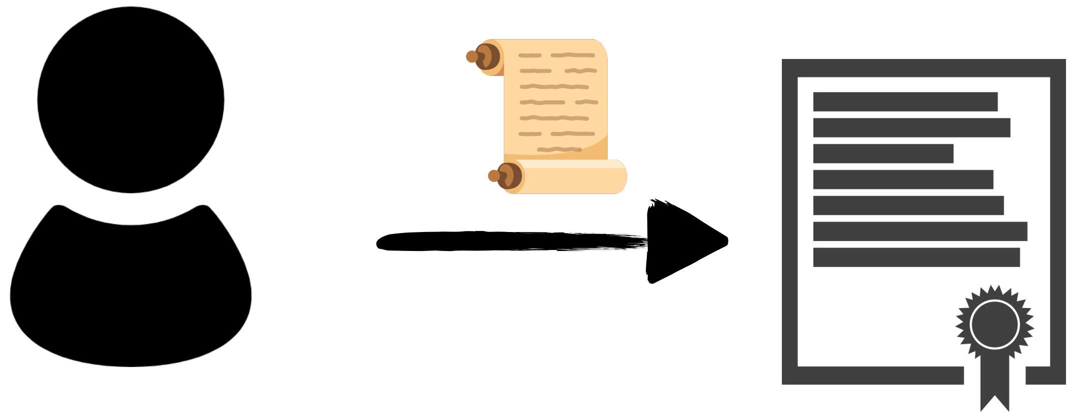
Proposal 1

Proposal 2

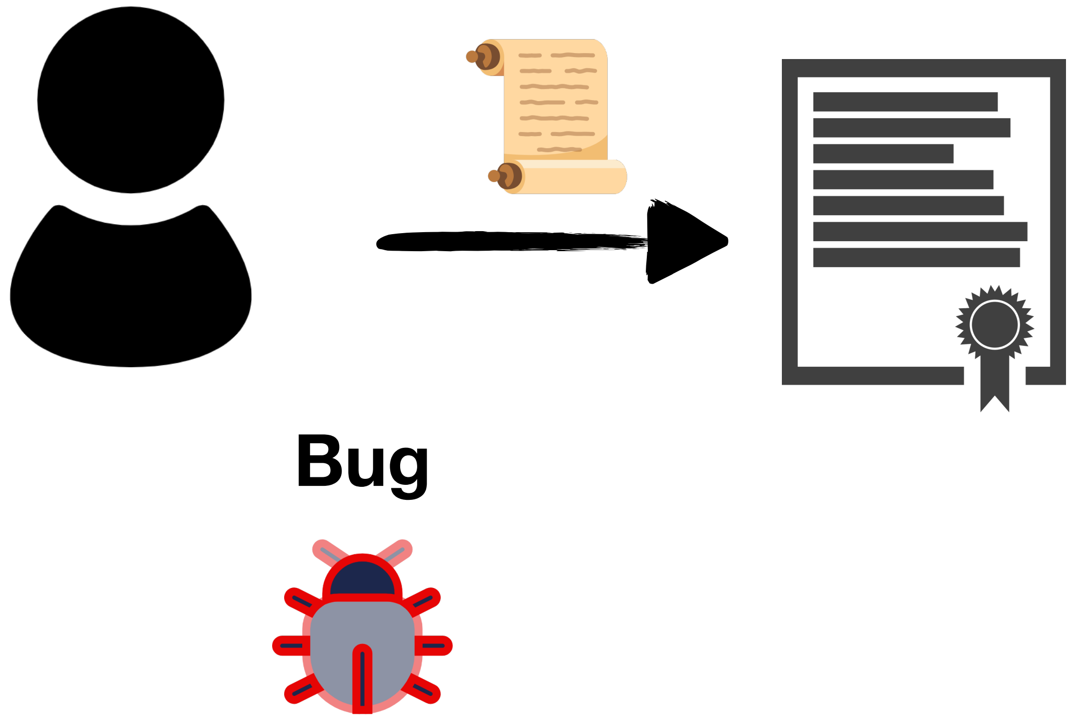
Decision made by an impartial third-party

Veto

Veto

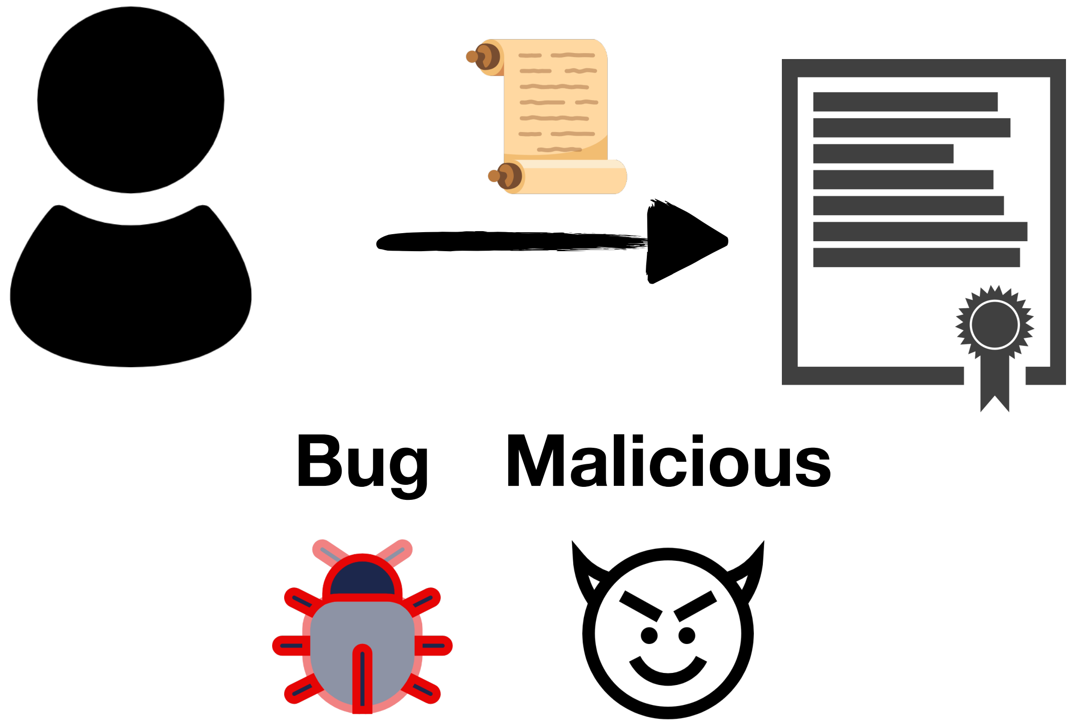


Veto

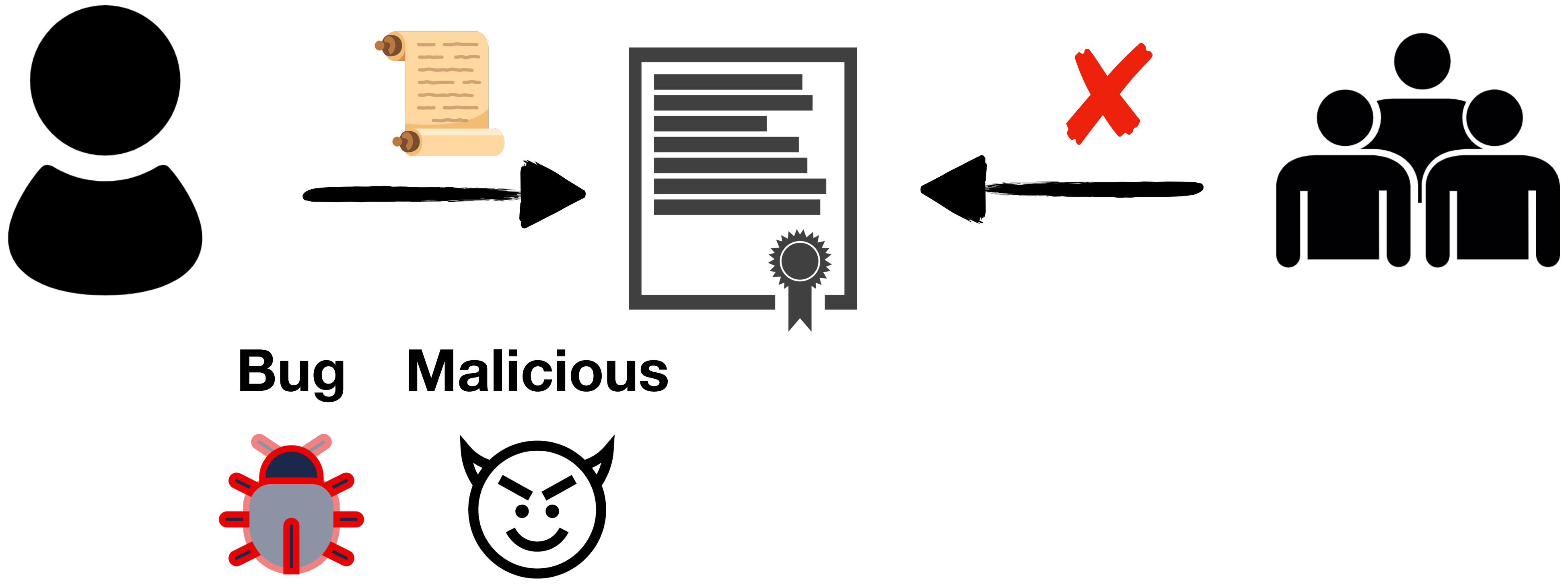


Bug

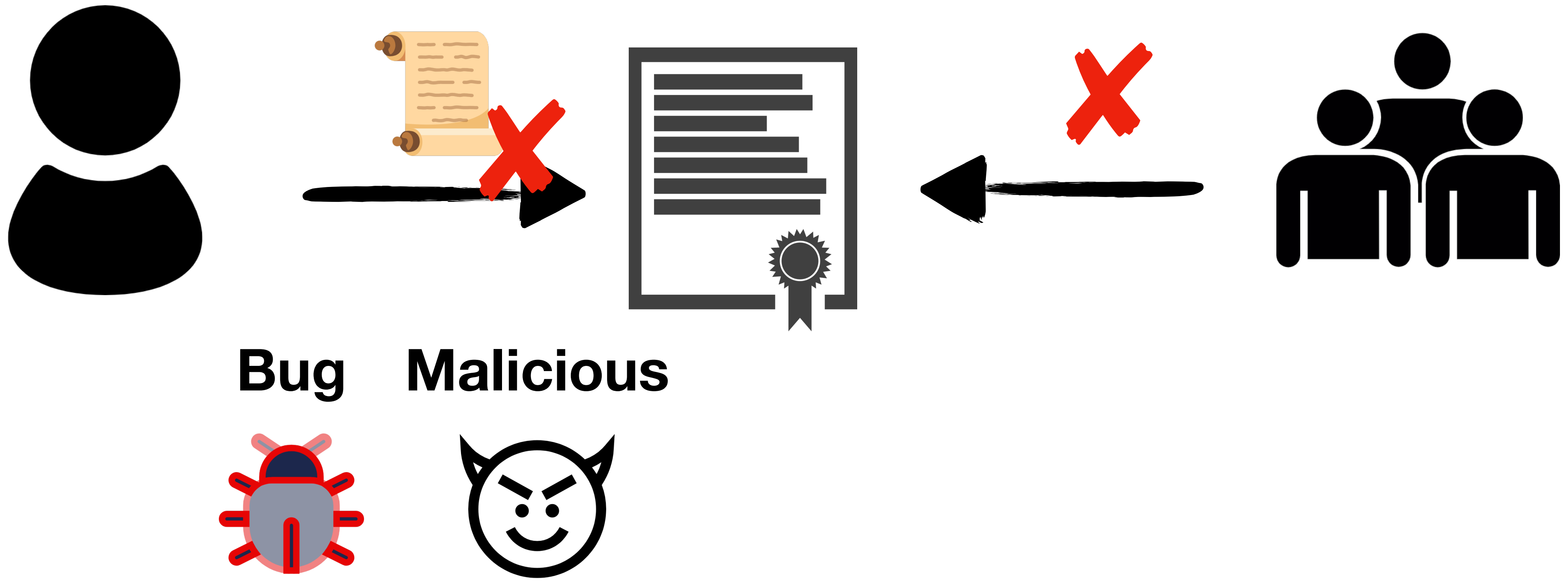
Veto



Veto

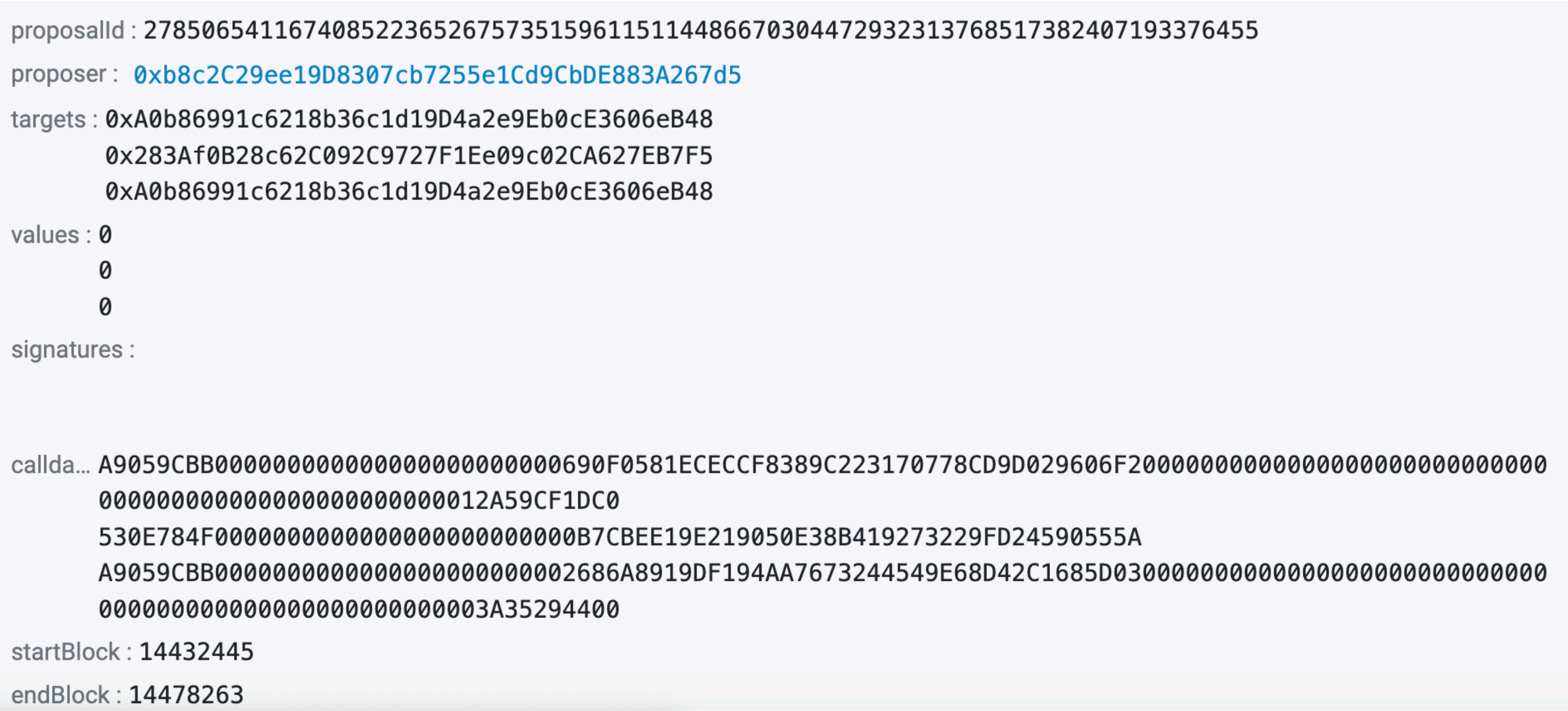


Veto



Veto

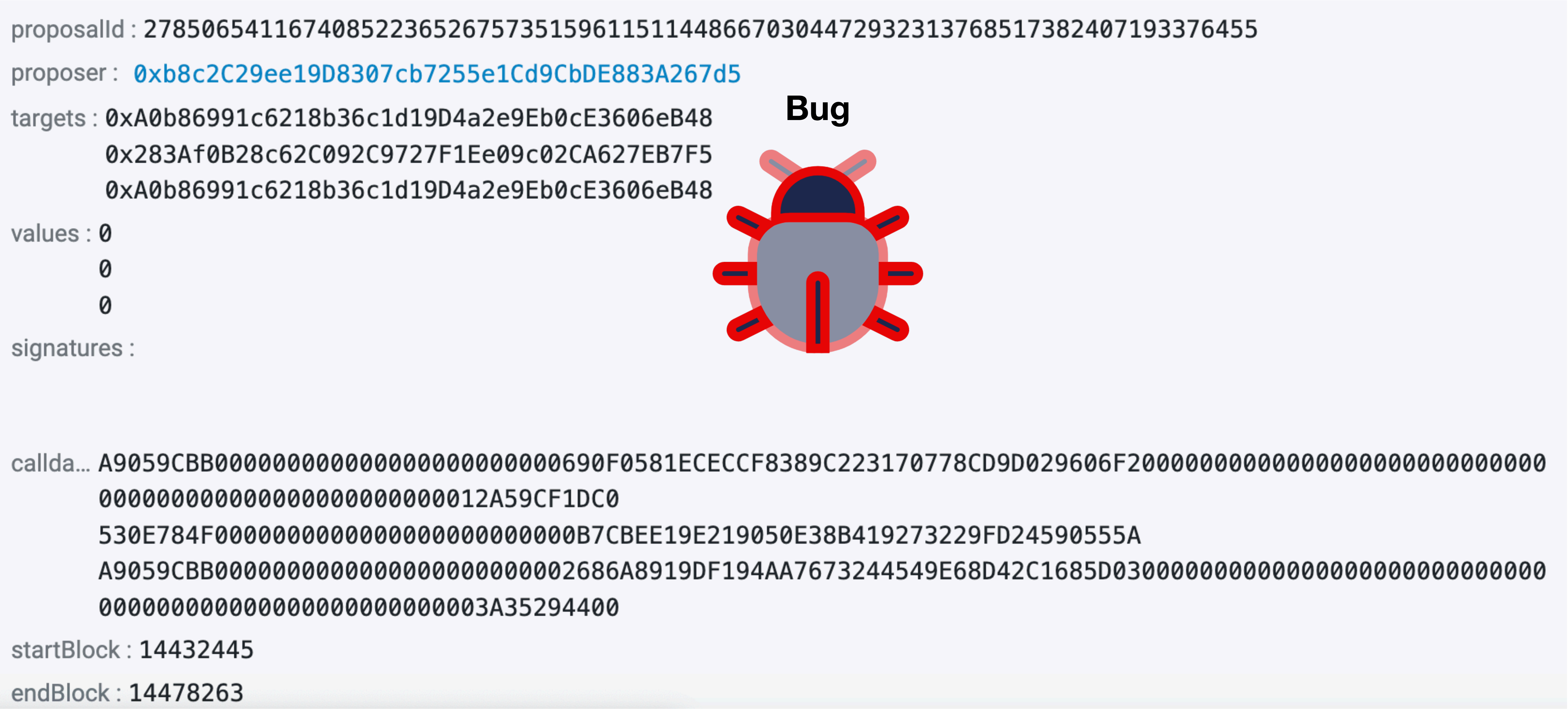
- **Veto is needed !!!**



```
proposalId : 27850654116740852236526757351596115114486670304472932313768517382407193376455
proposer :  0xb8c2C29ee19D8307cb7255e1Cd9CbDE883A267d5
targets : 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
          0x283Af0B28c62C092C9727F1Ee09c02CA627EB7F5
          0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
values : 0
         0
         0
signatures :


callda… A9059CBB000000000000000000000000690F0581ECECCF8389C223170778CD9D029606F20000000000000000000000000000
        000000000000000000000000012A59CF1DC0
        530E784F0000000000000000000000000B7CBEE19E219050E38B419273229FD24590555A
        A9059CBB0000000000000000000000002686A8919DF194AA7673244549E68D42C1685D030000000000000000000000000000
        000000000000000000000000003A35294400
startBlock : 14432445
endBlock : 14478263
```

Veto

- **Veto is needed !!!**



proposalId : 27850654116740852236526757351596115114486670304472932313768517382407193376455

proposer : 0xb8c2C29ee19D8307cb7255e1Cd9CbDE883A267d5

```
targets : 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
          0x283Af0B28c62C092C9727F1Ee09c02CA627EB7F5
          0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
values : 0
         0
         0
signatures :



callda... A9059CBB000000000000000000000000690F0581ECECCF8389C223170778CD9D029606F20000000000000000000000000000
          000000000000000000000000012A59CF1DC0
          530E784F0000000000000000000000000B7CBEE19E219050E38B419273229FD24590555A
          A9059CBB0000000000000000000000002686A8919DF194AA7673244549E68D42C1685D030000000000000000000000000000
          000000000000000000000000003A35294400
startBlock : 14432445
endBlock : 14478263
```

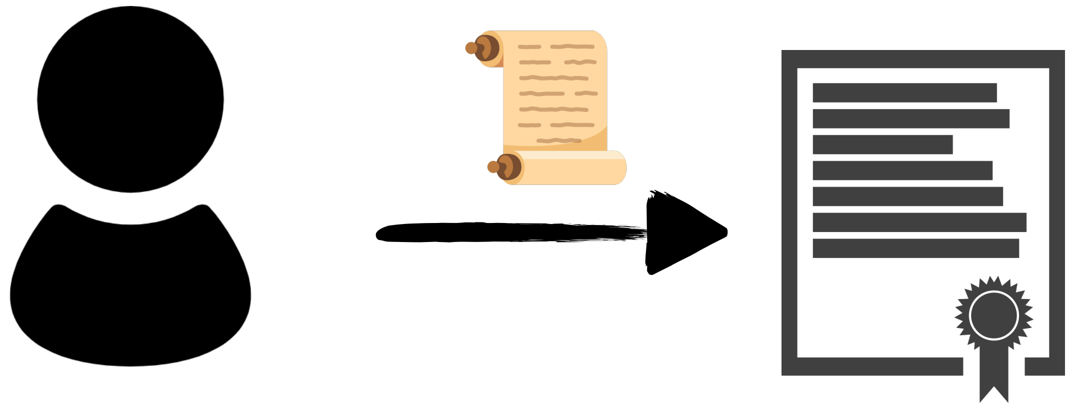
Bug

Veto

- **Vote Initiator**
  - The initiator of the vote can cancel the proposal

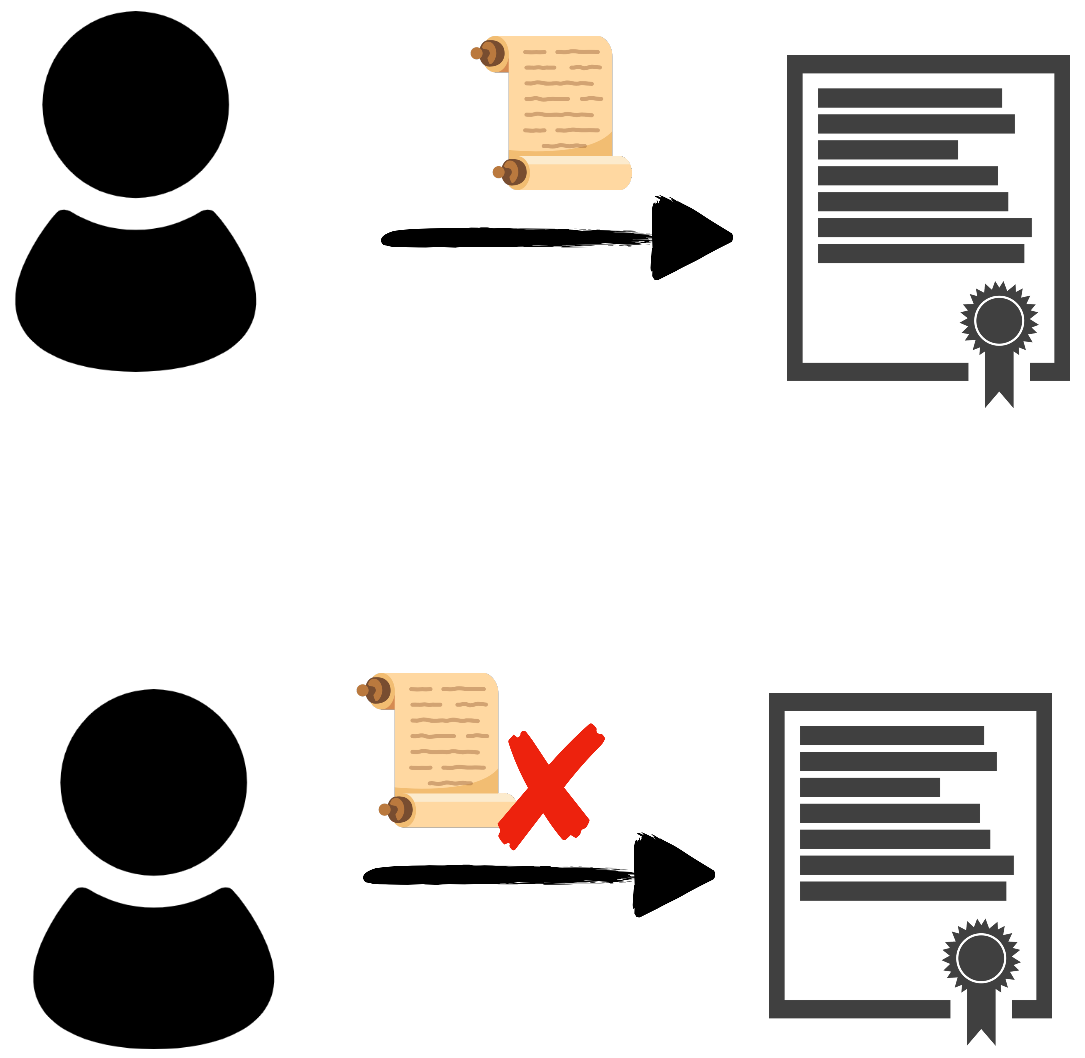
Veto

- **Vote Initiator**
  - The initiator of the vote can cancel the proposal



Veto

- **Vote Initiator**
    - The initiator of the vote can cancel the proposal

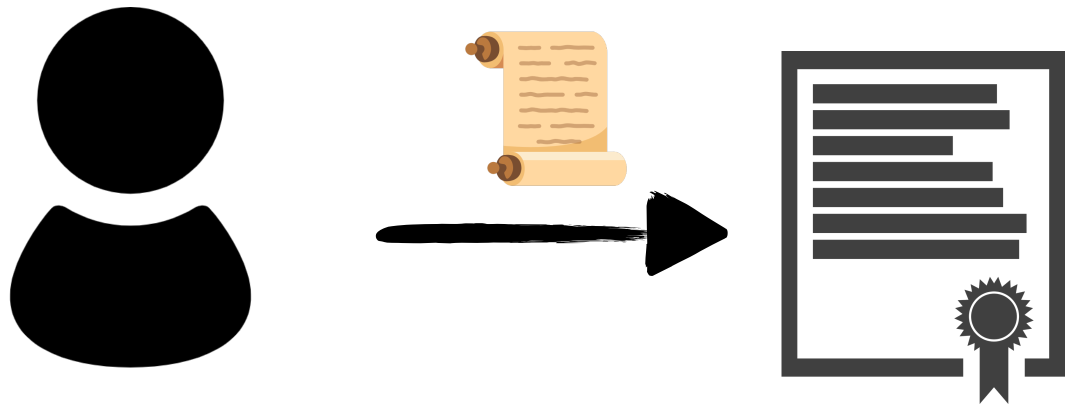


Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal

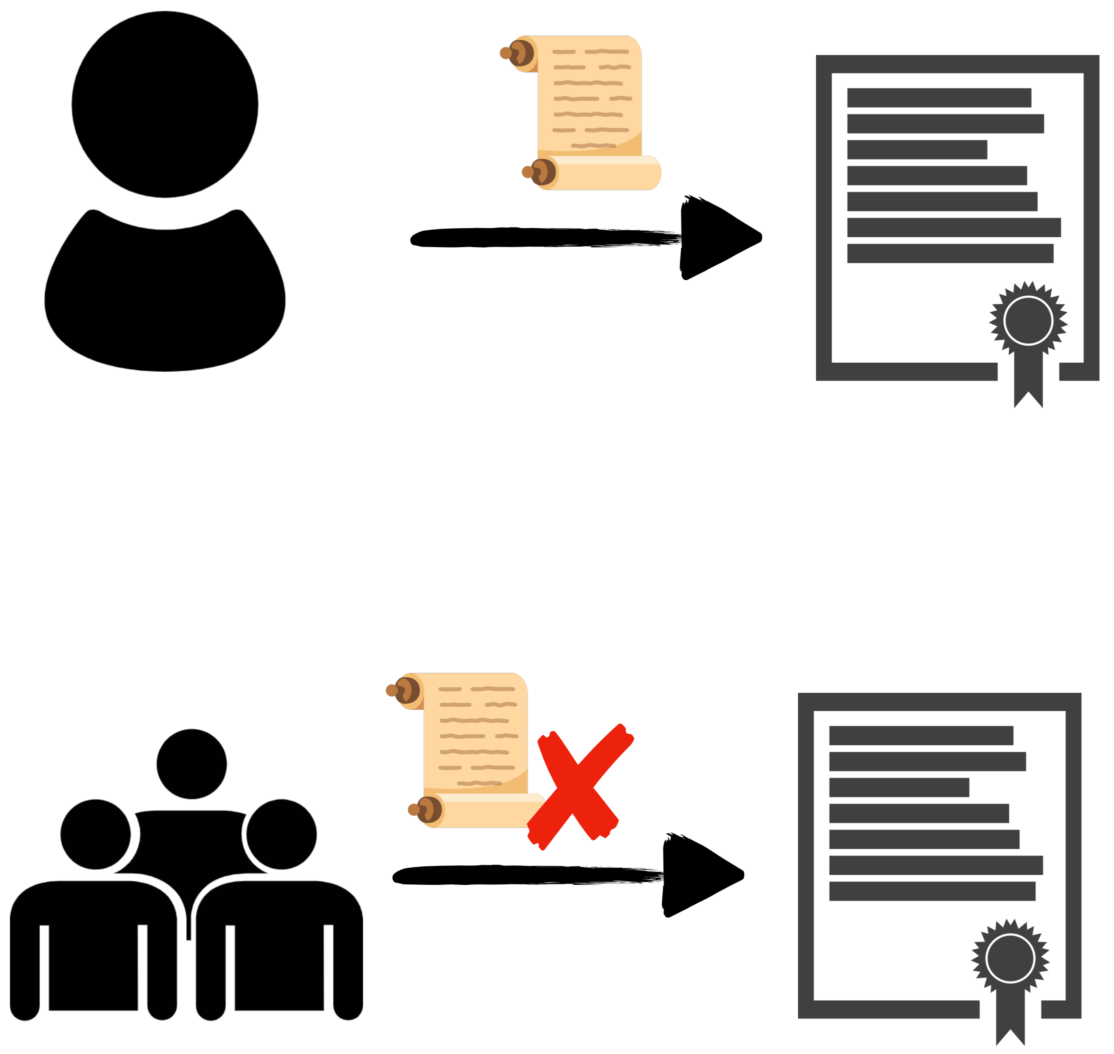
Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



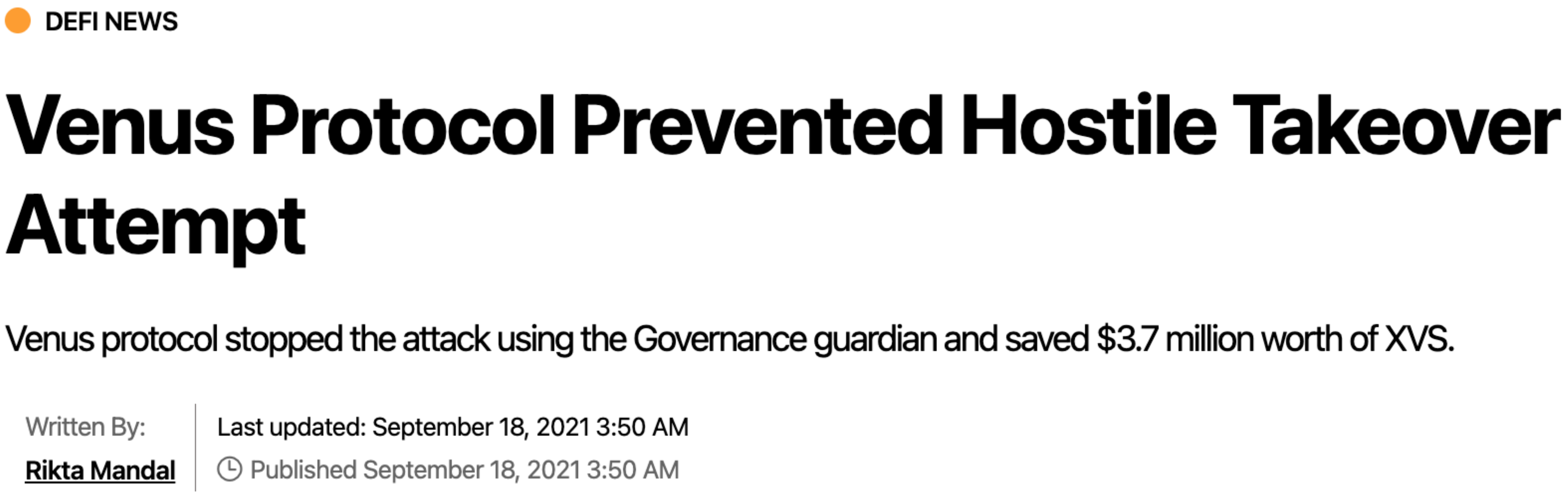
Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



● DEFI NEWS

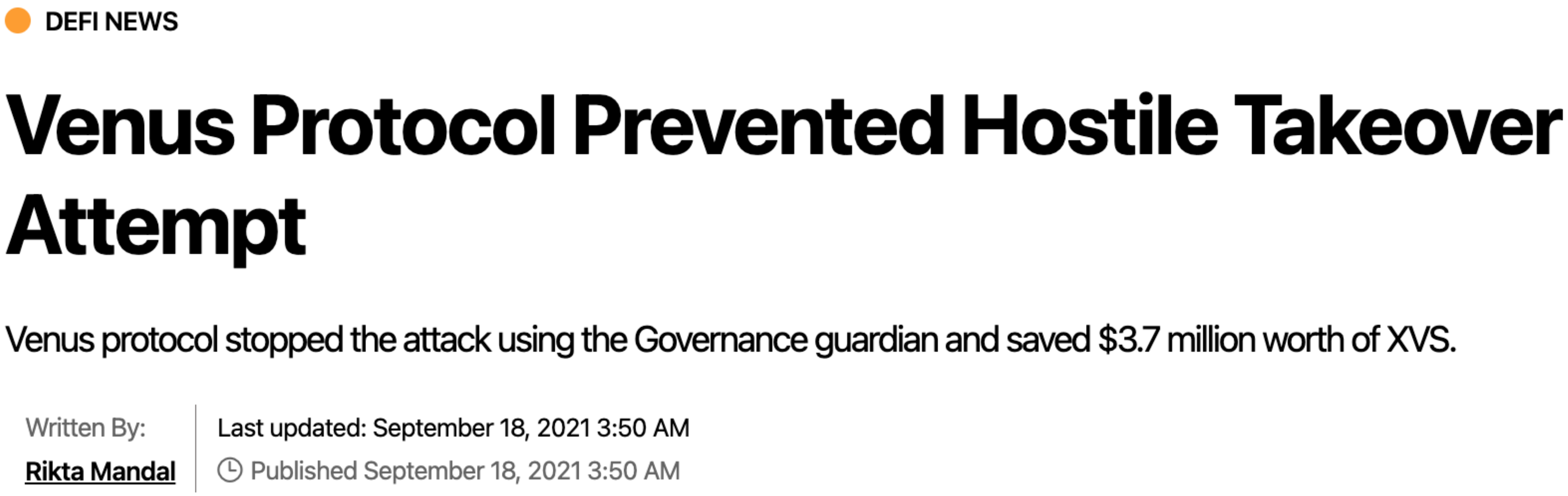
Venus Protocol Prevented Hostile Takeover Attempt

Venus protocol stopped the attack using the Governance guardian and saved $3.7 million worth of XVS.

Written By: Rikta Mandal | Last updated: September 18, 2021 3:50 AM
Published September 18, 2021 3:50 AM

Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



● DEFI NEWS

Venus Protocol Prevented Hostile Takeover Attempt

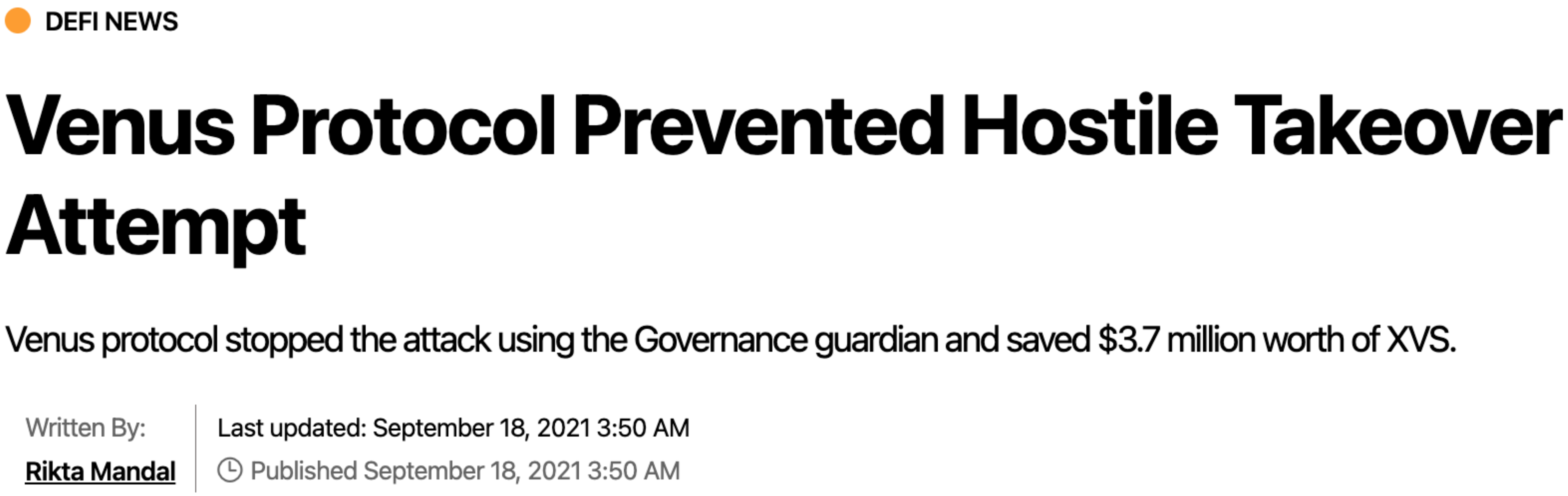
Venus protocol stopped the attack using the Governance guardian and saved $3.7 million worth of XVS.

Written By:
Rikta Mandal

Last updated: September 18, 2021 3:50 AM
Published September 18, 2021 3:50 AM

Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



● DEFI NEWS

Venus Protocol Prevented Hostile Takeover Attempt

Venus protocol stopped the attack using the Governance guardian and saved $3.7 million worth of XVS.

Written By: Rikta Mandal

Last updated: September 18, 2021 3:50 AM

Published September 18, 2021 3:50 AM

Compound Case Study

- We can characterise what can go wrong
- Real-attack on Compound protocol to take approx. **$25 million**

Compound Case Study

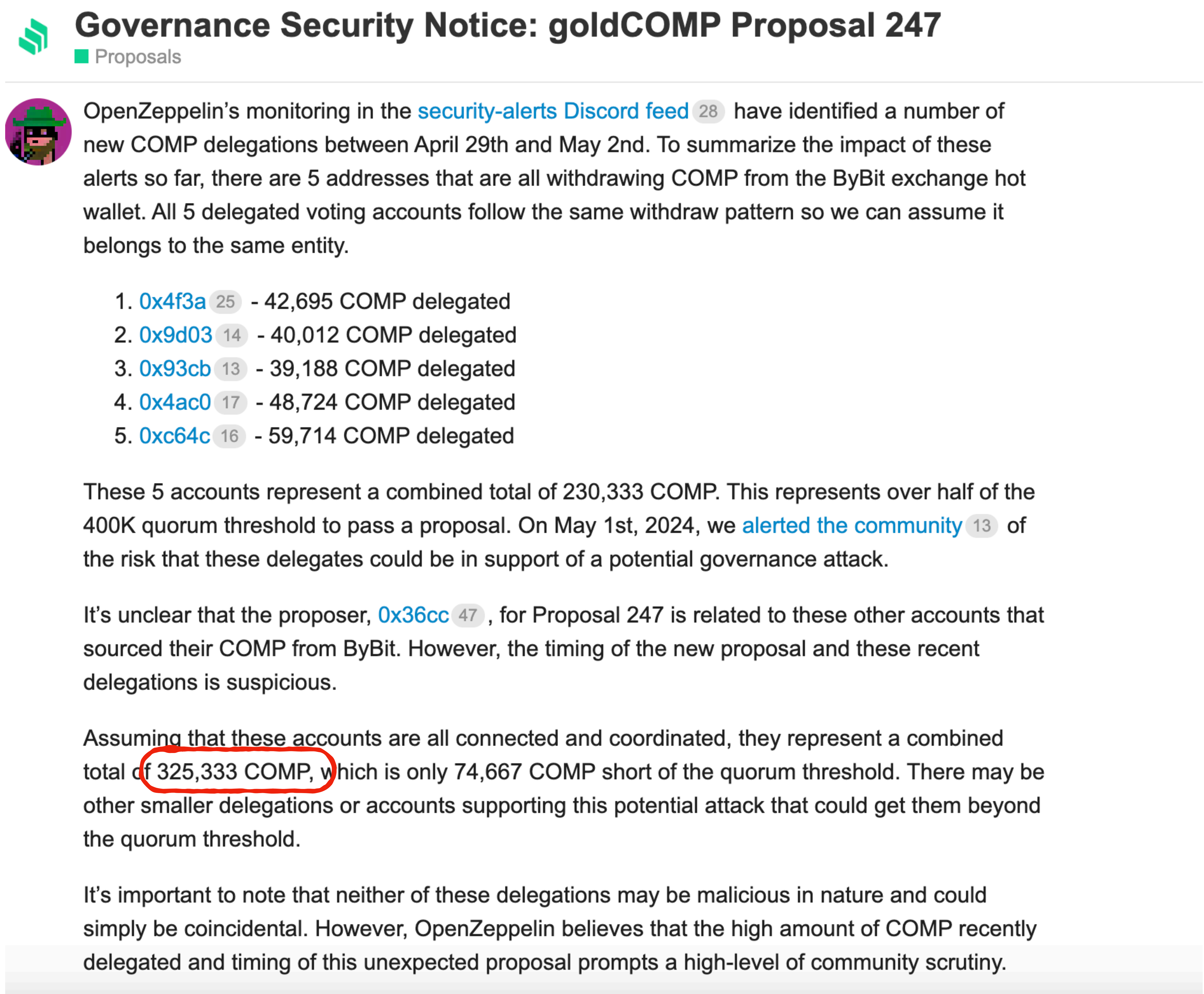
- Exploit 3 critical vulnerabilities:
  - Anonymous Registration
  - Voter Apathy and Vote Sniping
  - Lack of Oversight

Vulnerabilities

- Exploit 3 critical vulnerabilities
  - **Anonymous Registration**
  - Voter Apathy and Vote Sniping
  - Lack of Oversight

Anonymous Registration

- Nobody knew how large the malicious party was !!!



Governance Security Notice: goldCOMP Proposal 247

Proposals

OpenZeppelin's monitoring in the security-alerts Discord feed 28 have identified a number of new COMP delegations between April 29th and May 2nd. To summarize the impact of these alerts so far, there are 5 addresses that are all withdrawing COMP from the ByBit exchange hot wallet. All 5 delegated voting accounts follow the same withdraw pattern so we can assume it belongs to the same entity.

1. 0x4f3a 25 - 42,695 COMP delegated
2. 0x9d03 14 - 40,012 COMP delegated
3. 0x93cb 13 - 39,188 COMP delegated
4. 0x4ac0 17 - 48,724 COMP delegated
5. 0xc64c 16 - 59,714 COMP delegated

These 5 accounts represent a combined total of 230,333 COMP. This represents over half of the 400K quorum threshold to pass a proposal. On May 1st, 2024, we alerted the community 13 of the risk that these delegates could be in support of a potential governance attack.

It's unclear that the proposer, 0x36cc 47, for Proposal 247 is related to these other accounts that sourced their COMP from ByBit. However, the timing of the new proposal and these recent delegations is suspicious.

Assuming that these accounts are all connected and coordinated, they represent a combined total of 325,333 COMP, which is only 74,667 COMP short of the quorum threshold. There may be other smaller delegations or accounts supporting this potential attack that could get them beyond the quorum threshold.

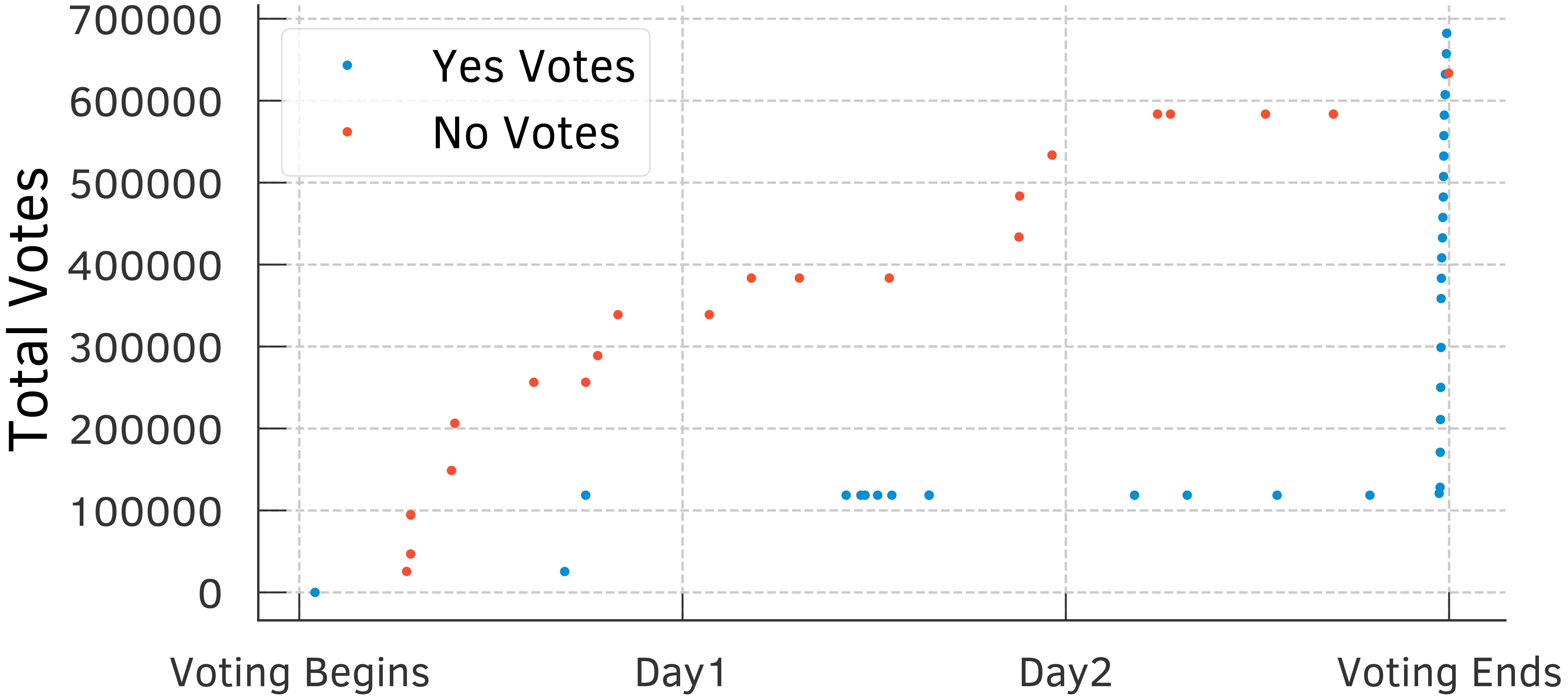
It's important to note that neither of these delegations may be malicious in nature and could simply be coincidental. However, OpenZeppelin believes that the high amount of COMP recently delegated and timing of this unexpected proposal prompts a high-level of community scrutiny.

Vulnerabilities

- Exploit 3 critical vulnerabilities
  - Anonymous Registration
  - **Voter Apathy and Vote Sniping**
  - Lack of Oversight

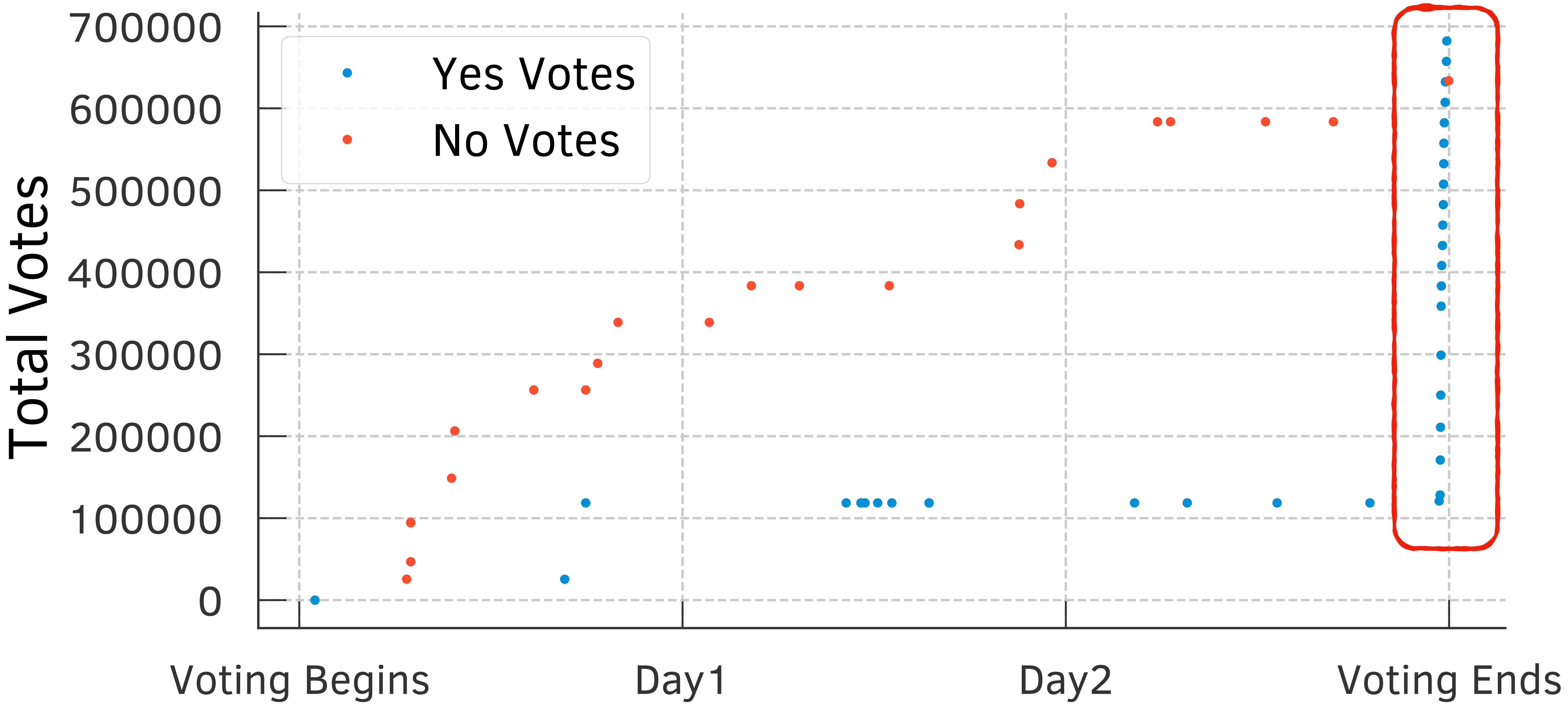
Voter Apathy and Vote Sniping

- On-chain voting has a cost
- Over **582K Votes (over 82%)** were cast in the last 30 minutes



Voter Apathy and Vote Sniping

- On-chain voting has a cost
- Over **582K Votes (over 82%)** were cast in the last 30 minutes



Vulnerabilities

- Exploit 3 critical vulnerabilities
  - Anonymous Registration
  - Voter Apathy and Vote Sniping
  - **Lack of Oversight**

Lack of Oversight

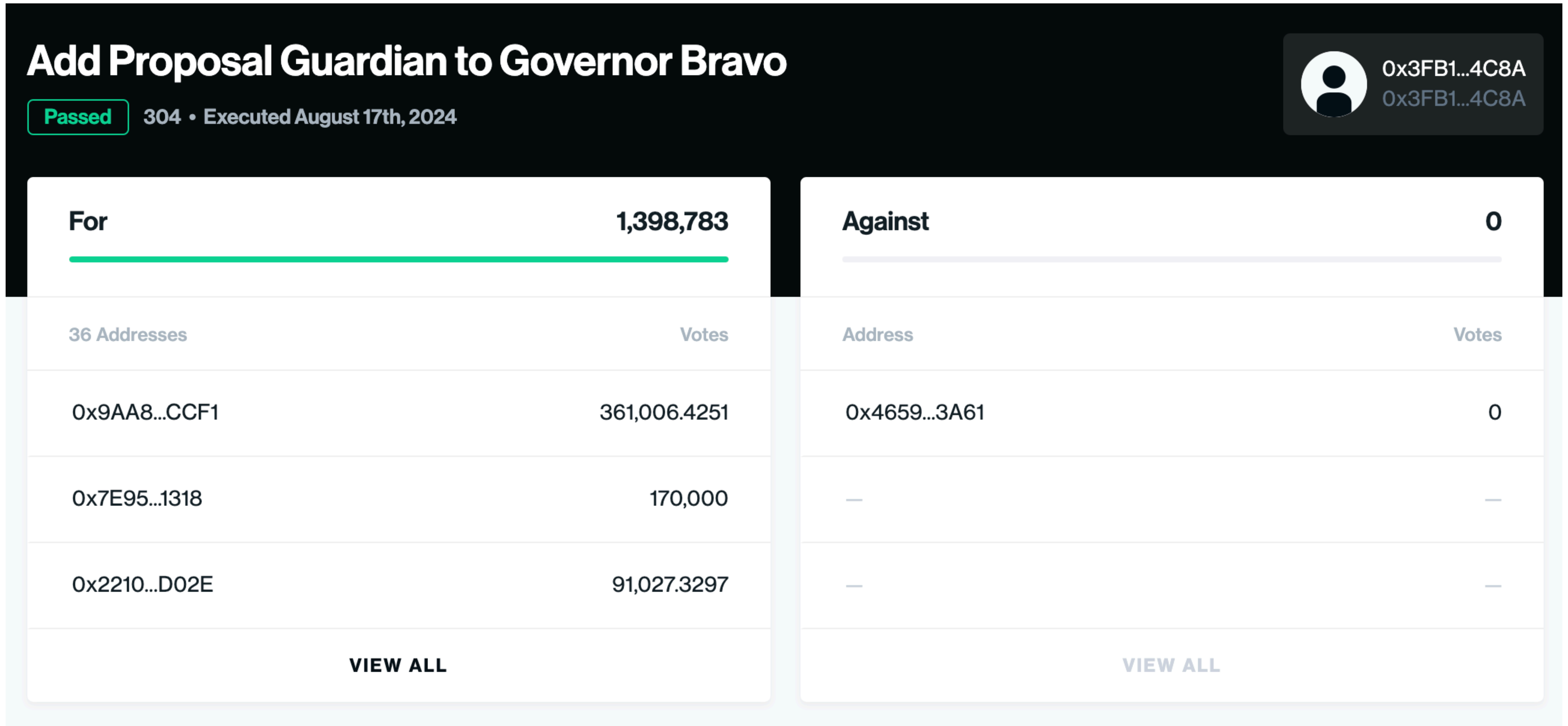
- No Veto Authority !!!

Lack of Oversight

- **No Veto Authority !!!**
- In response, Compound added a vetoer.

Lack of Oversight

- **No Veto Authority !!!**
- In response, Compound added a vetoer.



Add Proposal Guardian to Governor Bravo

Passed 304 • Executed August 17th, 2024

0x3FB1...4C8A
0x3FB1...4C8A

For	1,398,783
36 Addresses	Votes
0x9AA8...CCF1	361,006.4251
0x7E95...1318	170,000
0x2210...D02E	91,027.3297

VIEW ALL

Against	0
Address	Votes
0x4659...3A61	0
—	—
—	—

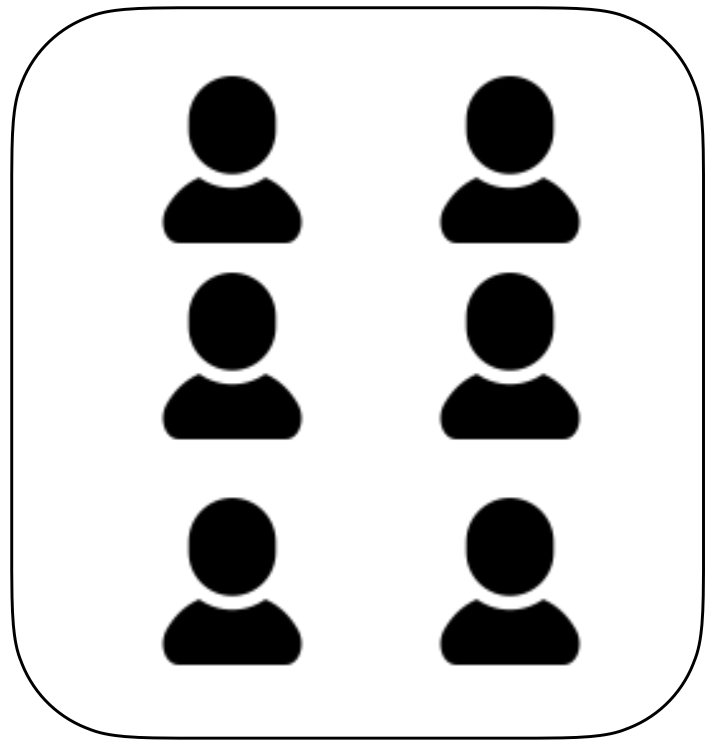
VIEW ALL

Conclusion

- Classified DAOs along different security critical dimensions
  - Decentralisation vs Security

Conclusion

- Classified DAOs along different security critical dimensions
  - Decentralisation vs Security

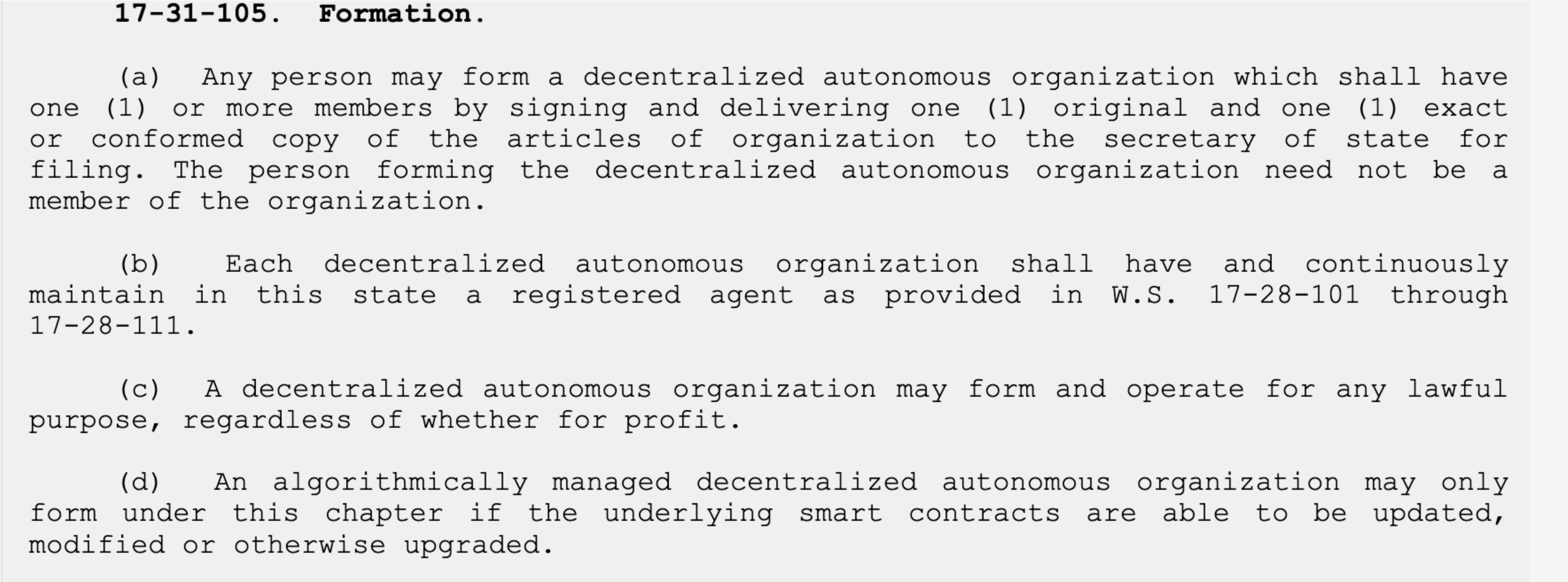


Conclusion

- Classified DAOs along different security critical dimensions
  - Decentralisation vs Security

Conclusion

- *“An algorithmically managed decentralized autonomous organisation may only form under this chapter if the underlying smart contracts are able to be* ***updated, modified or otherwise upgraded****”*



17-31-105. Formation.

(a) Any person may form a decentralized autonomous organization which shall have one (1) or more members by signing and delivering one (1) original and one (1) exact or conformed copy of the articles of organization to the secretary of state for filing. The person forming the decentralized autonomous organization need not be a member of the organization.

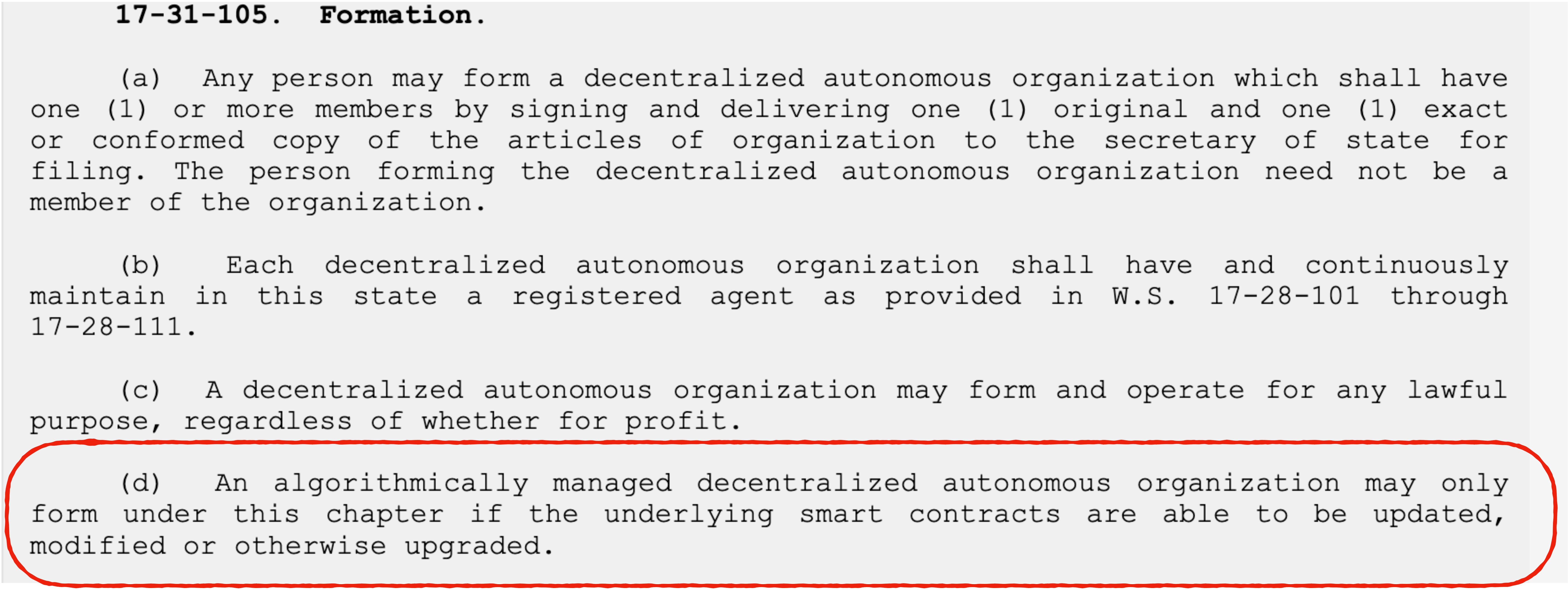
(b) Each decentralized autonomous organization shall have and continuously maintain in this state a registered agent as provided in W.S. 17-28-101 through 17-28-111.

(c) A decentralized autonomous organization may form and operate for any lawful purpose, regardless of whether for profit.

(d) An algorithmically managed decentralized autonomous organization may only form under this chapter if the underlying smart contracts are able to be updated, modified or otherwise upgraded.

Conclusion

- *“An algorithmically managed decentralized autonomous organisation may only form under this chapter if the underlying smart contracts are able to be **updated, modified or otherwise upgraded**”*



17-31-105. Formation.

(a) Any person may form a decentralized autonomous organization which shall have one (1) or more members by signing and delivering one (1) original and one (1) exact or conformed copy of the articles of organization to the secretary of state for filing. The person forming the decentralized autonomous organization need not be a member of the organization.

(b) Each decentralized autonomous organization shall have and continuously maintain in this state a registered agent as provided in W.S. 17-28-101 through 17-28-111.

(c) A decentralized autonomous organization may form and operate for any lawful purpose, regardless of whether for profit.

(d) An algorithmically managed decentralized autonomous organization may only form under this chapter if the underlying smart contracts are able to be updated, modified or otherwise upgraded.

Thank you!

Introduction

- Decentralized systems are becoming increasingly popular

Introduction

- Decentralized systems are becoming increasingly popular

Introduction

- Decentralized systems are becoming increasingly popular

Introduction

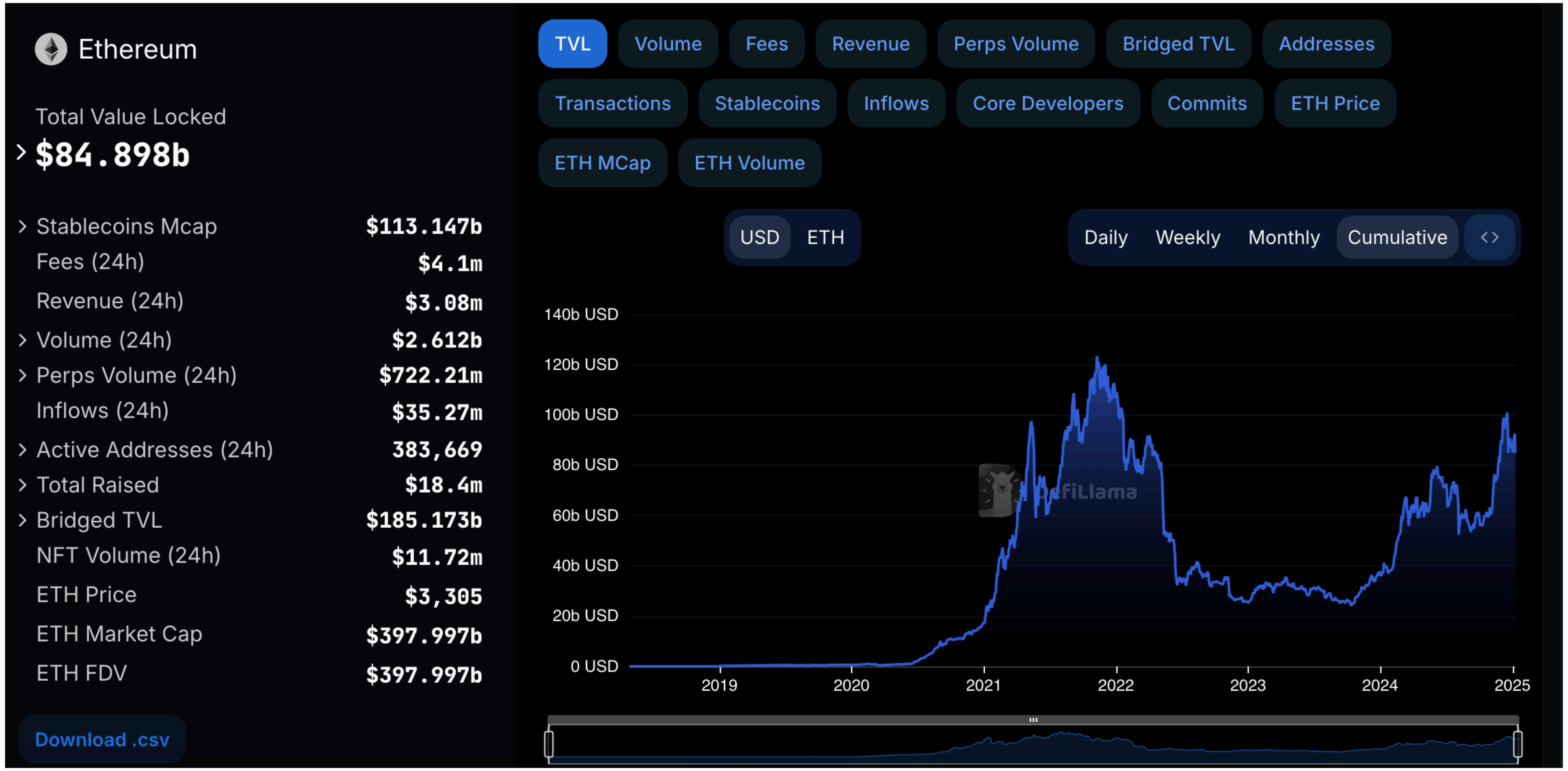
- Decentralized systems are becoming increasingly popular

Introduction

- Decentralized systems are becoming increasingly popular

ONDC
Open Network for Digital Commerce

Introduction



Ethereum

Total Value Locked

$84.898b

Stablecoins Mcap	$113.147b
Fees (24h)	$4.1m
Revenue (24h)	$3.08m
Volume (24h)	$2.612b
Perps Volume (24h)	$722.21m
Inflows (24h)	$35.27m
Active Addresses (24h)	383,669
Total Raised	$18.4m
Bridged TVL	$185.173b
NFT Volume (24h)	$11.72m
ETH Price	$3,305
ETH Market Cap	$397.997b
ETH FDV	$397.997b

Introduction

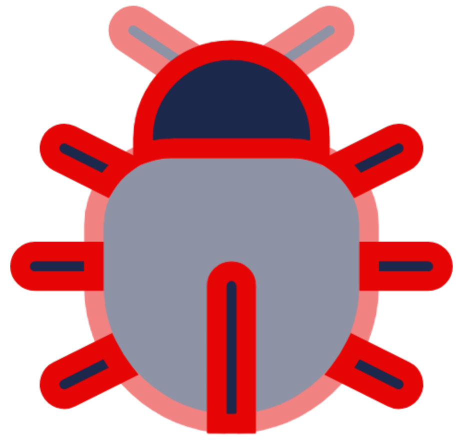
Introduction

Smart Contract

Introduction

Smart Contract

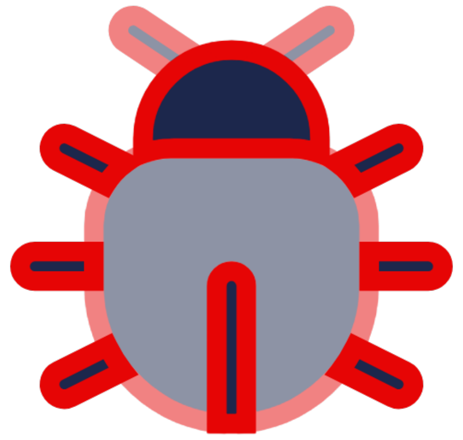
Bug



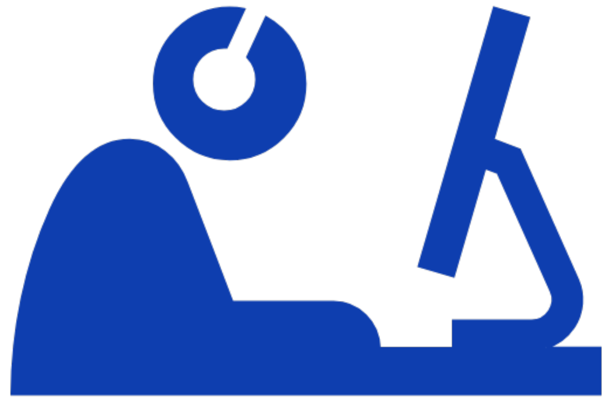
Introduction

Smart Contract

Bug



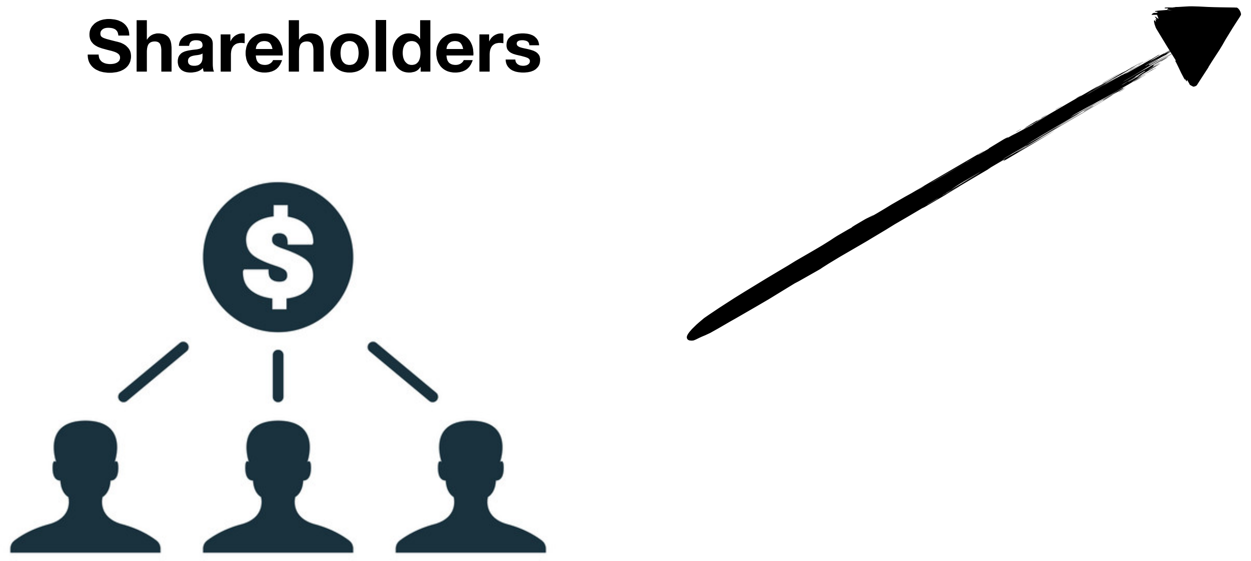
Coder



How do organisations govern?

Shareholders

How do organisations govern?



Shareholders

How do organisations govern?

Shareholders

How do organisations govern?

- What happens if the members are anonymous?

How do organisations govern?

- What happens if the members are anonymous?

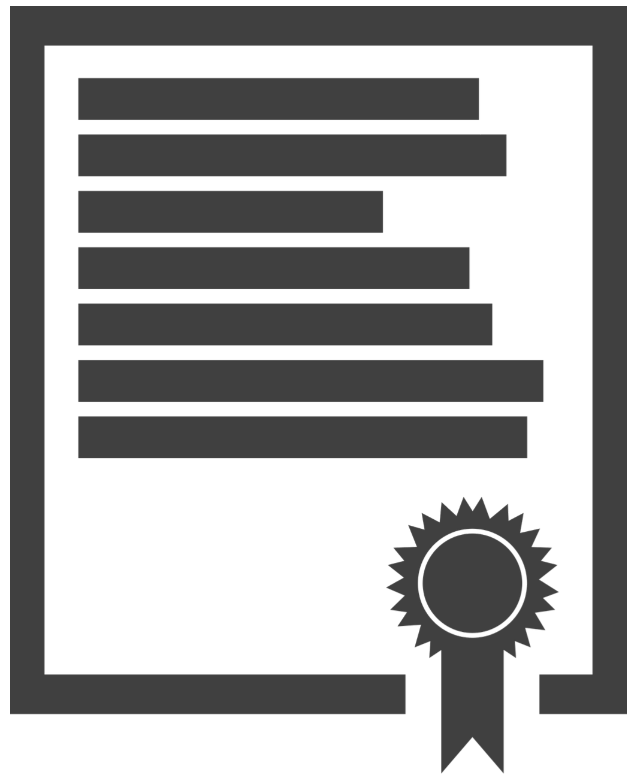
How do organisations govern?

- What happens if the members are anonymous?
- Establish trust through **Governance Contracts**

How do organisations govern?

- What happens if the members are anonymous?
- Establish trust through **Governance Contracts**

Governance Contract

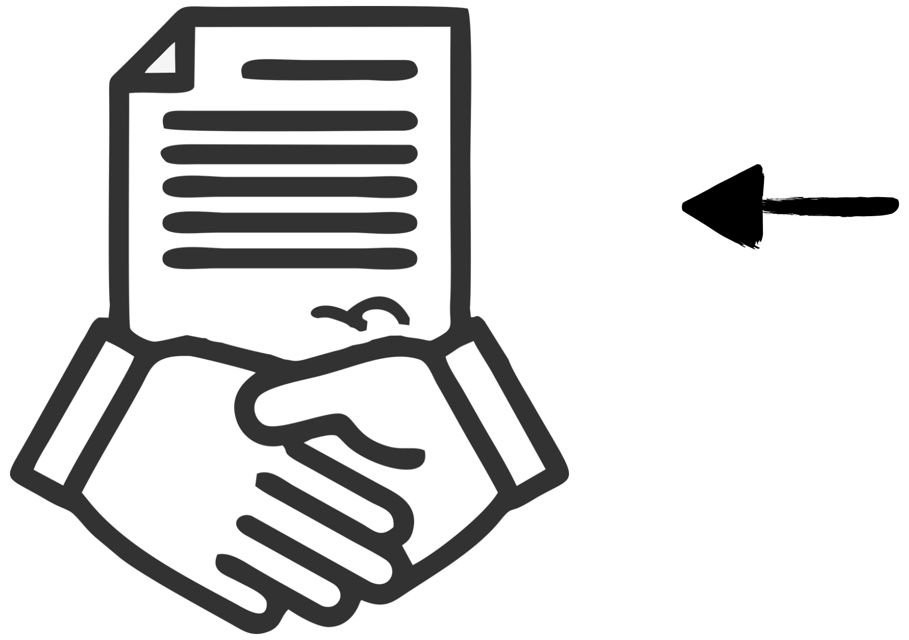


Governance Contracts and DAOs

Governance Contracts and DAOs

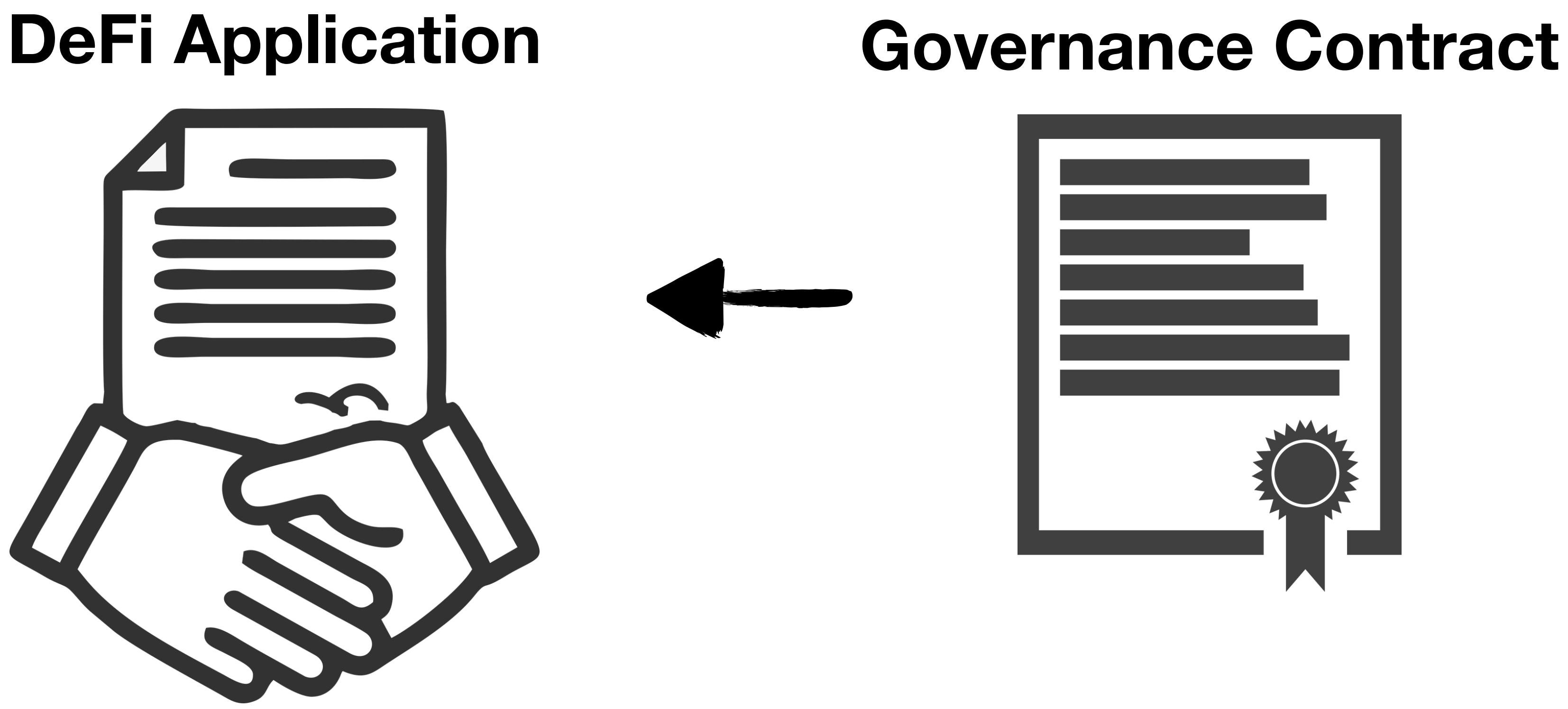
DeFi Application

Governance Contracts and DAOs



DeFi Application

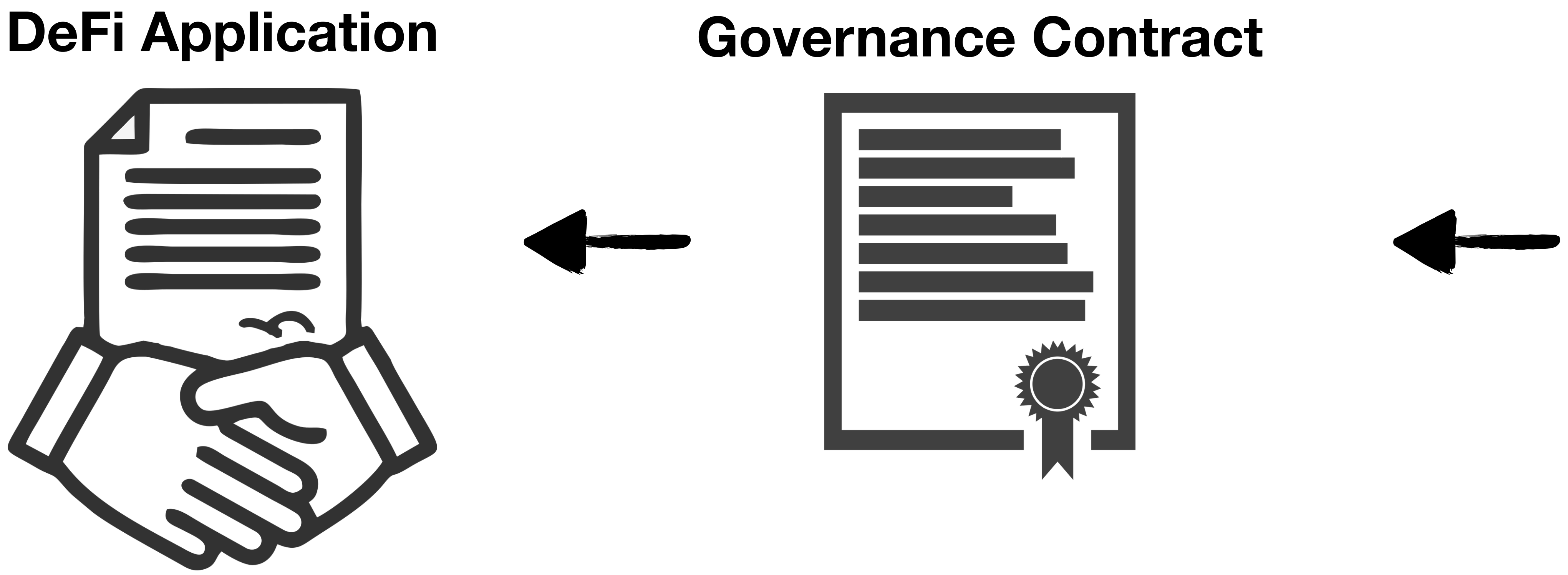
Governance Contracts and DAOs



DeFi Application

Governance Contract

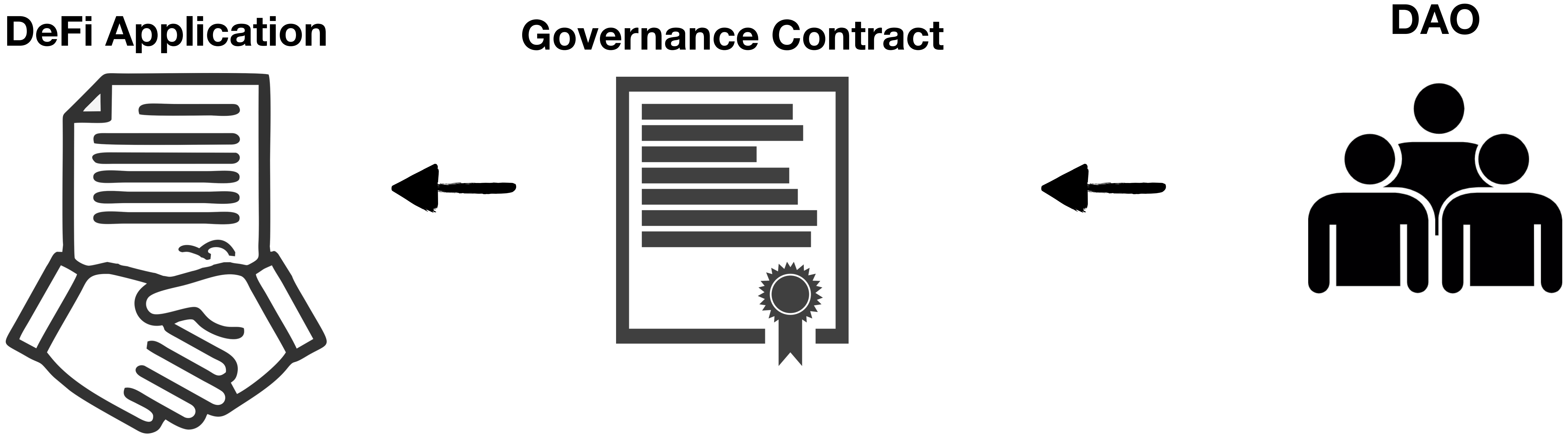
Governance Contracts and DAOs



DeFi Application

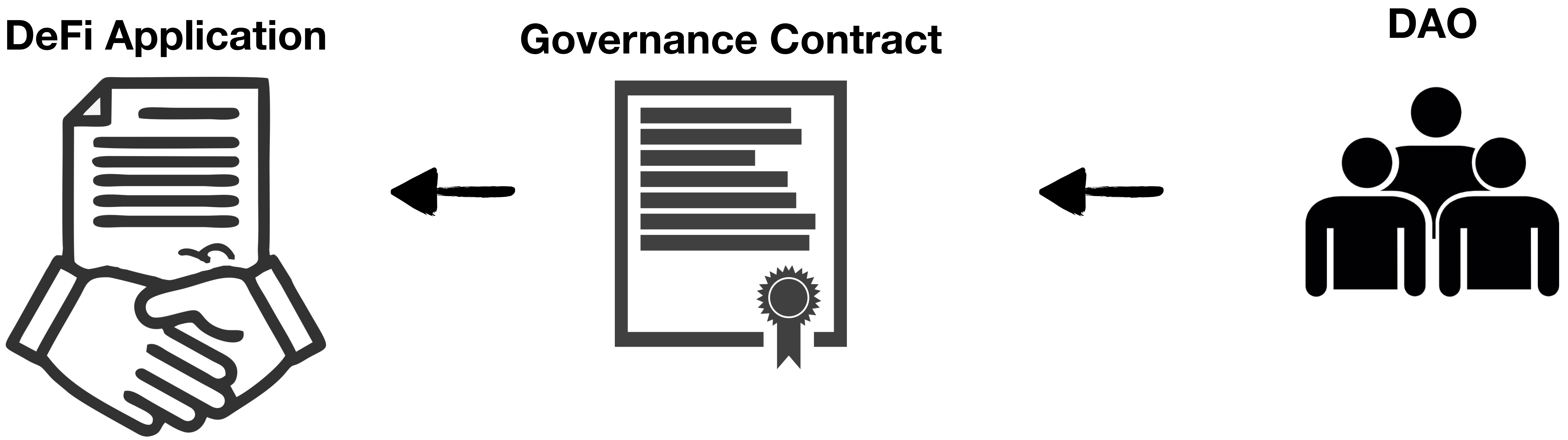
Governance Contract

Governance Contracts and DAOs



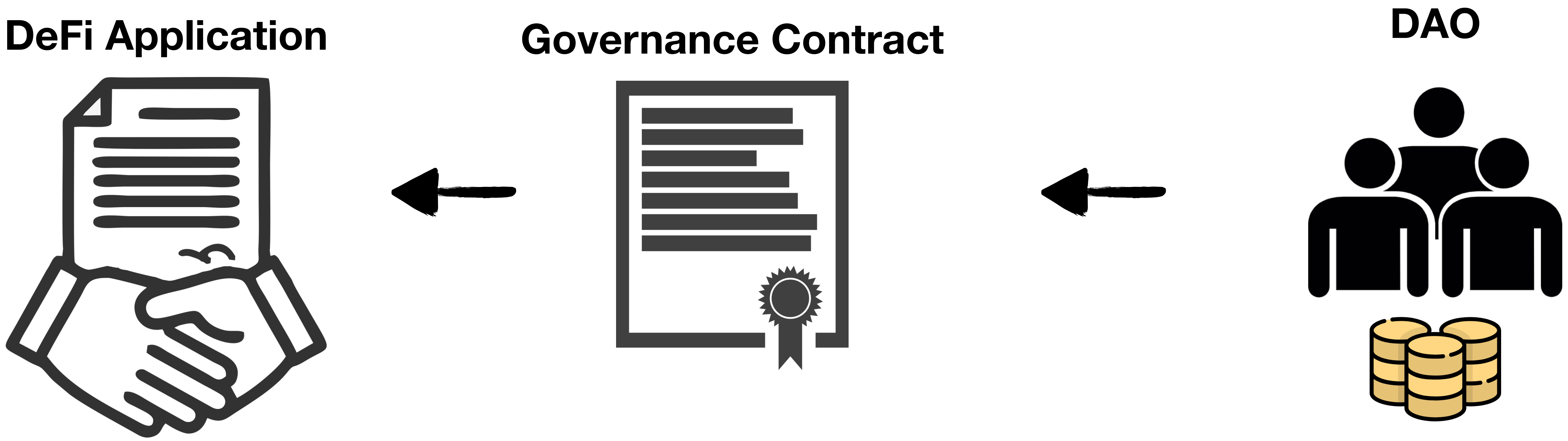
Governance Contracts and DAOs

- DAO consists of the group of holders of the **Governance Token**

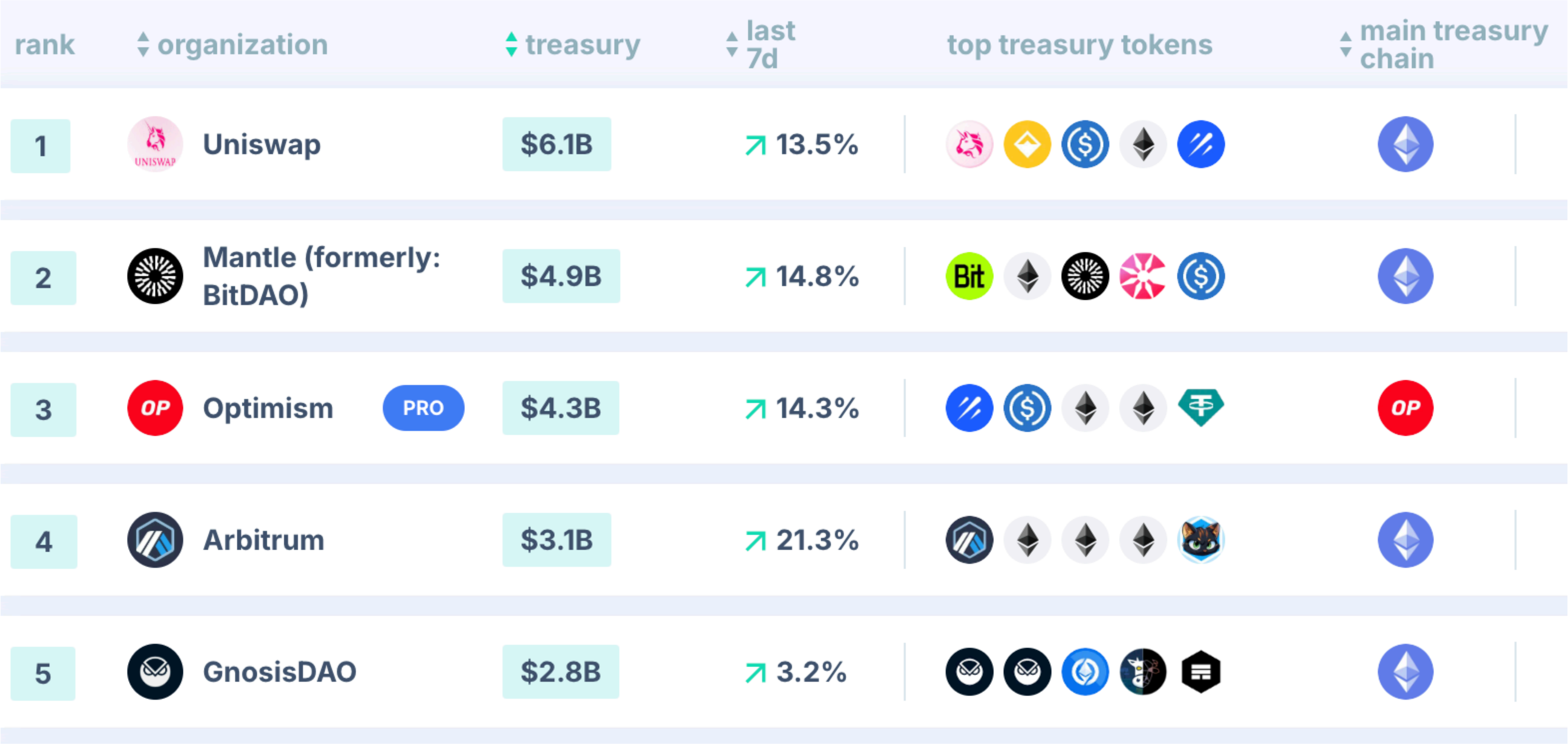


Governance Contracts and DAOs

- DAO consists of the group of holders of the **Governance Token**

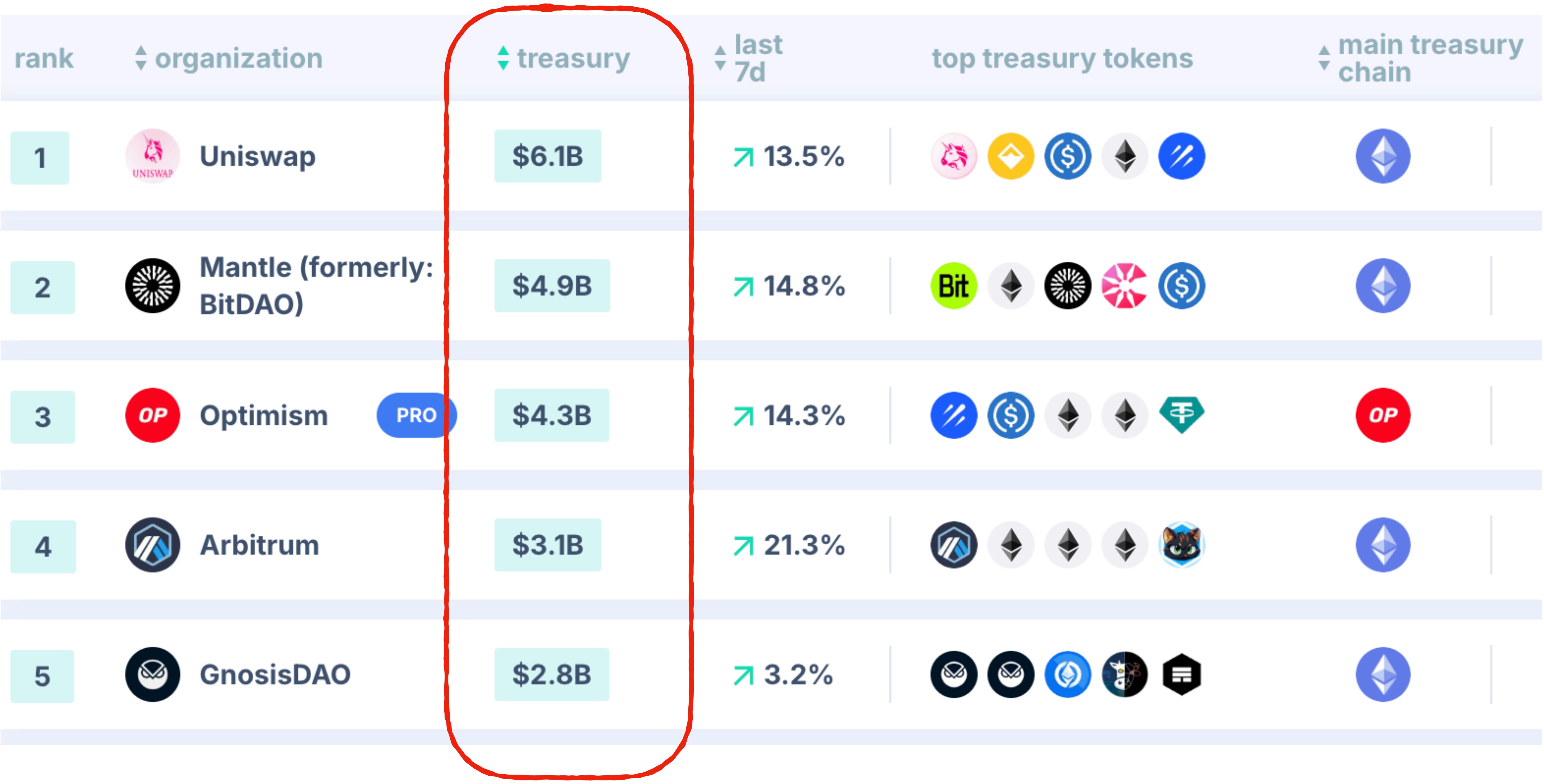


What can go wrong?



rank	organization	treasury	last 7d	top treasury tokens	main treasury chain
1	Uniswap	$6.1B	↗ 13.5%		
2	Mantle (formerly: BitDAO)	$4.9B	↗ 14.8%	Bit	
3	Optimism PRO	$4.3B	↗ 14.3%		OP
4	Arbitrum	$3.1B	↗ 21.3%		
5	GnosisDAO	$2.8B	↗ 3.2%		

What can go wrong?



rank	organization	treasury	last 7d	top treasury tokens	main treasury chain
1	Uniswap	$6.1B	↗ 13.5%		
2	Mantle (formerly: BitDAO)	$4.9B	↗ 14.8%	Bit	
3	Optimism PRO	$4.3B	↗ 14.3%		OP
4	Arbitrum	$3.1B	↗ 21.3%		
5	GnosisDAO	$2.8B	↗ 3.2%		

What can go wrong?

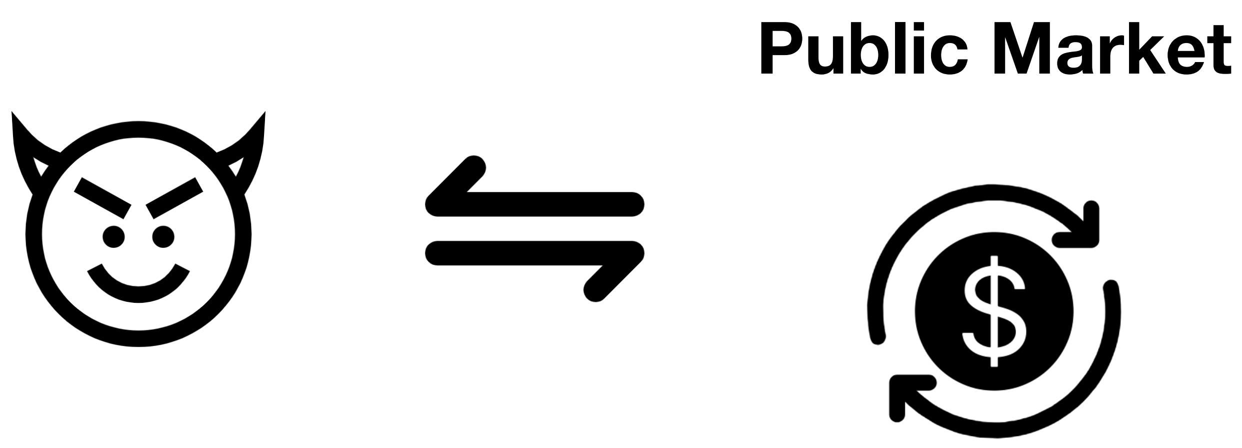
What can go wrong?

Public Market

What can go wrong?

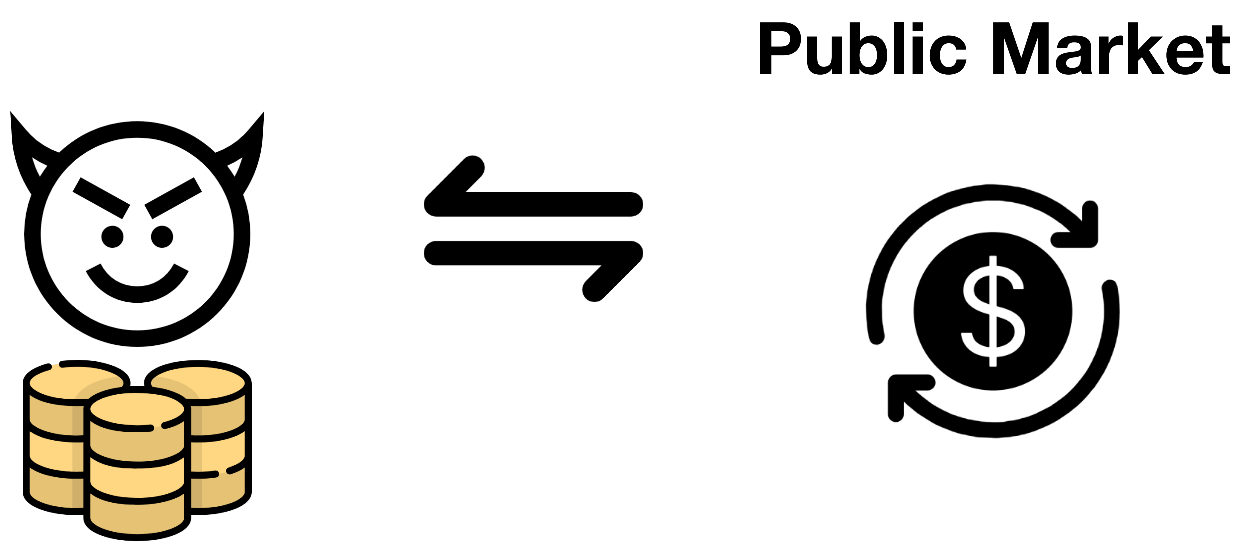
Public Market

What can go wrong?

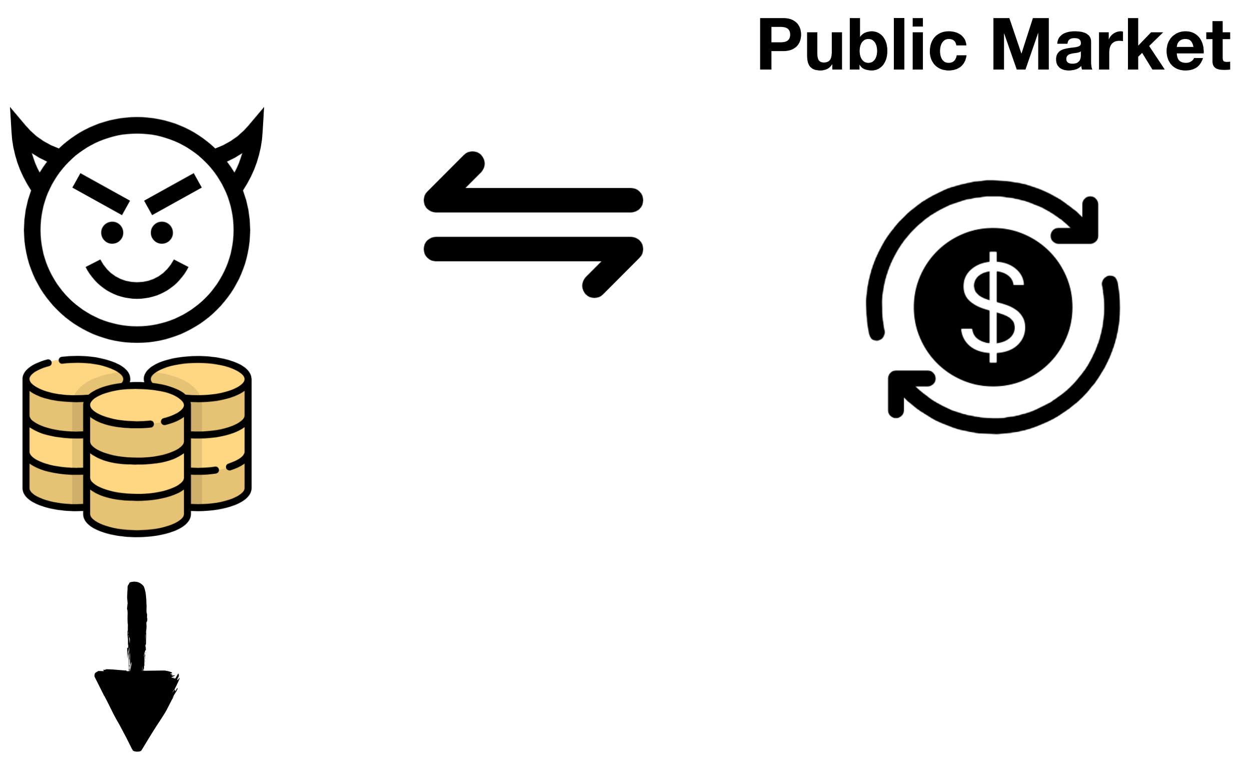


Public Market

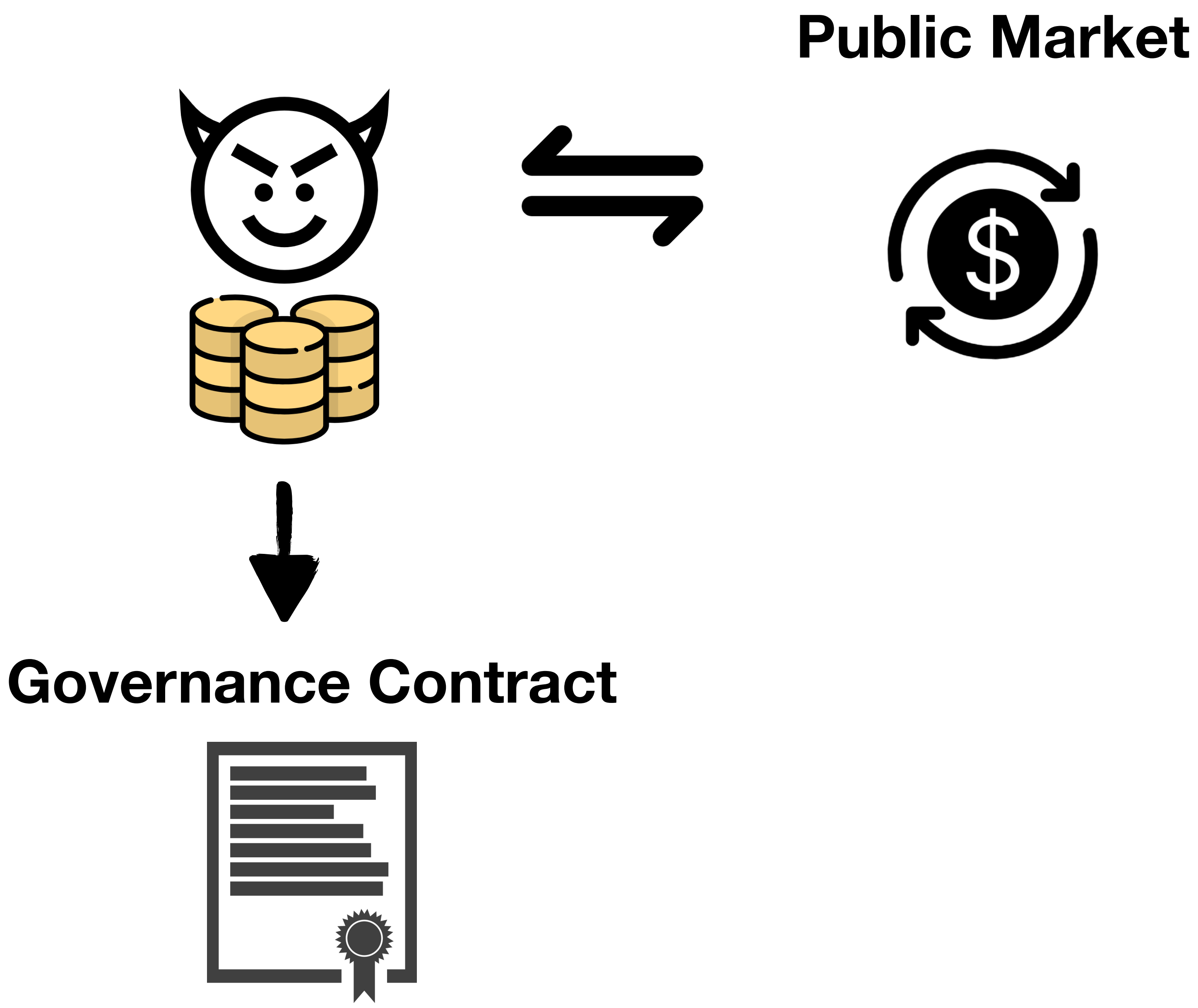
What can go wrong?


Public Market

What can go wrong?



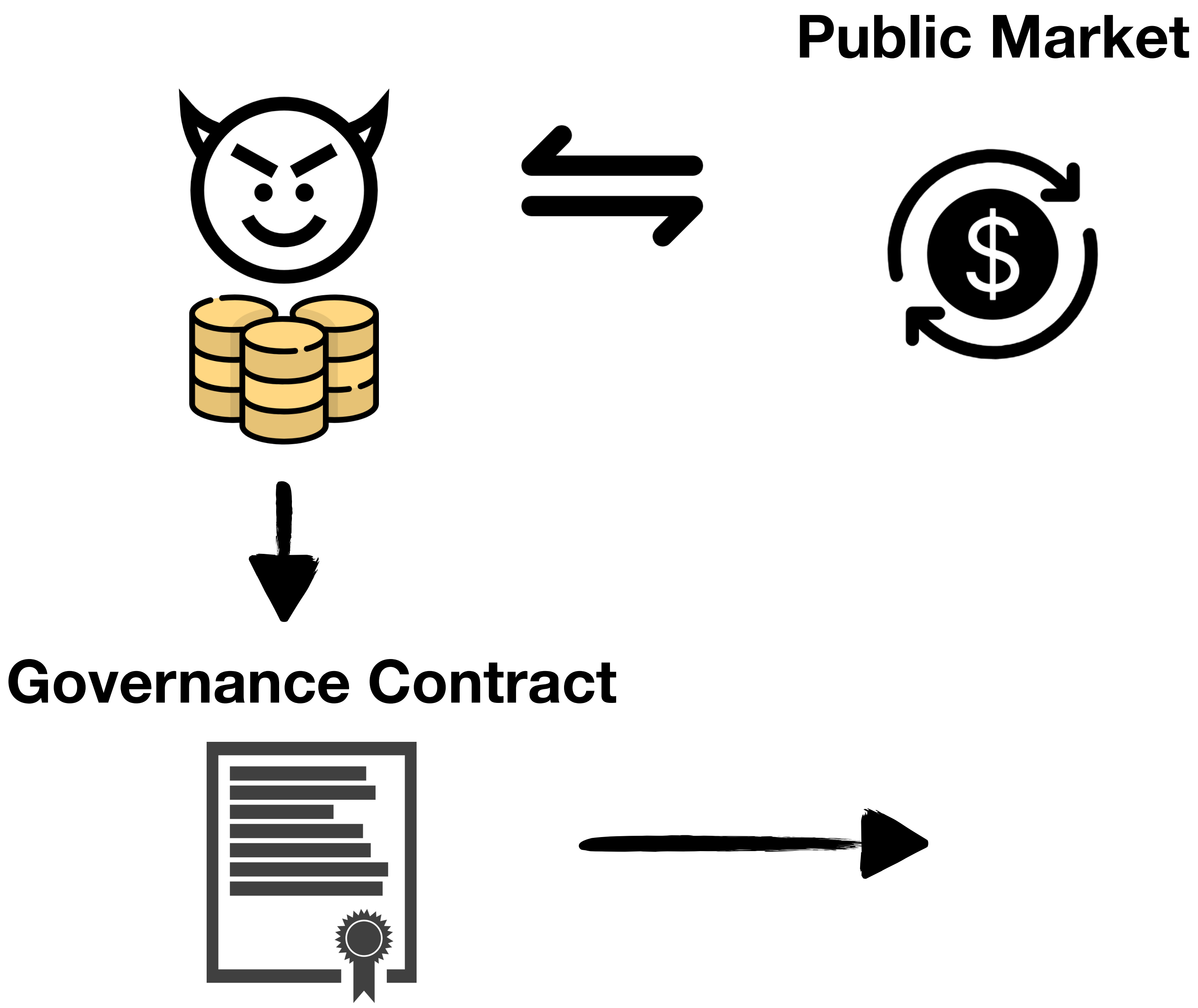
What can go wrong?



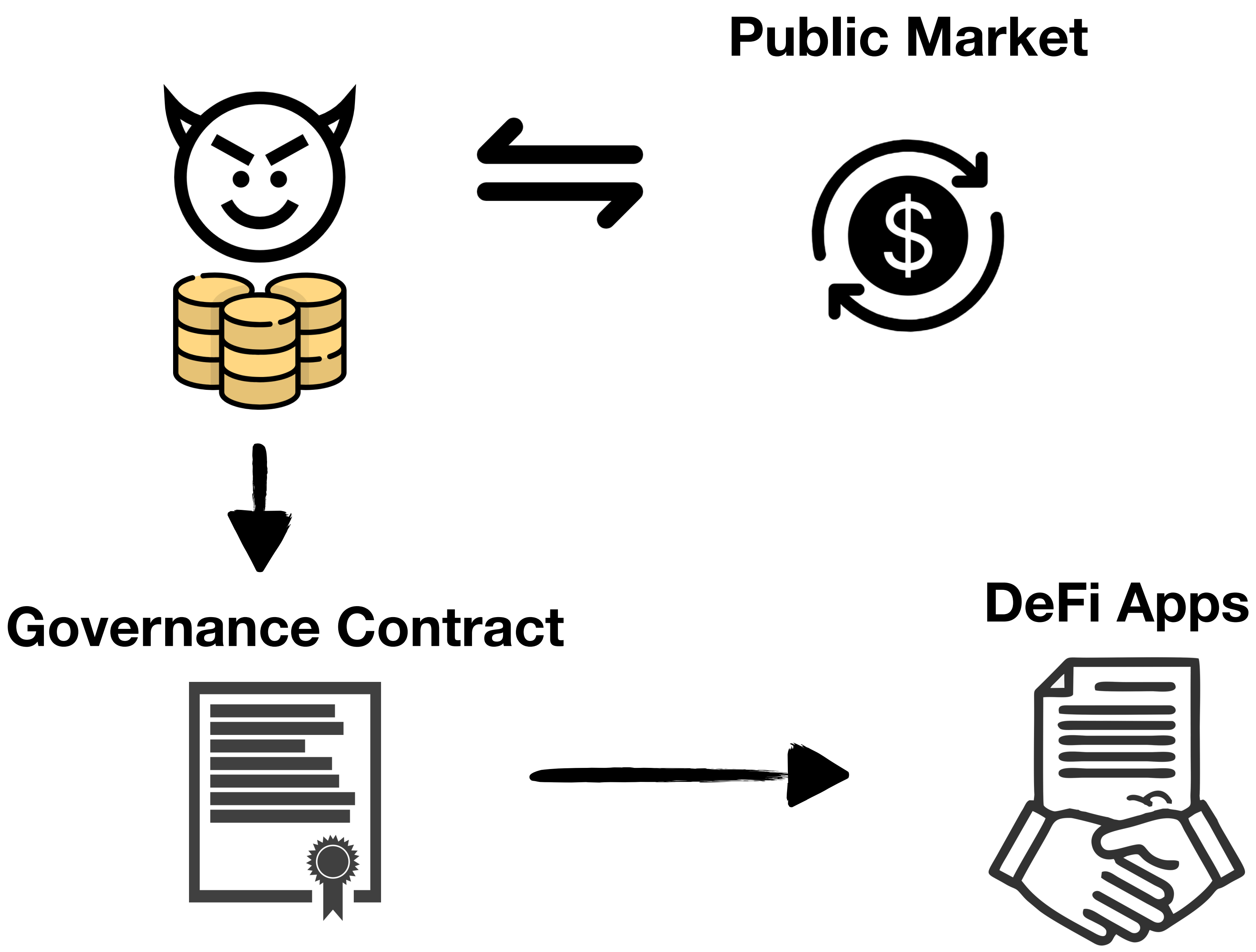
Public Market

Governance Contract

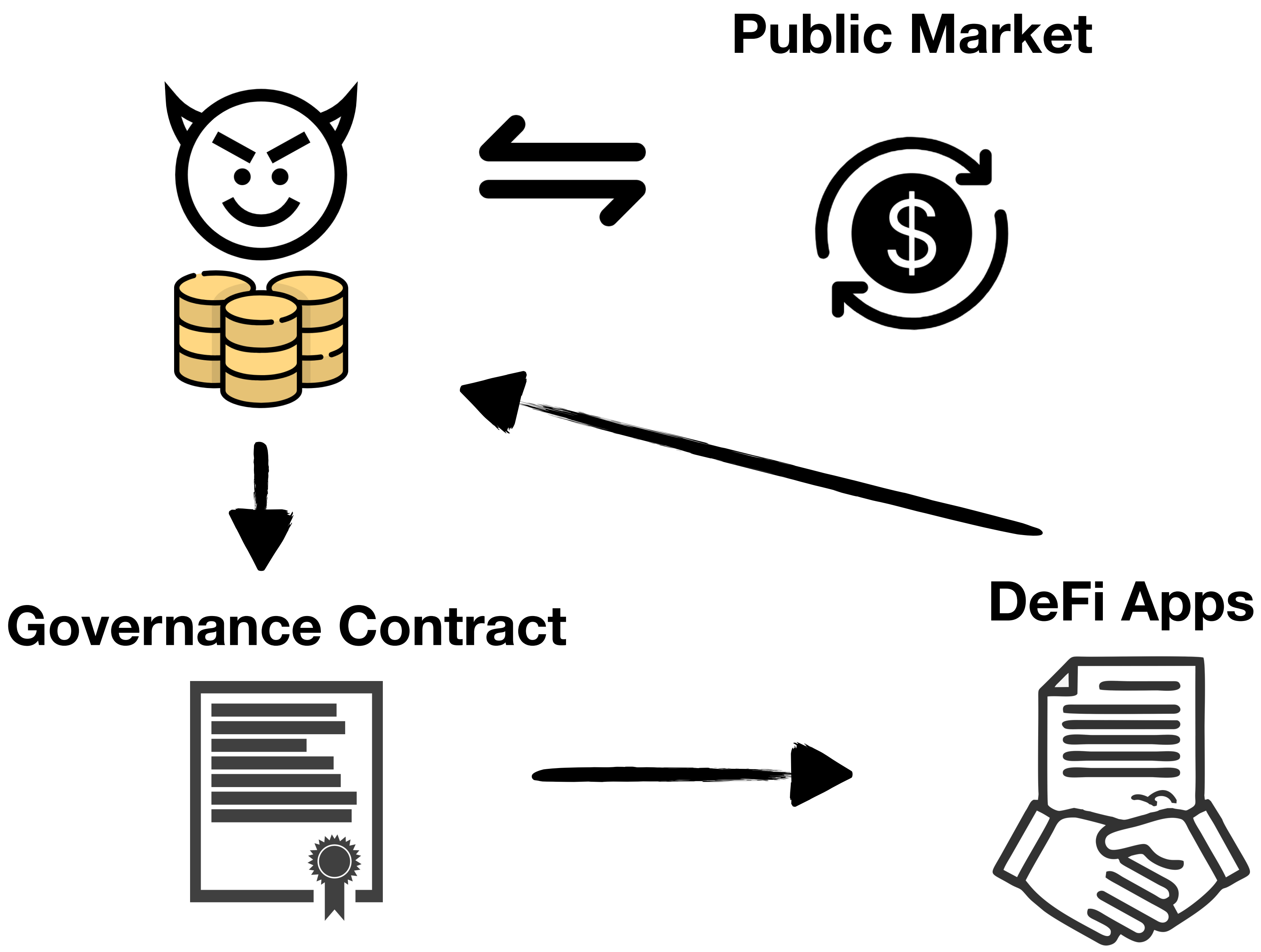
What can go wrong?



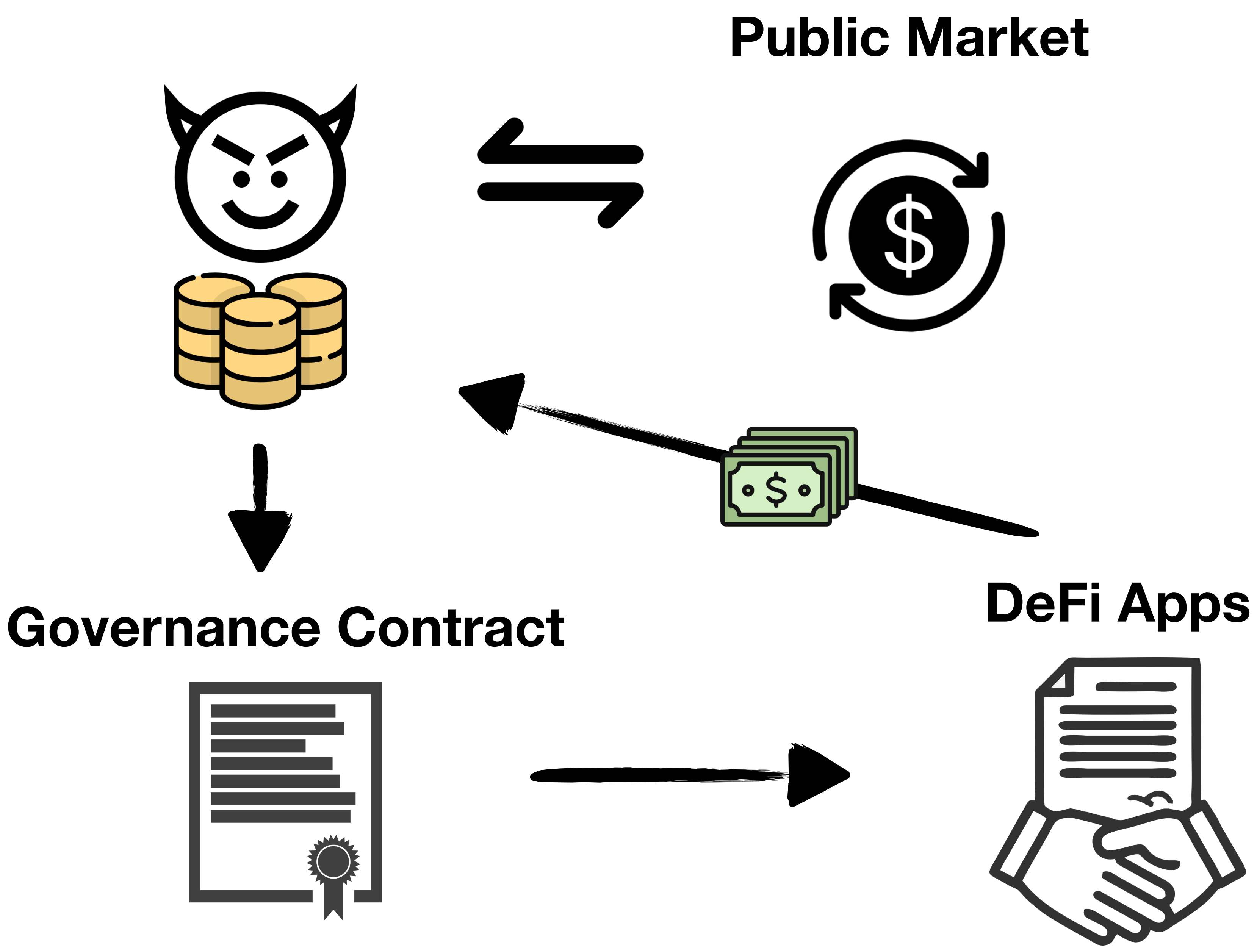
What can go wrong?



What can go wrong?



What can go wrong?



DAOs in practice

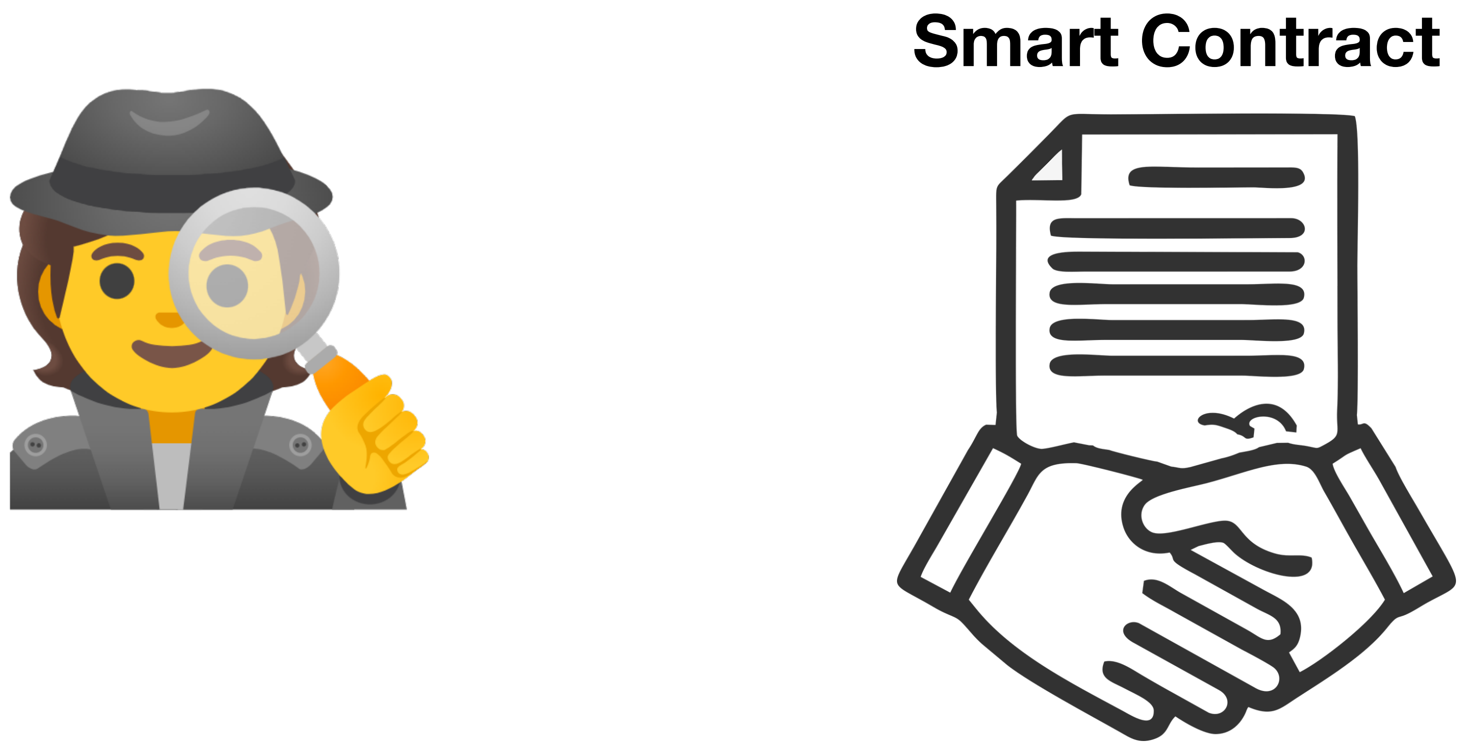
- We analysed the top **51** DAOs on Ethereum

DAOs in practice

- We analysed the top **51** DAOs on Ethereum

DAOs in practice

- We analysed the top **51** DAOs on Ethereum



DAOs in practice

- We analysed the top **51** DAOs on Ethereum

Smart Contract

Governance Contract

DAOs in practice

- We analysed the top **51** DAOs on Ethereum

Smart Contract

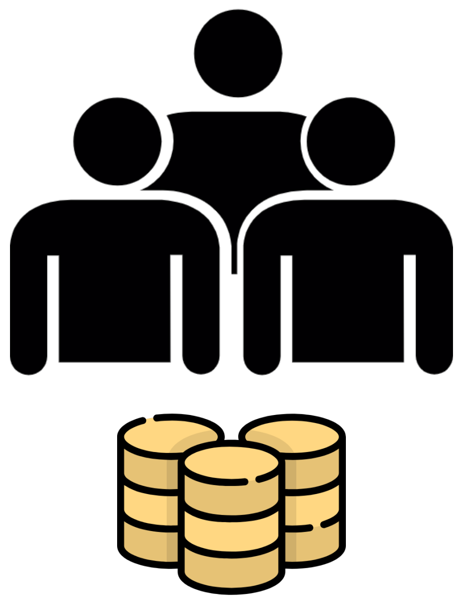
Governance Contract

Developer Documentations

ID	Protocol	RegReq	RegMeth	VM	Call	Vot. Plat.	Vot. Fmt.	Vot. Typ.	Vot. Agg	Cert.	Exec.	Veto.
1	*Uniswap* [9]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	VI
2	*ENS* [10]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	VA
3	*Maker* [11]	👛	S	D	👤	🟢	♻	P	P	👤	👤	–
4	*Lido (Easy Track)* [12]	🏷	H	D	👤🛡	🟢	🕓	R	M	👤	👤	VI, VA
4	*Lido Governance* [13]	🏷	H	D	☻	🟢	🕓	P	M	👤	👤	–
5	*Frax Finance Omega* [14]	👛	S	D, D•	👤🛡	🟢	🕓	R	M	👤	👤	VA
5	*Frax Finance Alpha* [14]	👛	S	D, D•	☻	🟢	🕓	R	M	👤	👤	-
6	*AAVE* [15]	🏷	H, S	D, D•	☻	🟢	🕓	P	V	👤	👤	VA
7	*Compound* [16]	👛	H	D, D•	👤🛡☻	🟢	🕓	P	M	👤	👤	VI, VA
8	*Radicle* [17]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	–
9	*0x Protocol* [18]	👛	S	D, D•	☻	🟢	🕓	P	M	👤	👤	–
10	*Gitcoin* [19]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	–
11	*Silo Finance* [20]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	–
12	*Lyra* [21]	👛	S	D, D•	☻	🟢	🕓	P	M	👤	👤	VA
13	*API3* [22]	👛	S	D, D•	☻	🟢	🕓	P	M	👤	👤	–
14	*Ampleforth* [23]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	VI
15	*Instadapp* [24]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	VI, VA
16	*Rari* [25]	👛	S	D, D•	☻	🟢	🕓	P	M	👤	👤	VI, VA
17	*NounsDAO* [26]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	VI, VA
18	*Curve* [27]	👛	S	D	☻	🟢	🕓	P	T	👤	👤	–
19	*Origin* [28]	👛	S	D, D•	☻	🟢	🕓	P	M	👤	👤	VI
20	*Hop DAO* [29]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	–
21	*Cryptex* [30]	👛	H	D, D•	☻	🟢	🕓	P	M	👤	👤	–
22	*Angle Protocol* [31]	👛	S	D, D•	☻	🟢	🕓	P	M	👤	👤	VI, VA
23	*DxDao* [32]	👛	H	D	👤	🟢	🕓	P	T	👤	👤	–
24	*Nexus Mutual* [33]	👤✓	H	D	👤🛡	🟢	🕓	P	M	👤, C	👤	VA
25	*Goldfinch* [34]	👤✓	H	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
26	*ParagonsDAO* [35]	🏷	H, S	R	👤🛡	○	🕓	P	T	C	C	VI, VA
27	*Illuvium* [36]	👛	S	R	👤🛡	○	🕓	P	T	C	C	VI, VA
28	*SuperRare* [37]	🏷	H	D, D•	👤🛡	○	🕓	P	M	C, OC	C	VI, VA
29	*Mantle* [38]	👛	H	D, D•	👤🛡	○	🕓	P	M	C	C	VI, VA
30	*Res. Hub Fdn.* [39]	🏷	H	D	👤🛡☻	○	🕓	P	M	C	C	VI, VA
31	*Stargate Finance* [40]	👛	S	D, D•	👤🛡,☻	○	🕓	P	M	C	C	VI, VA
32	*Uma* [41]	👛	S	D, D•	👤🛡	○	🕓	P	M	C	C	VI, VA
33	*Cowswap* [42]	🏷	H, S	D, D•	👤🛡☻	○	🕓	P	M	C, OC	C	VI, VA
34	*Sturdy Finance* [43]	🏷	H	D	👤🛡☻	○	🕓	P	M	C	C	VI, VA
35	*Euler* [44]	👛	H	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
36	*SAFE* [45]	🏷	H, S	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
37	*Tokenlon* [46]	🏷	H, S	D	👤🛡	○	🕓	P	M	C	C	VI, VA
38	*Botto* [47]	👛	S	D	👤🛡	○	🕓	P	M	C	C	VI, VA
39	*Balancer* [48]	👛	S	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
40	*Sushiswap* [49]	👛	S	D, D•	👤🛡	○	🕓	P	M	C	C	VI, VA
41	*Gearbox* [50]	👛	S	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
42	*Paraswap* [51]	👛	S	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
43	*Alchemix* [52]	🏷	H, S	D, D•	👤🛡	○	🕓	P	M	C	C	VI, VA
44	*1Inch* [53]	👛	S	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
45	*Shutter DAO 0x36* [54]	👛	H	D, D•	👤🛡,☻	○	🕓	P	M	C	C	VI, VA
46	*Yearn Finance* [55]	👛	S	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
47	*Shapeshift* [56]	🏷	H, S	D, D•	👤🛡☻	○	🕓	P	M	C	C	VI, VA
48	*Decentraland* [57]	🏷	H	D, D•	👤🛡	○	🕓	P	M	C	C	VI, VA
49	*Optimism* [58]	👛	H	D, D•	👤🛡	🟢	🕓	P	M	👤	👤	VA
50	*Arbitrum* [59]	👛	H	D, D•	👤🛡☻	🟢	🕓	P	M	👤, C	👤	VA
51	*Synthetix* [60]	👛	H	R	👤🛡	○	🕓	P	T	C	C	VA

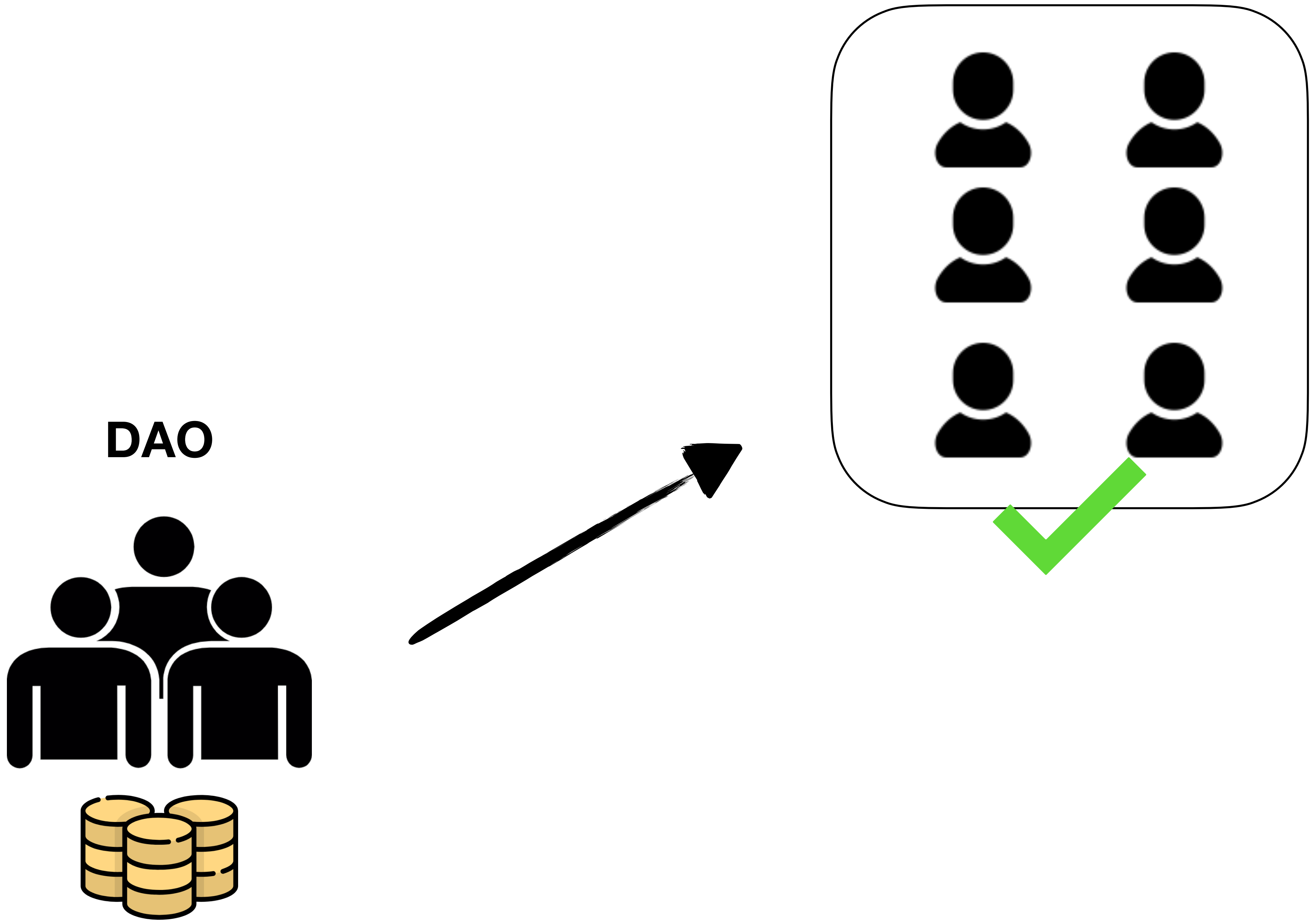
DAOs in practice

DAOs in practice

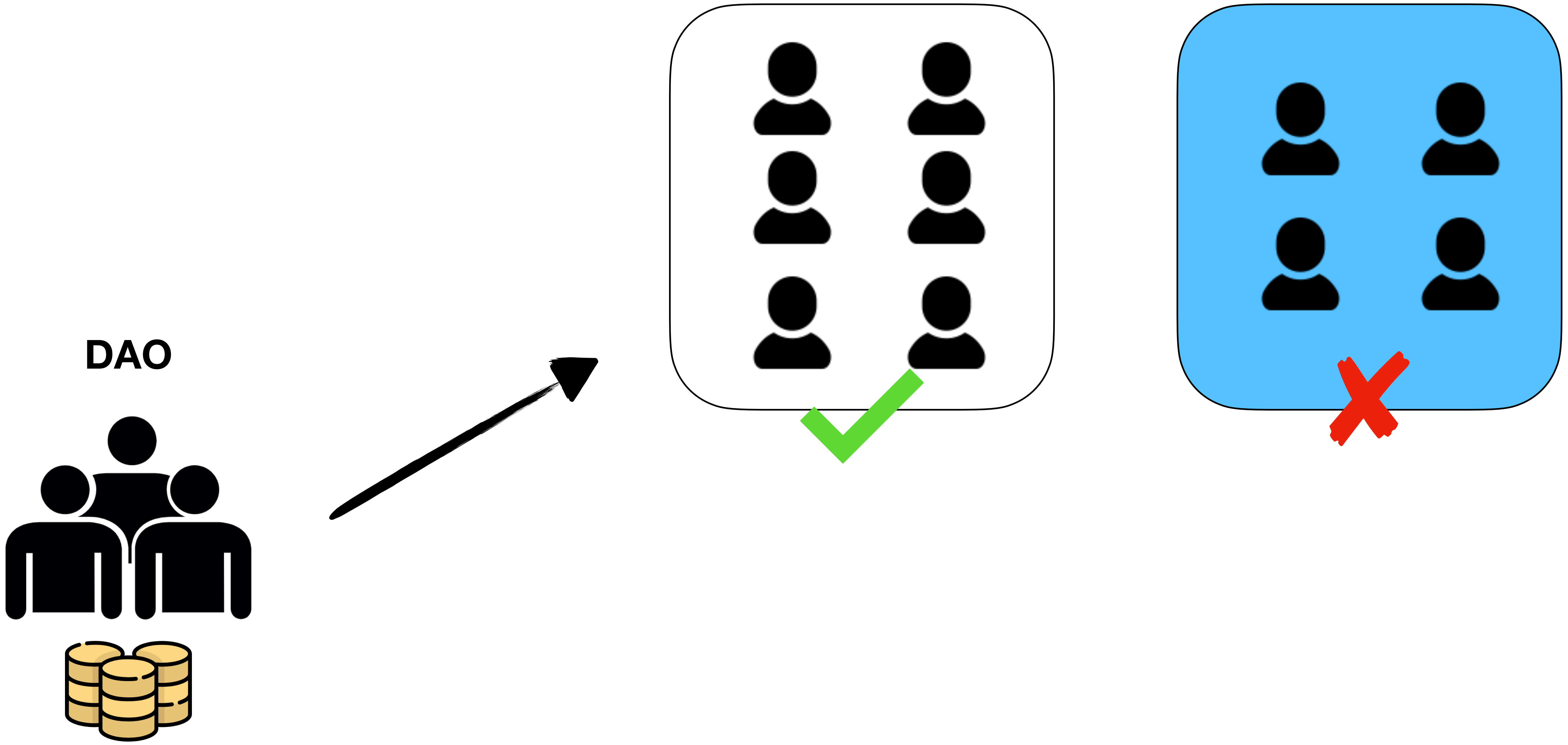


DAO

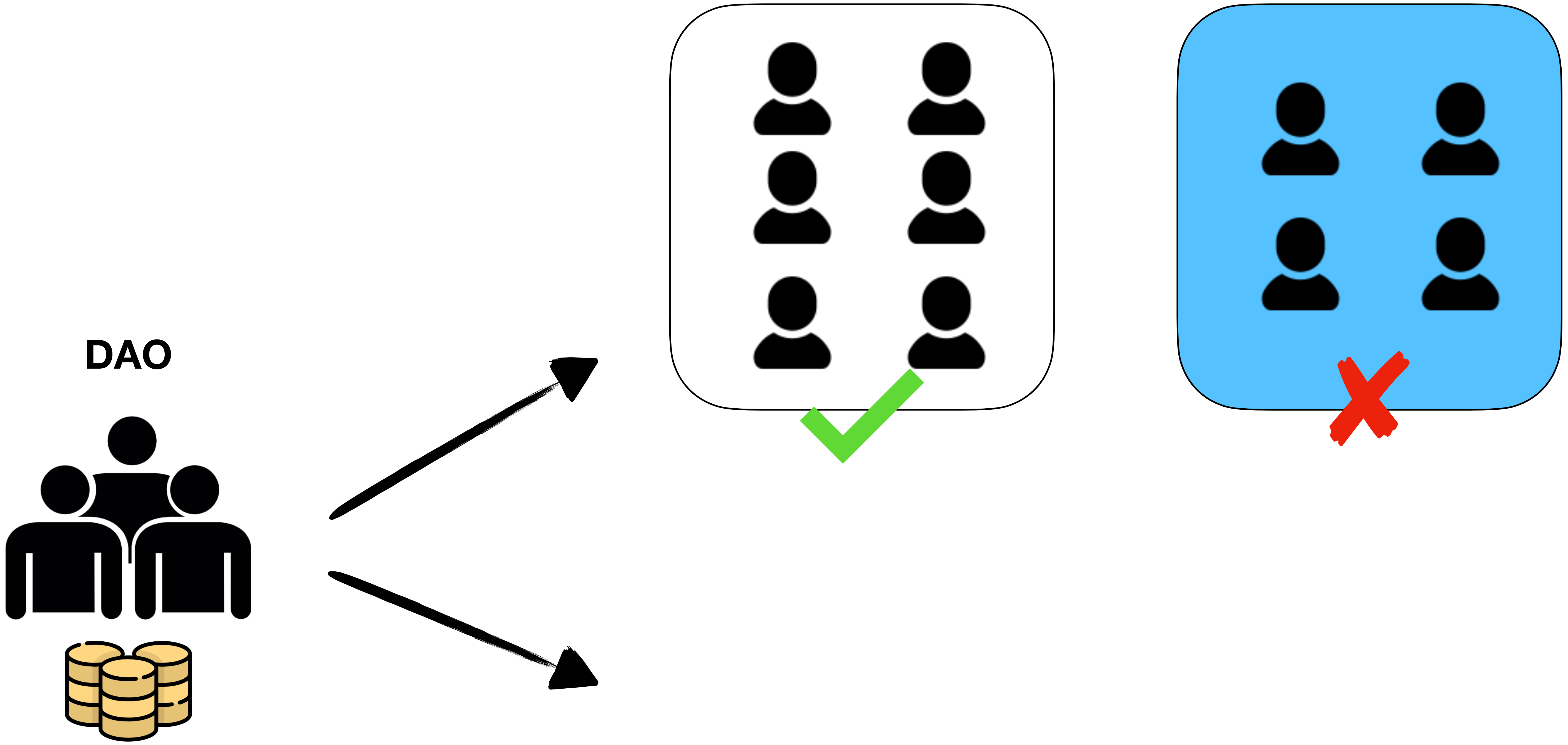
DAOs in practice



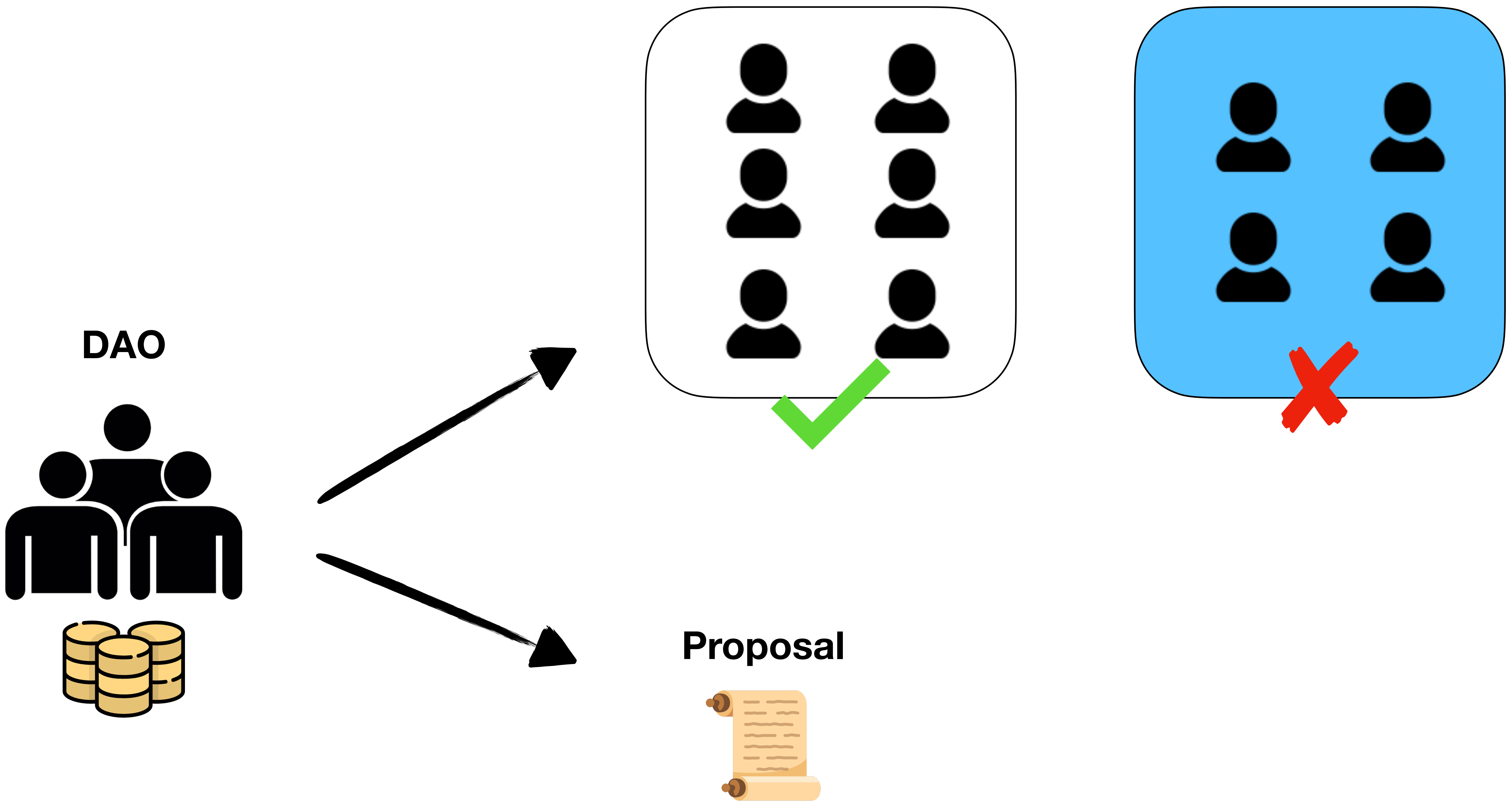
DAOs in practice



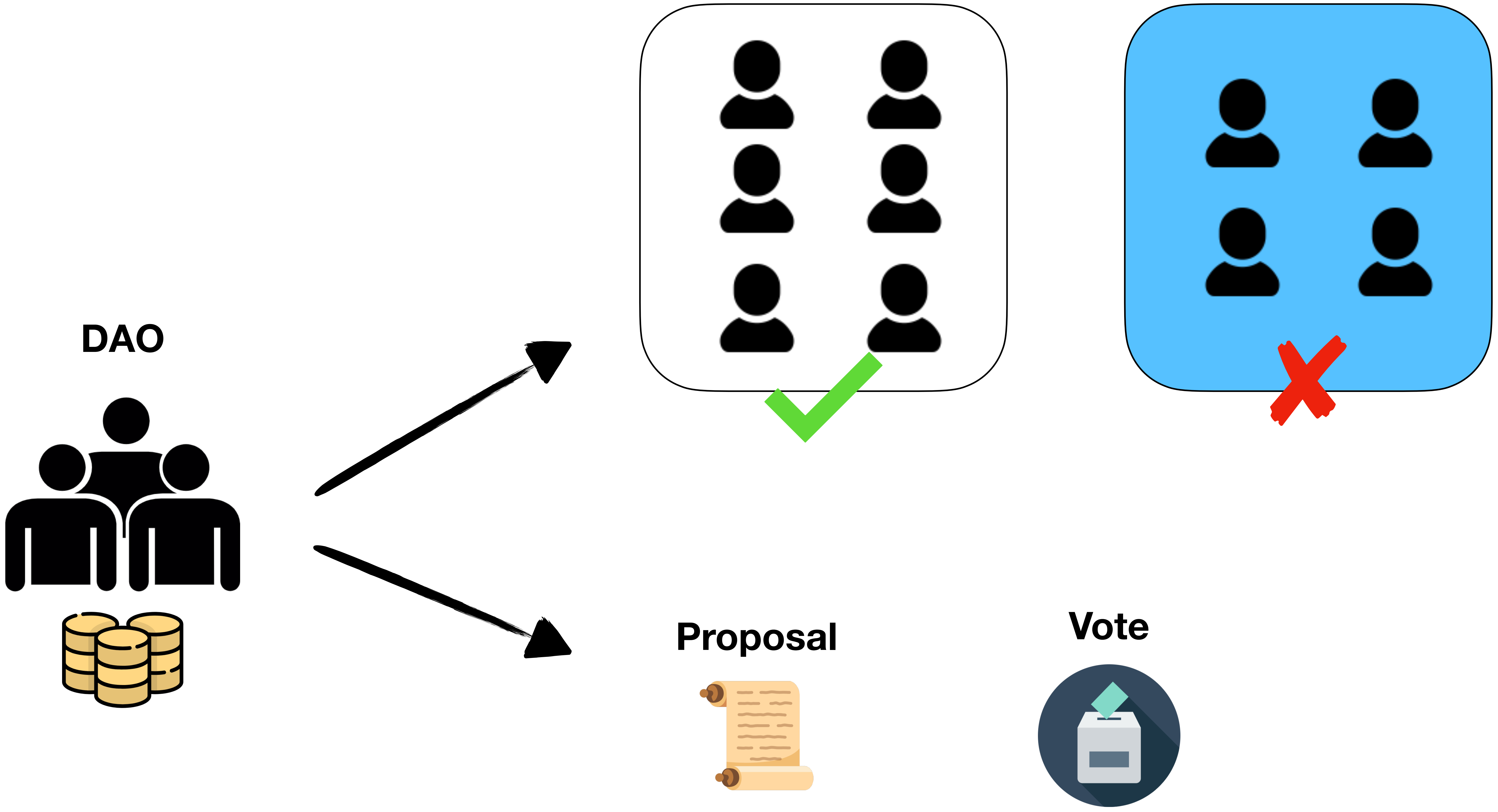
DAOs in practice



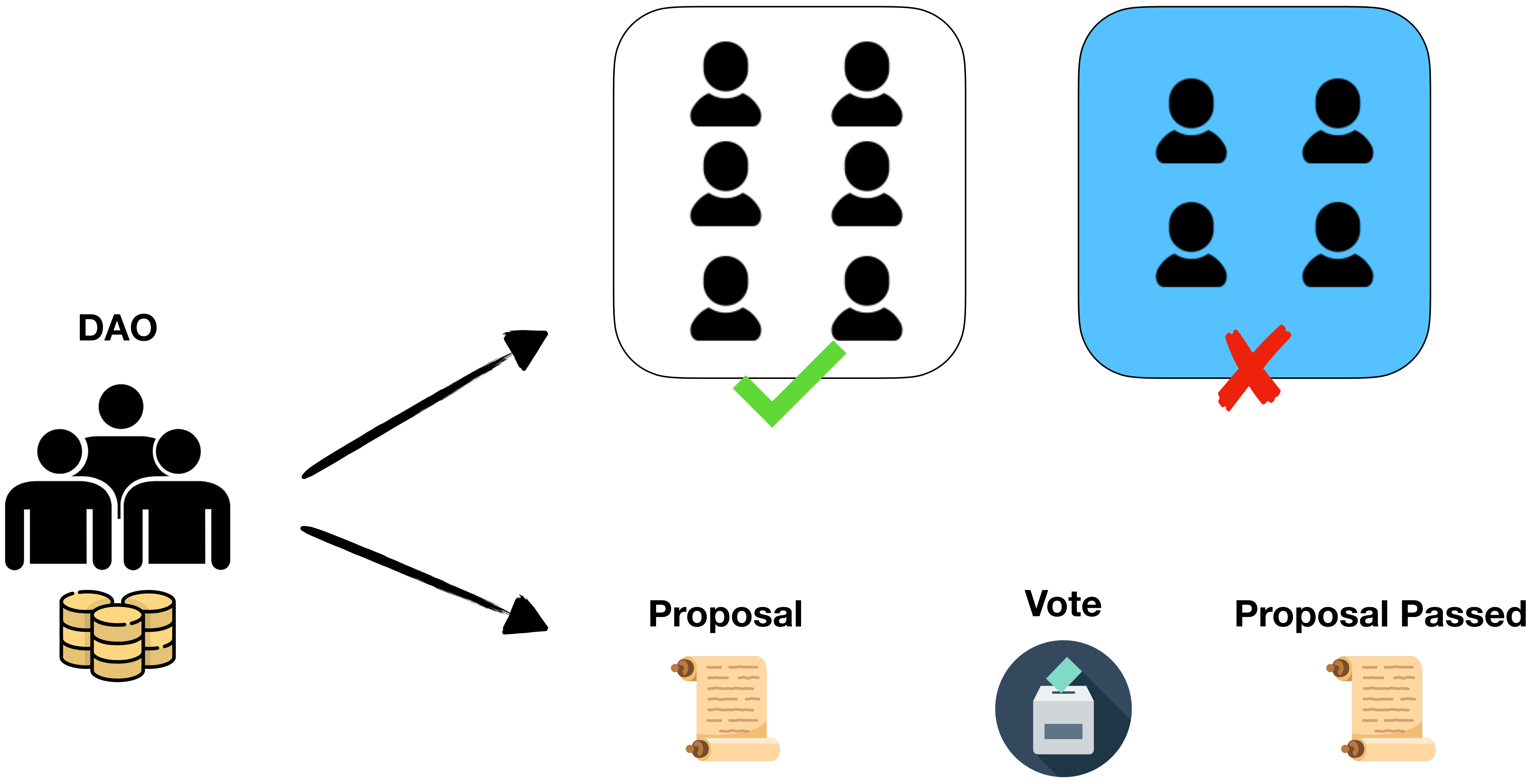
DAOs in practice



DAOs in practice



DAOs in practice



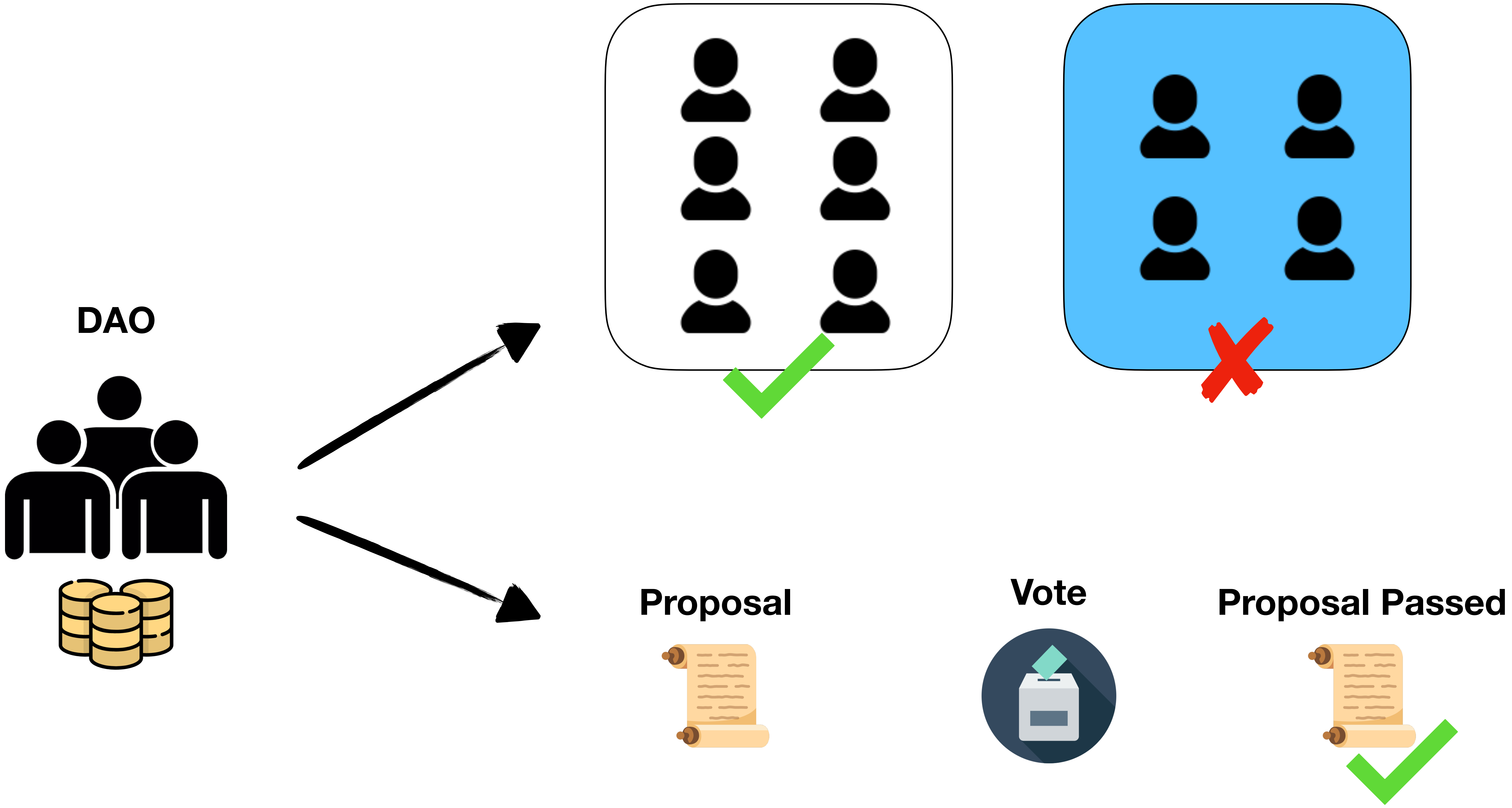
DAO

Proposal

Vote

Proposal Passed

DAOs in practice



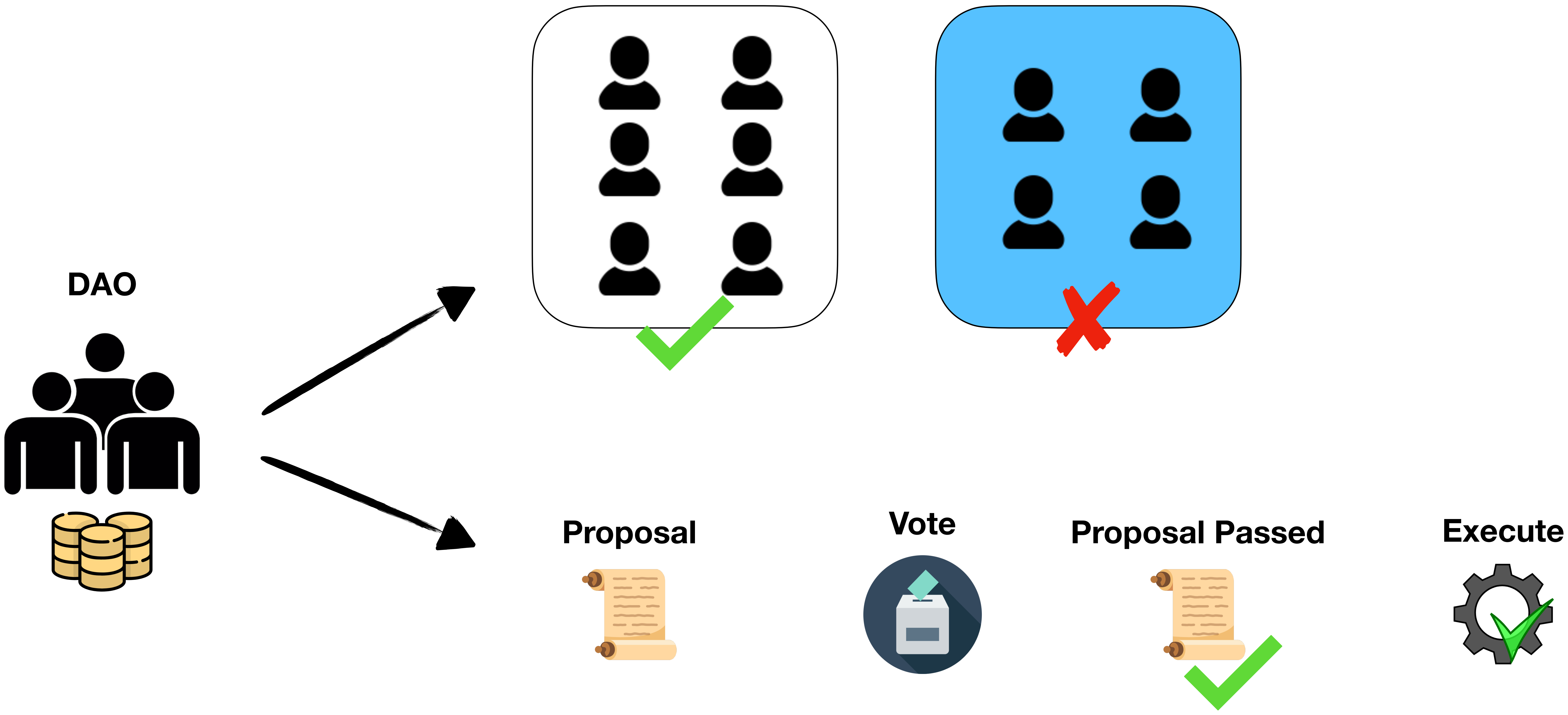
DAO

Proposal

Vote

Proposal Passed

DAOs in practice



DAO

Proposal

Vote

Proposal Passed

Execute

Who can participate in governance?

Registration

- Owning Governance Tokens is not enough!!!
- Most protocols (39 out of 51) require registration

Registration

- Why require Registration?
  - Gatekeeping
  - Size of the electorate

Registration

- Why require Registration?
  - Gatekeeping 👤
  - Size of the electorate

Registration

- Why require Registration?
    - Gatekeeping
    - Size of the electorate

Registration

- Why require Registration?
  - Gatekeeping

  - Size of the electorate

Registration

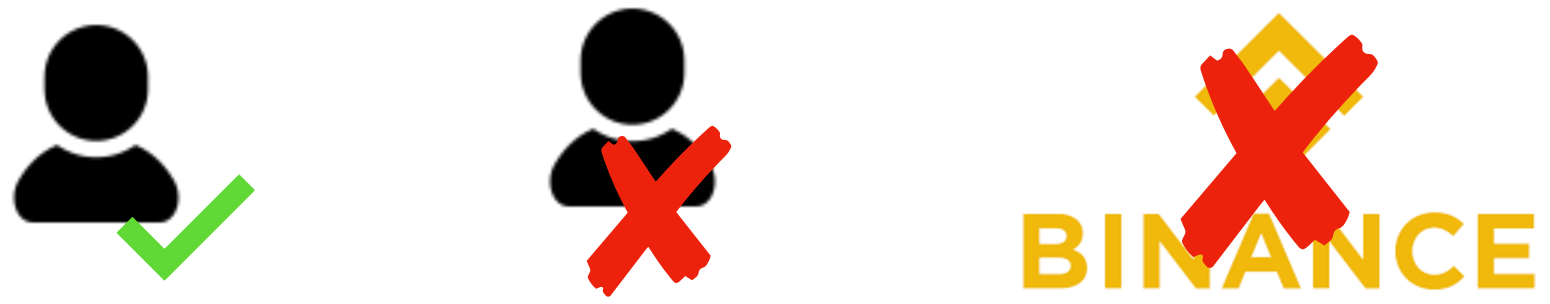
- Why require Registration?
  - Gatekeeping 👤✓ 👤✗
  - Size of the electorate

Registration

- Why require Registration?
  - Gatekeeping ✓ ✗ BINANCE
  - Size of the electorate

Registration

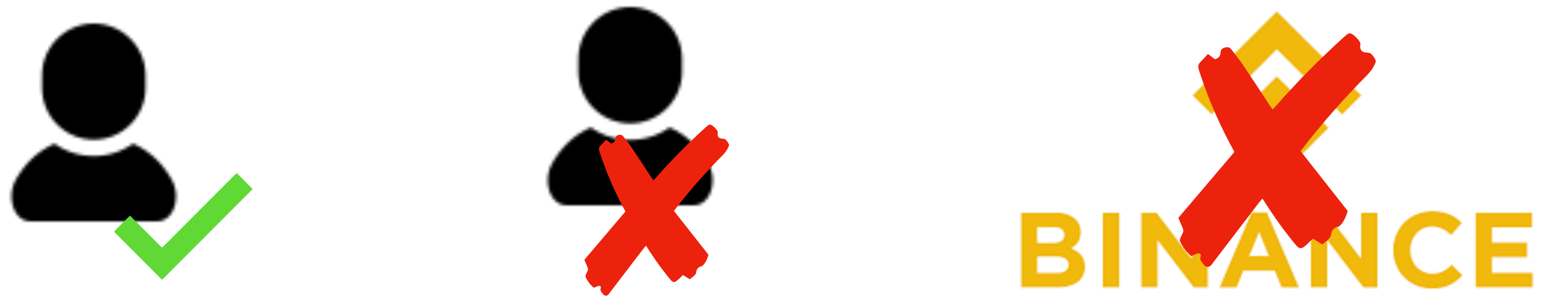
- Why require Registration?
  - Gatekeeping

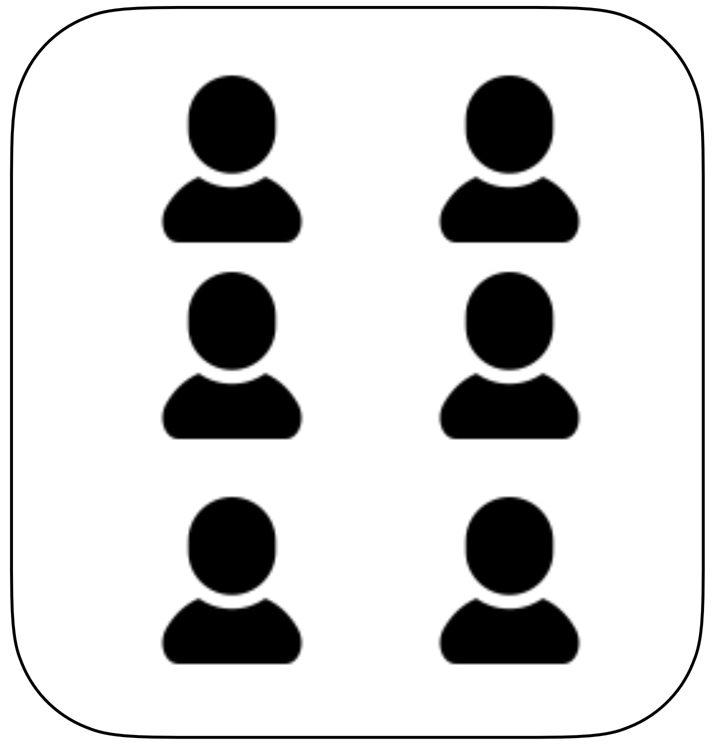
  - Size of the electorate

Registration

- Why require Registration?
  - Gatekeeping



  - Size of the electorate



Registration: Anonymous vs Verified

Registration: Anonymous vs Verified

Anonymous

37 total

Registration: Anonymous vs Verified

Anonymous

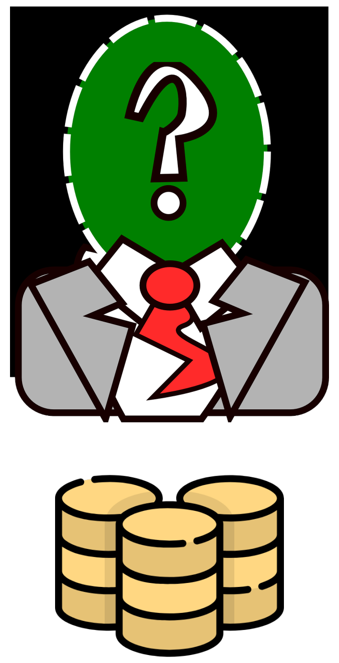
37 total

Verified

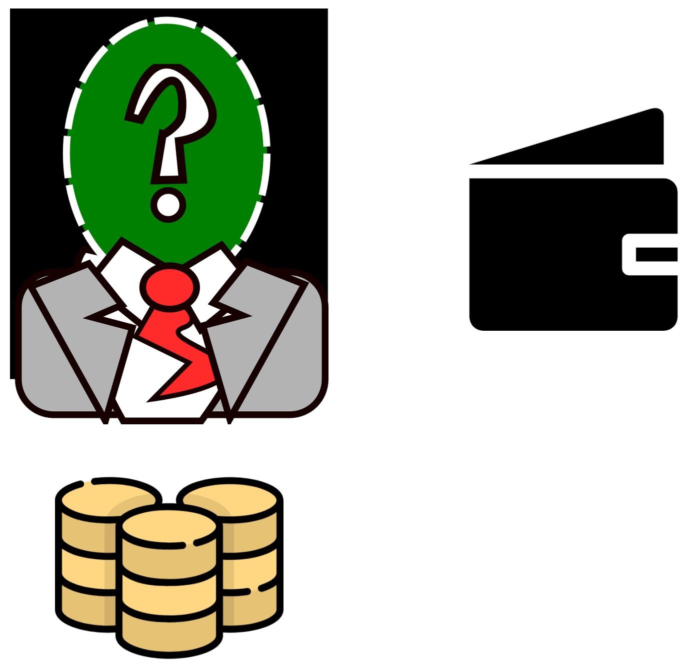
2 total

Anonymous Registration

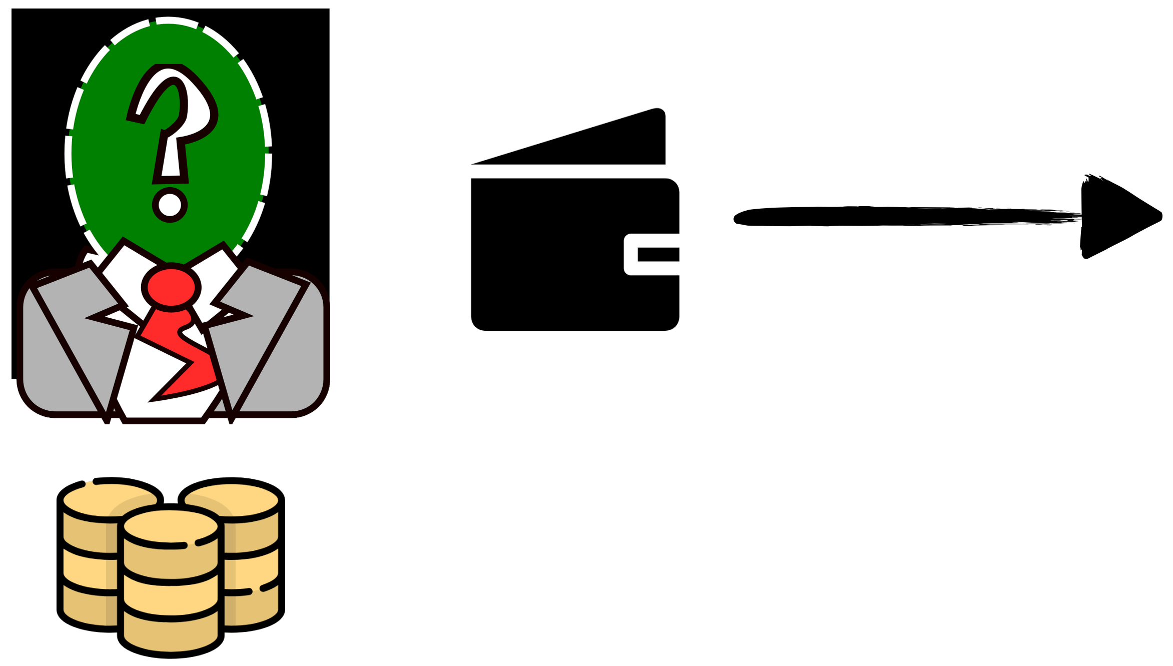
Anonymous Registration



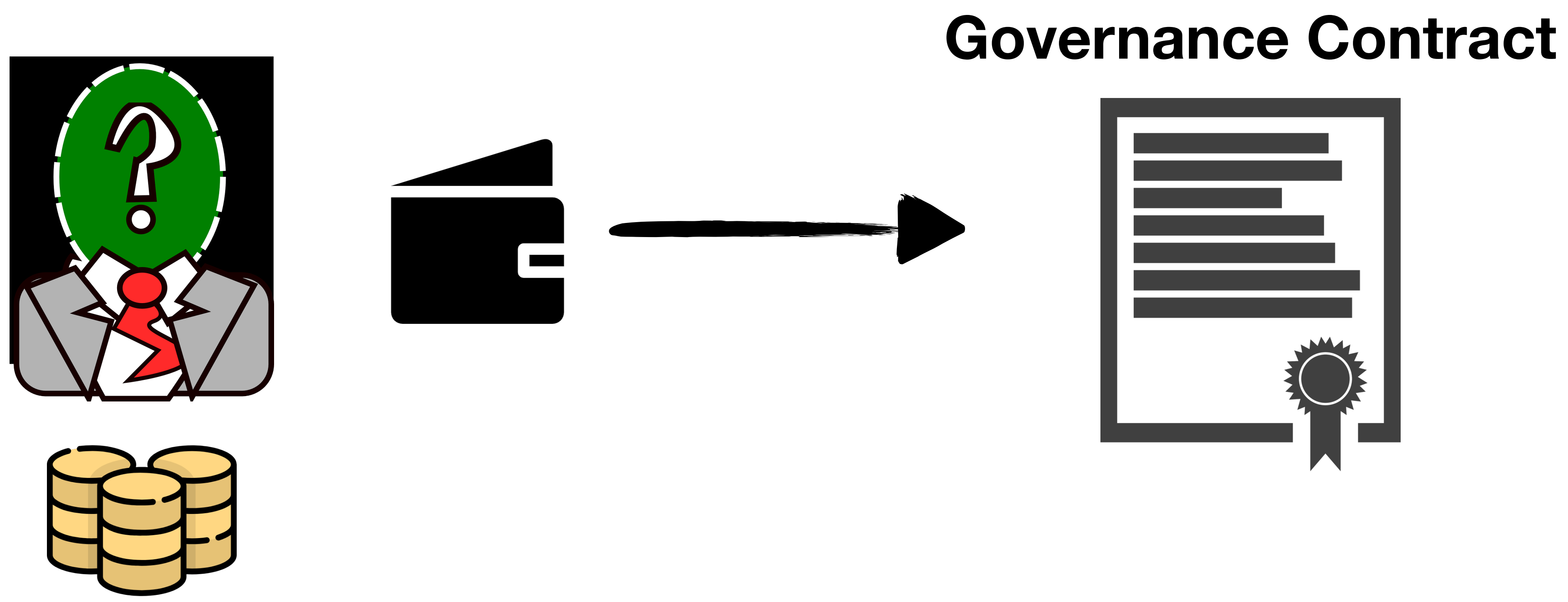
Anonymous Registration



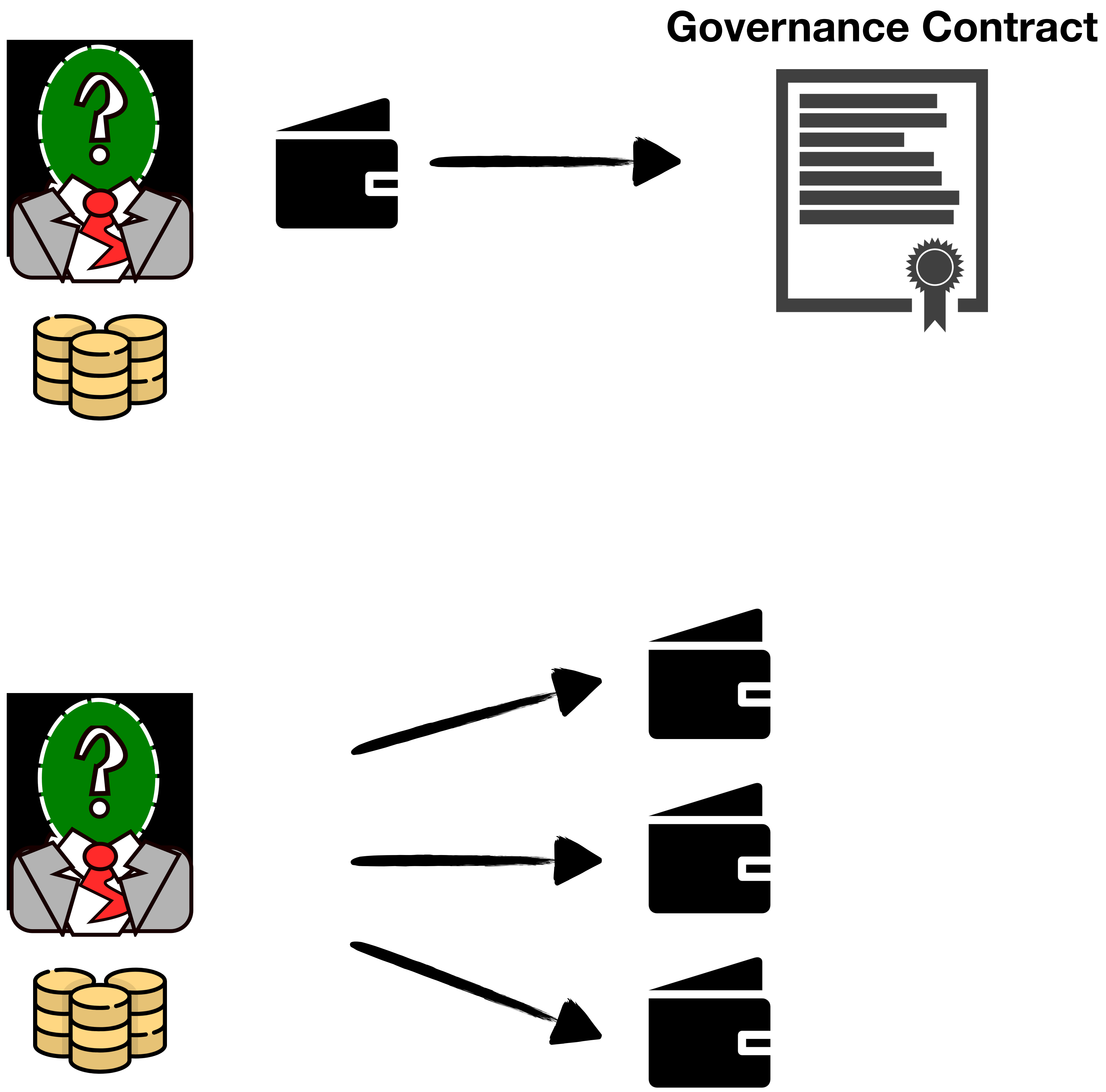
Anonymous Registration



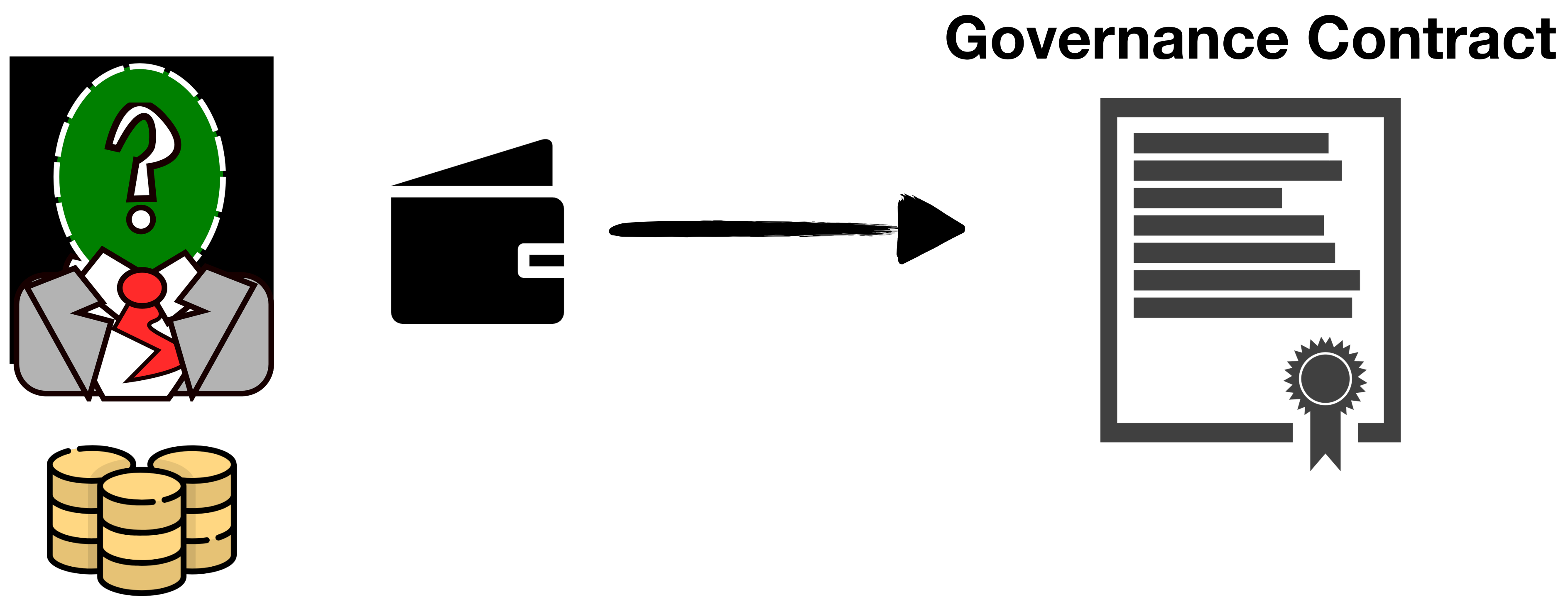
Anonymous Registration



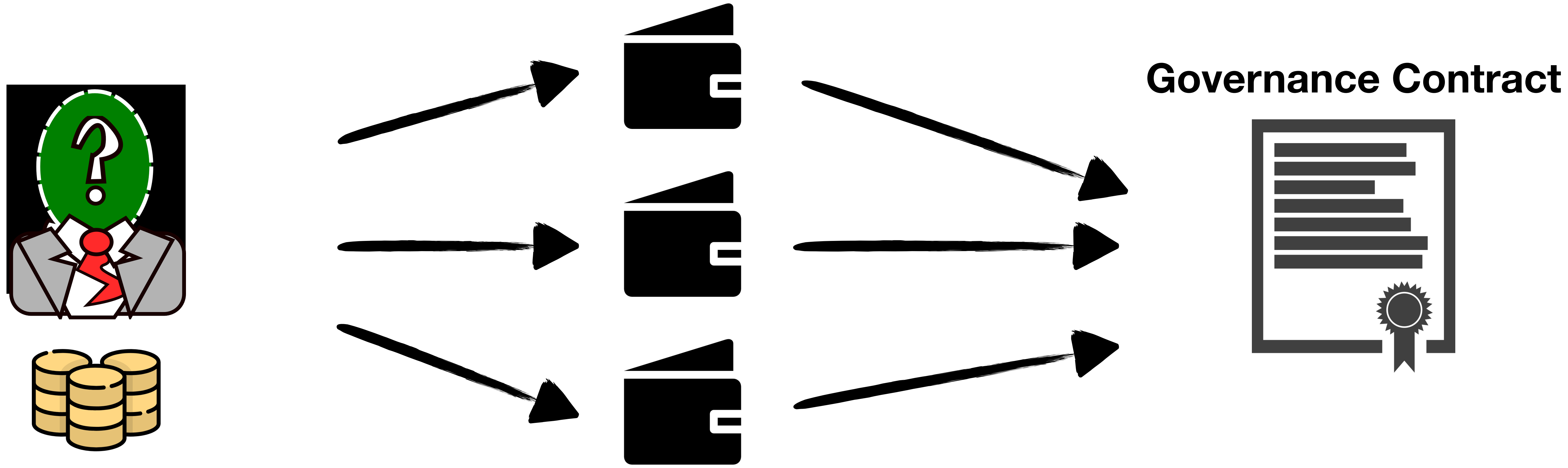
Anonymous Registration



Anonymous Registration



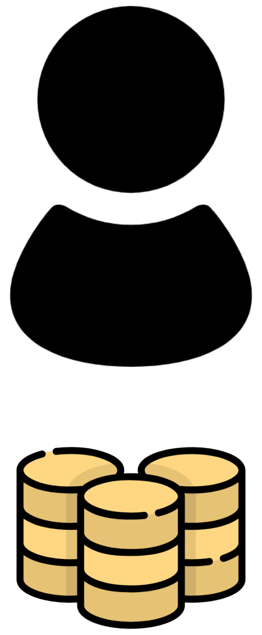
Governance Contract



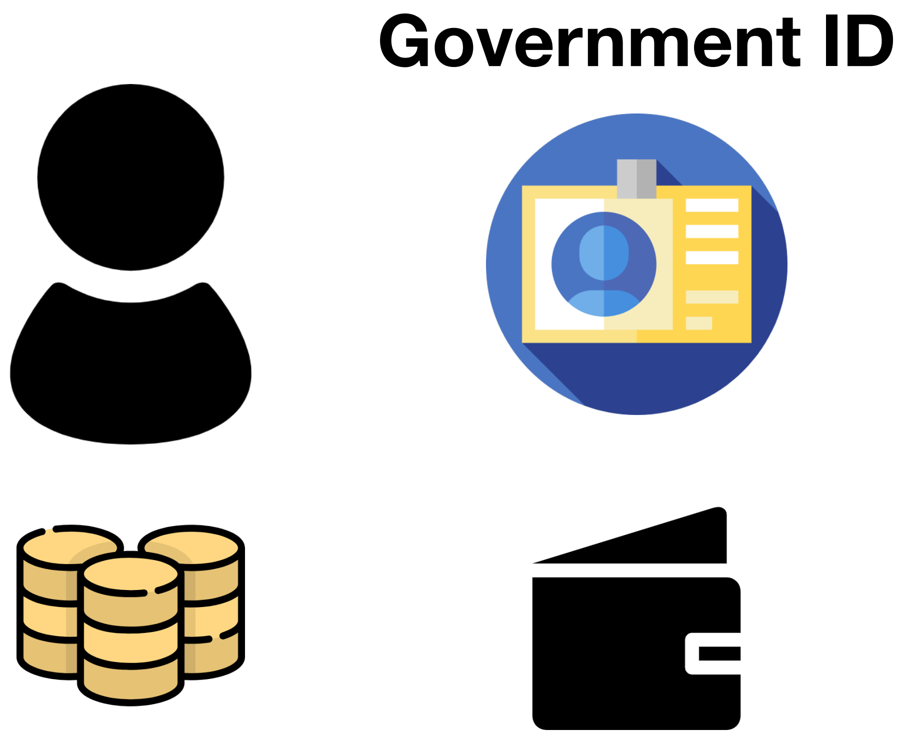
Governance Contract

Verified Registration

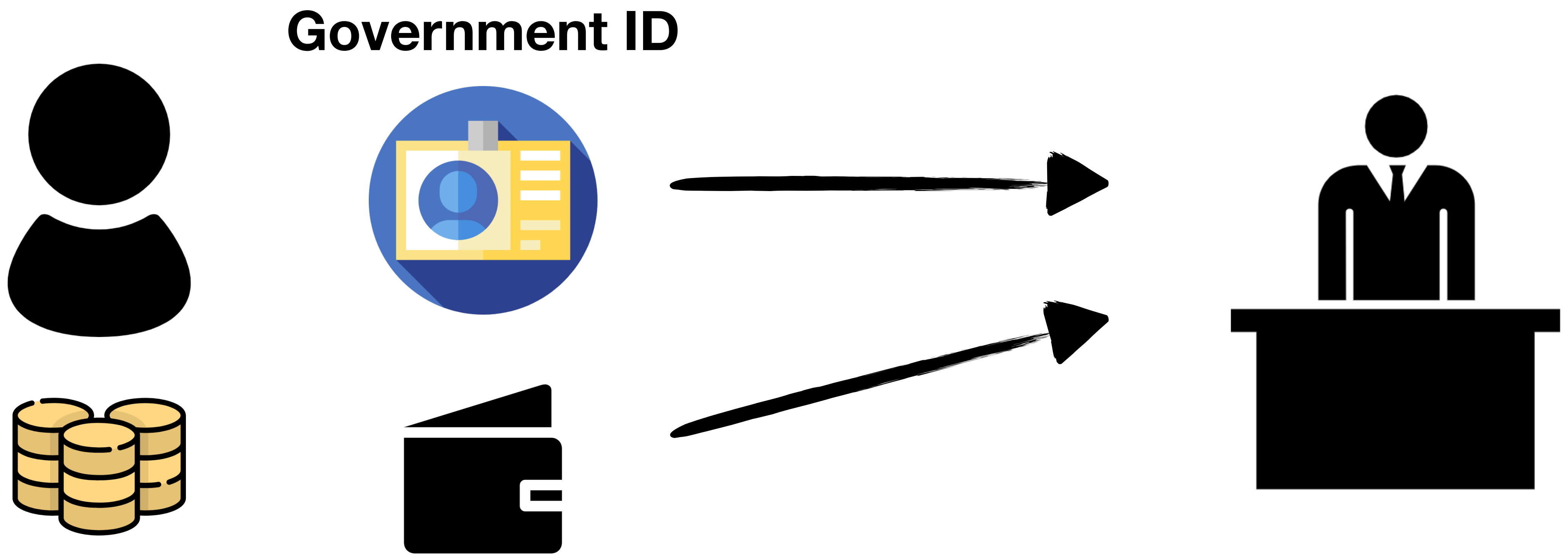
Verified Registration



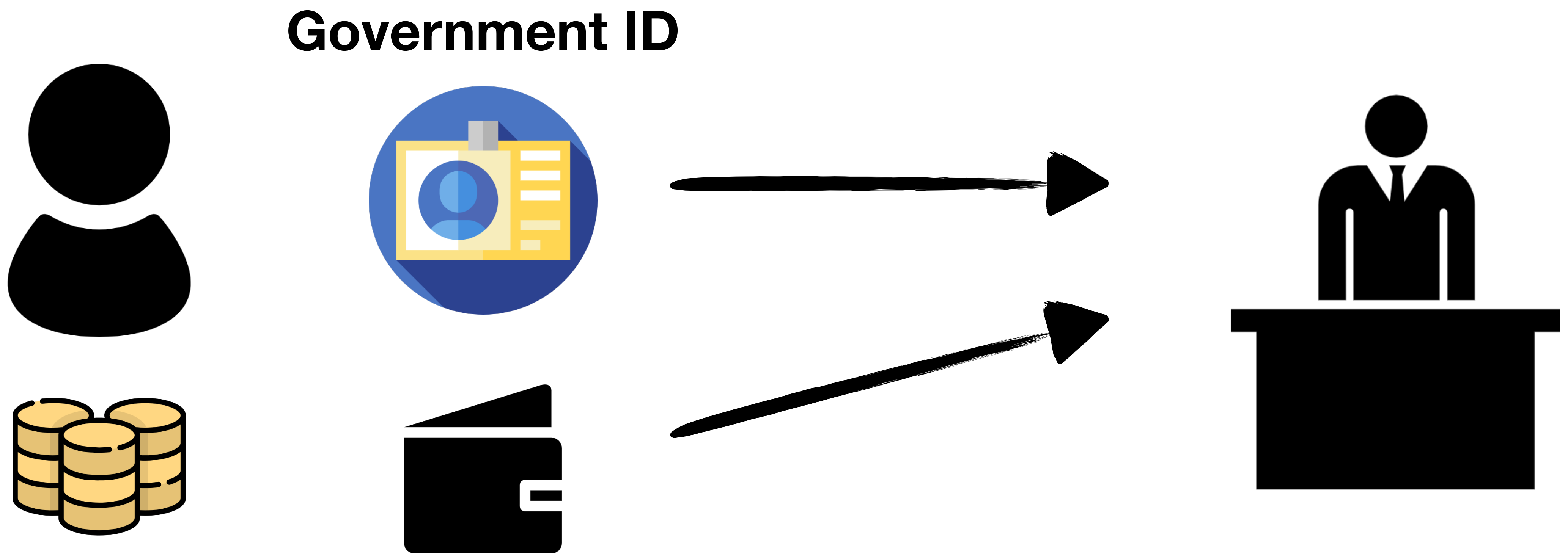
Verified Registration



Verified Registration



Verified Registration



CENTRALIZED

Registration: Token Holding vs. Staking

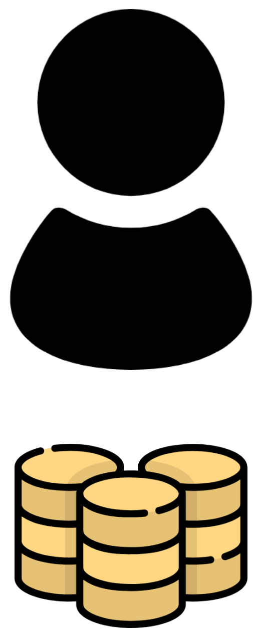
- Token Holding

Registration: Token Holding vs. Staking

- Token Holding

Registration: Token Holding vs. Staking

- Token Holding



Registration: Token Holding vs. Staking

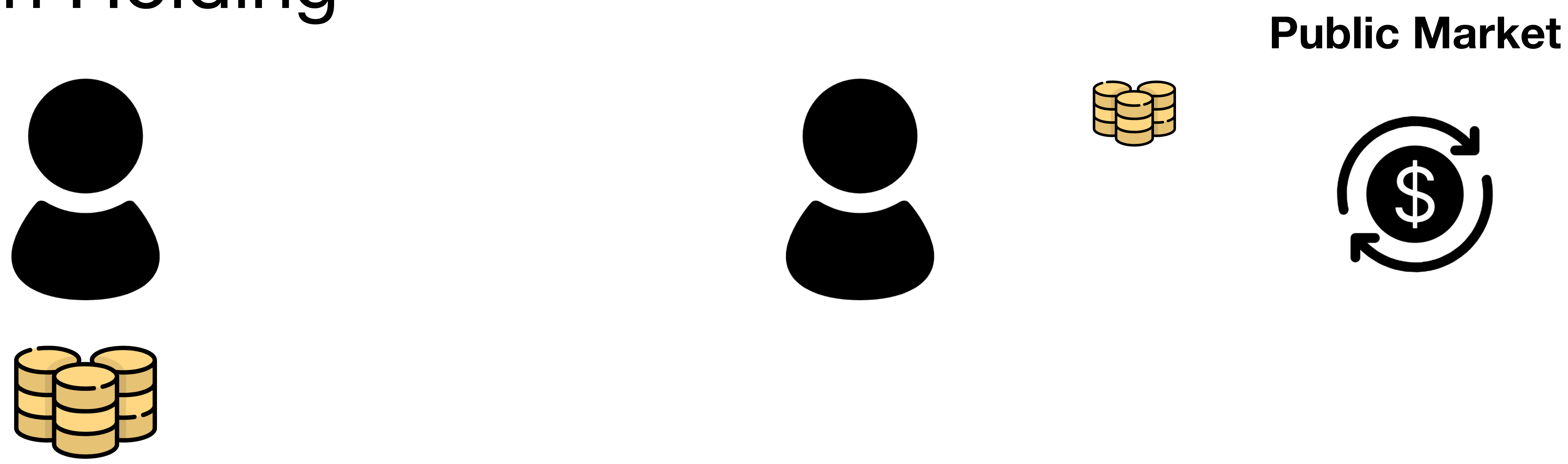
- Token Holding

Registration: Token Holding vs. Staking

- Token Holding

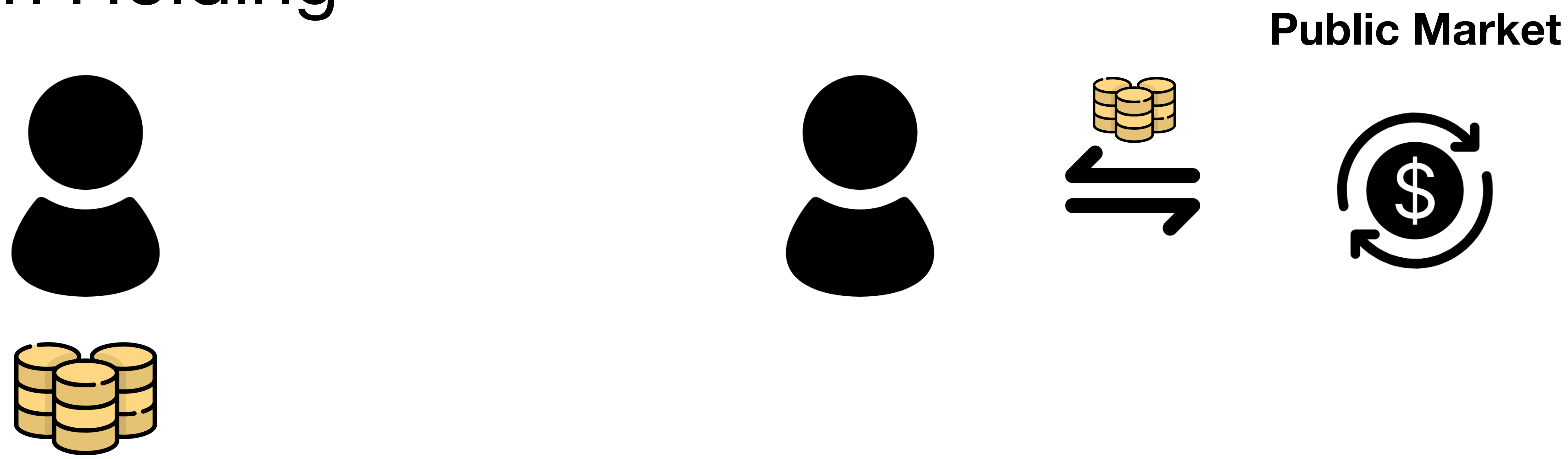
Registration: Token Holding vs. Staking

- Token Holding



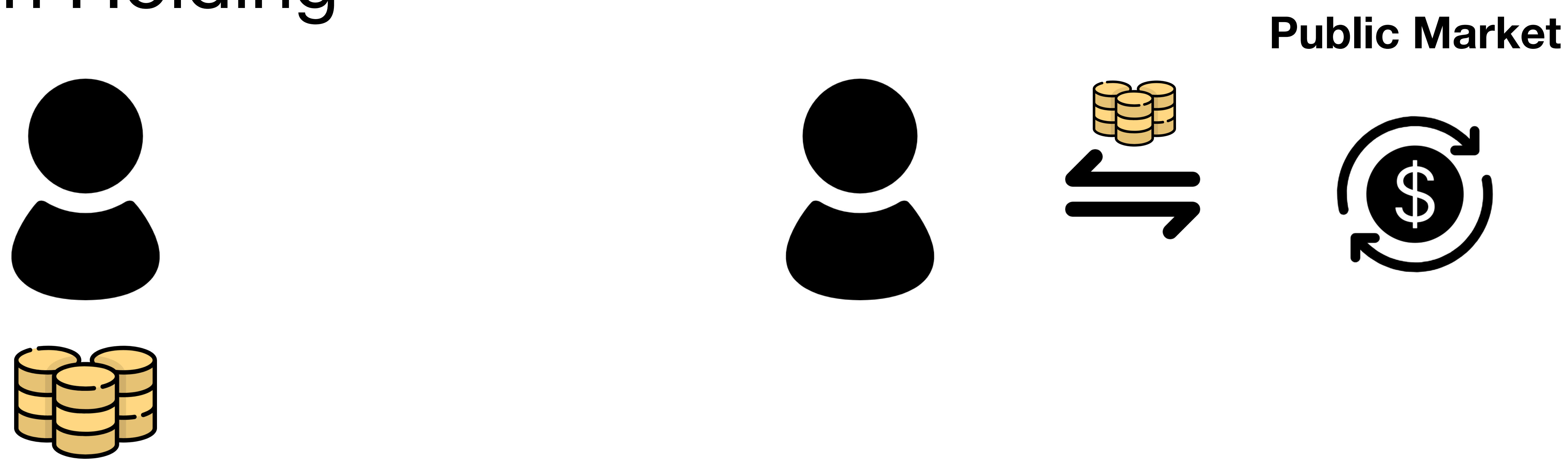
Registration: Token Holding vs. Staking

- Token Holding

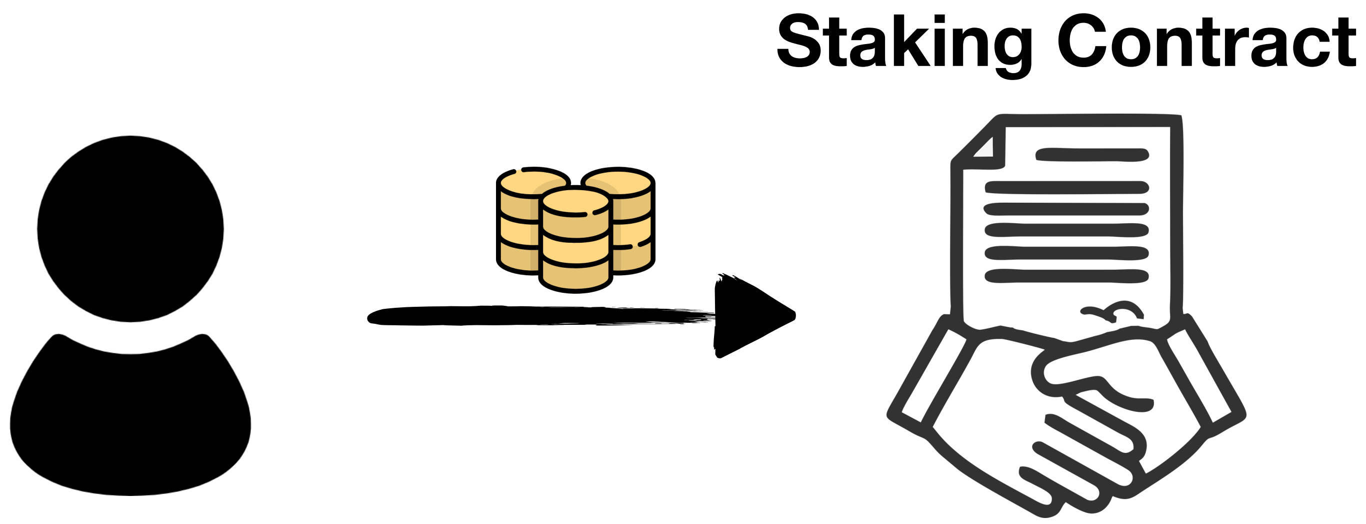


Registration: Token Holding vs. Staking

- Token Holding



- Token Staking

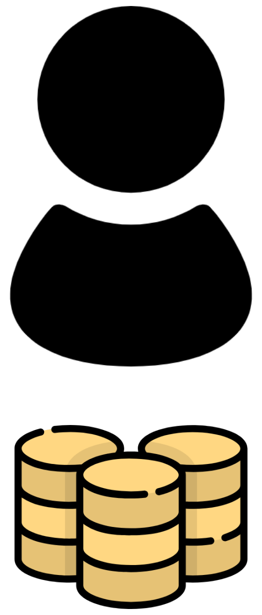


Governance and Monetary Rights

- Governance Tokens have both **governance** and **monetary** rights !!!

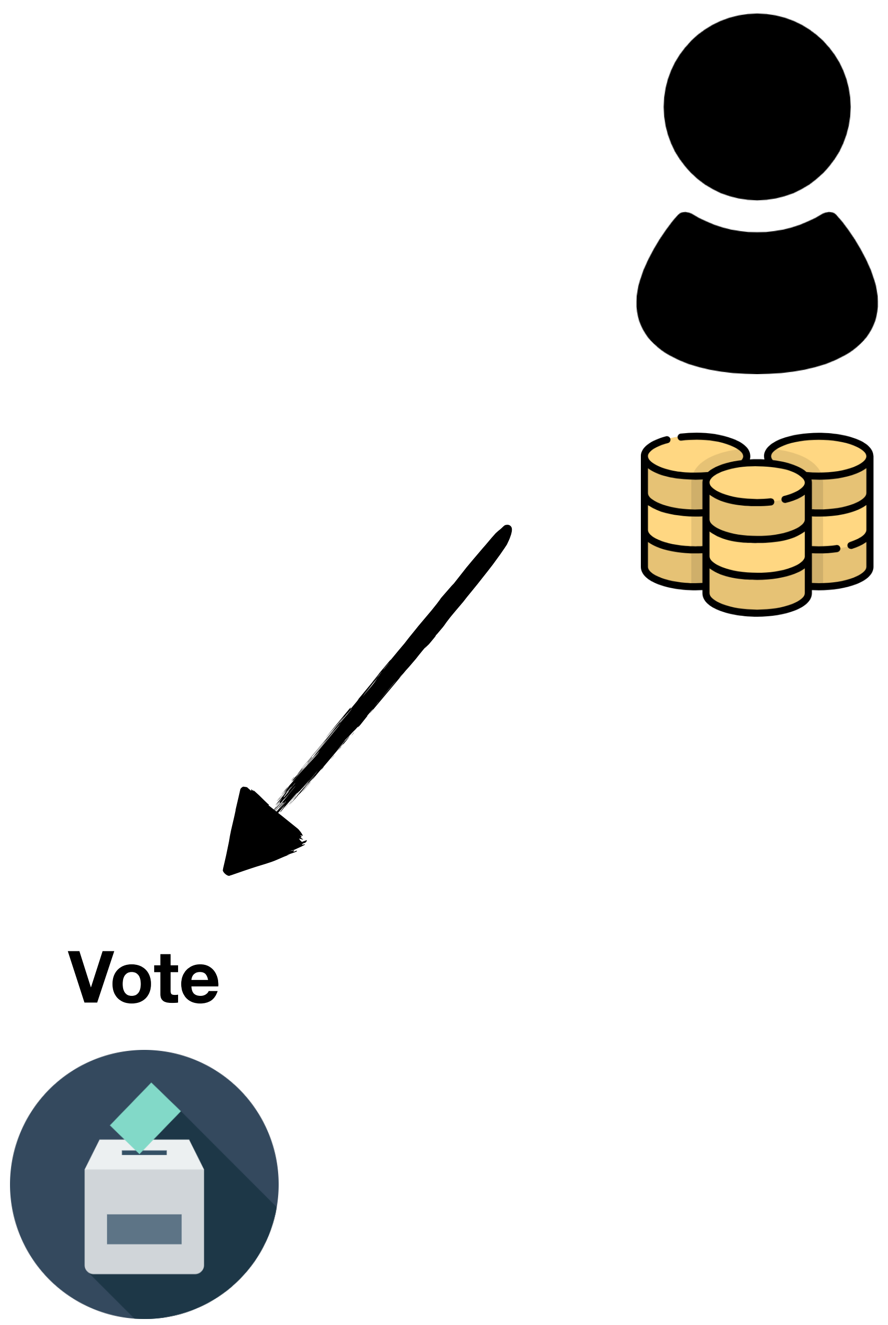
Governance and Monetary Rights

- Governance Tokens have both **governance** and **monetary** rights !!!



Governance and Monetary Rights

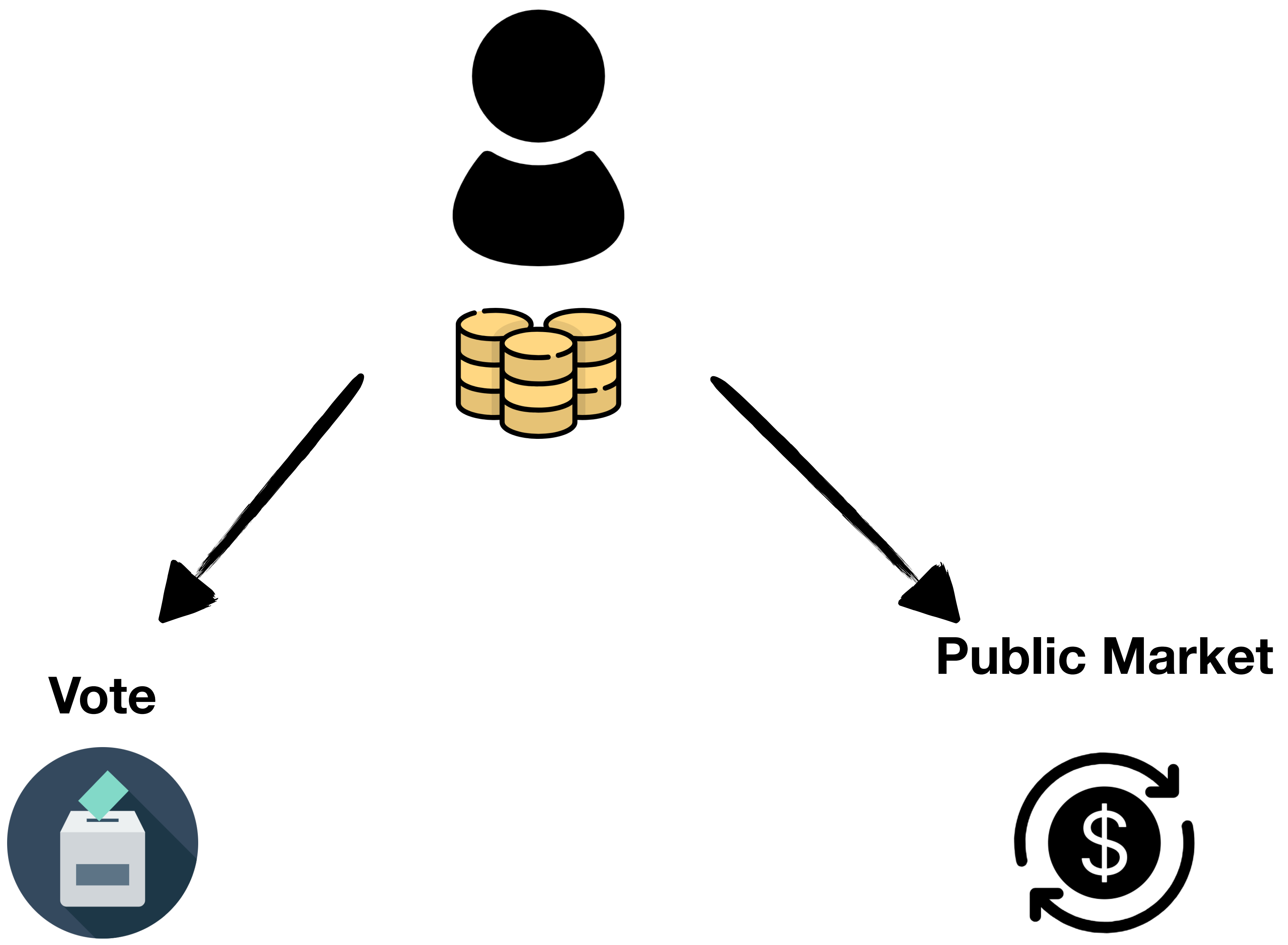
- Governance Tokens have both **governance** and **monetary** rights !!!



Vote

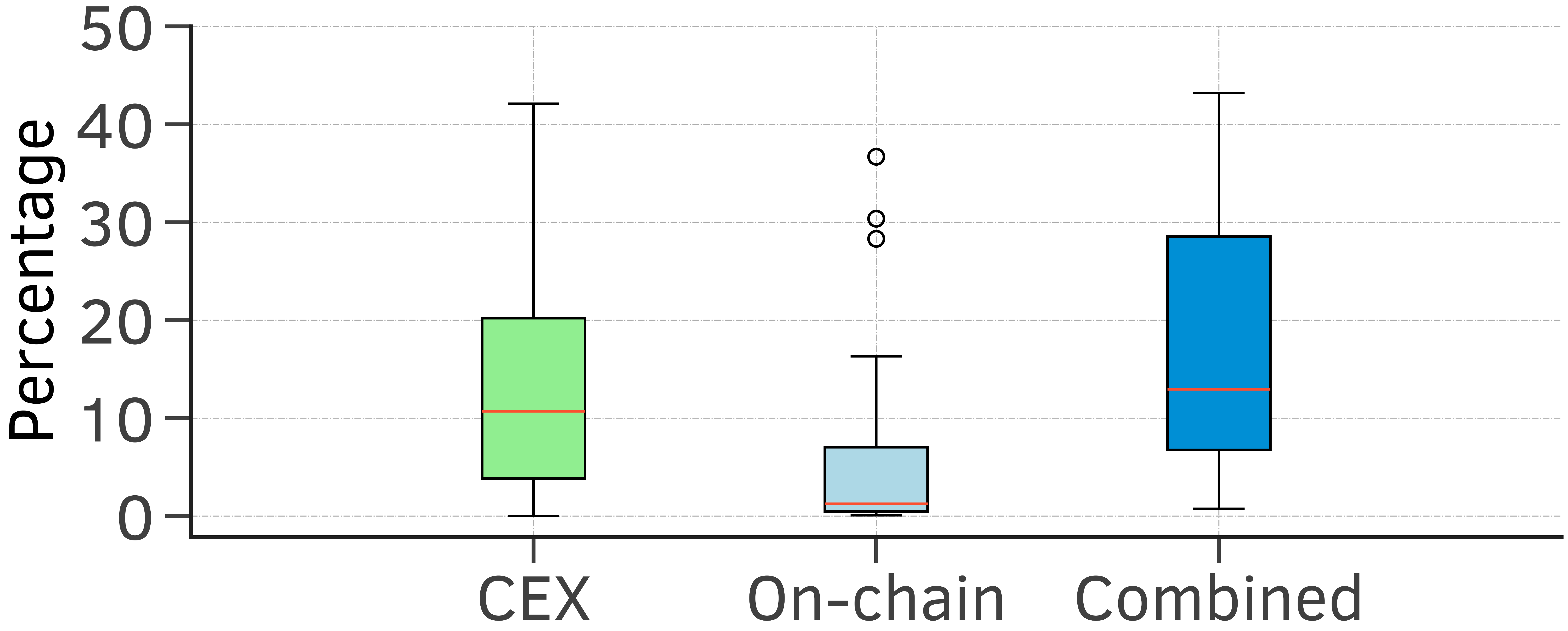
Governance and Monetary Rights

- Governance Tokens have both **governance** and **monetary** rights !!!



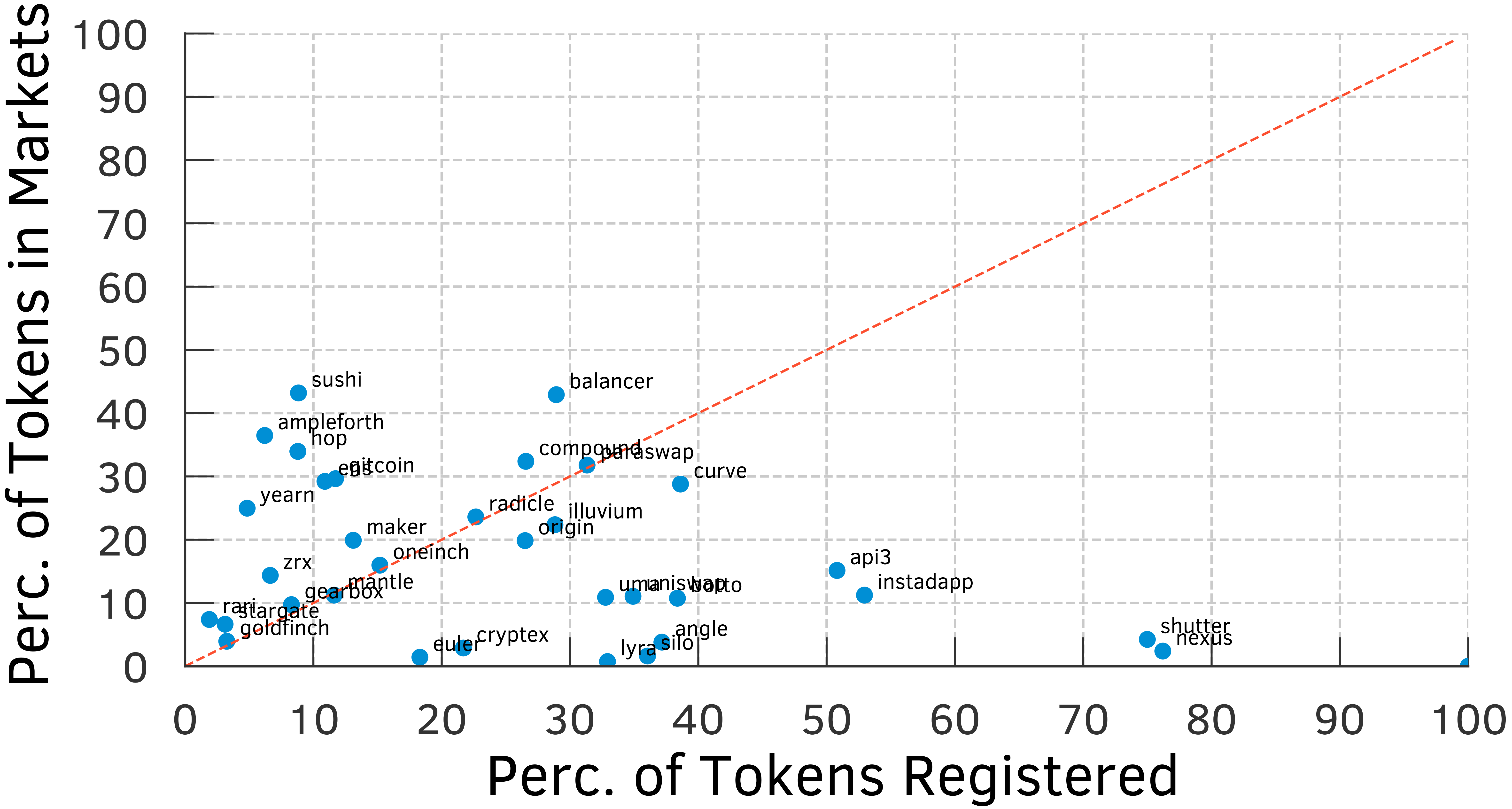
Public Markets

- Custodians own a lot of tokens



Public Markets

- For **44% of DAOs (16 of 36)**, there are more tokens in Markets than are registered to vote



Public Markets

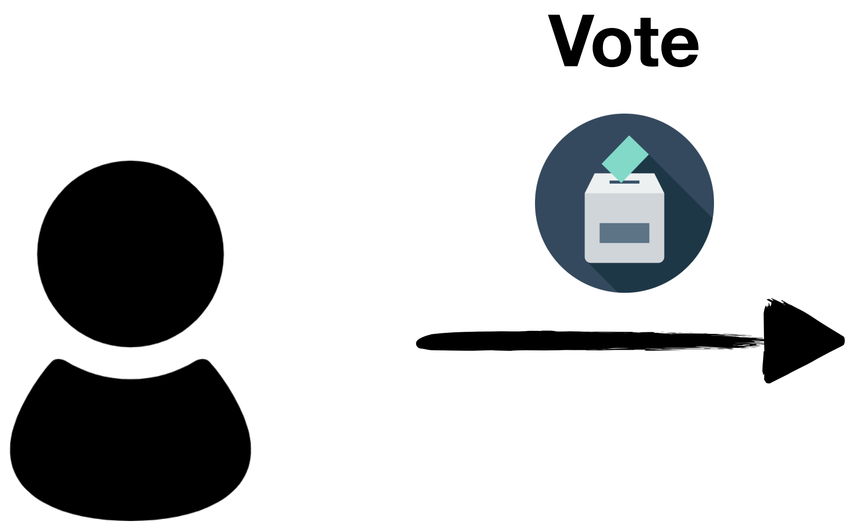
- Taking a real-world analogy, brokers allow users on their platform to vote

Public Markets

- Taking a real-world analogy, brokers allow users on their platform to vote

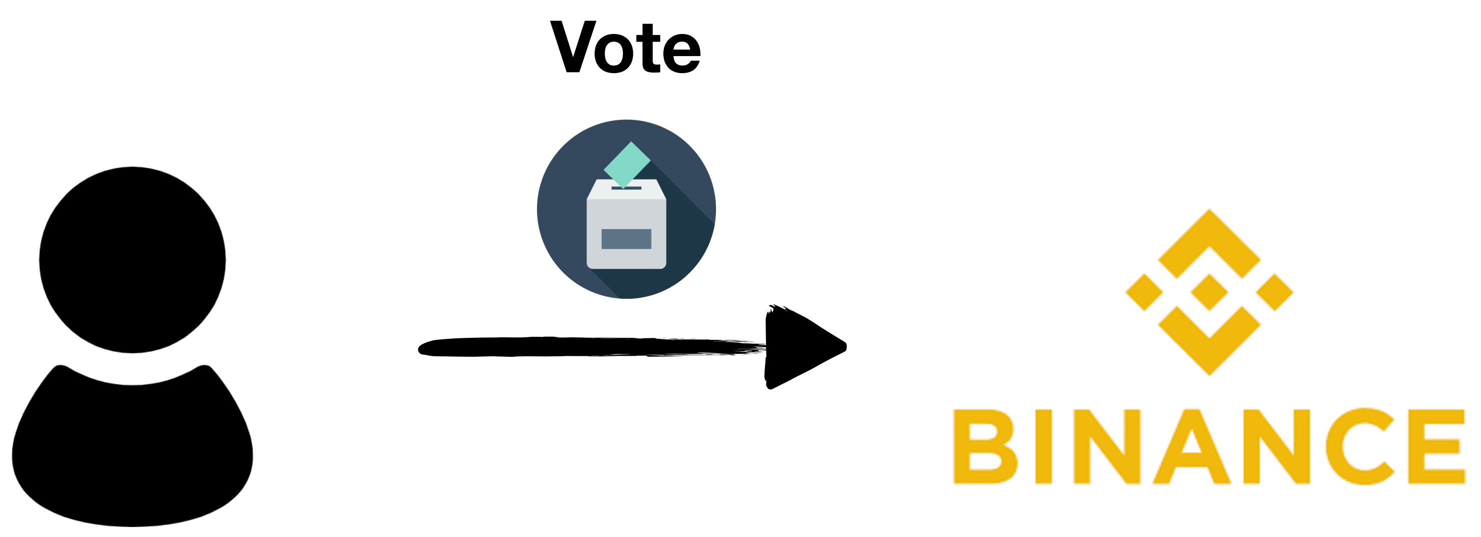
Public Markets

- Taking a real-world analogy, brokers allow users on their platform to vote



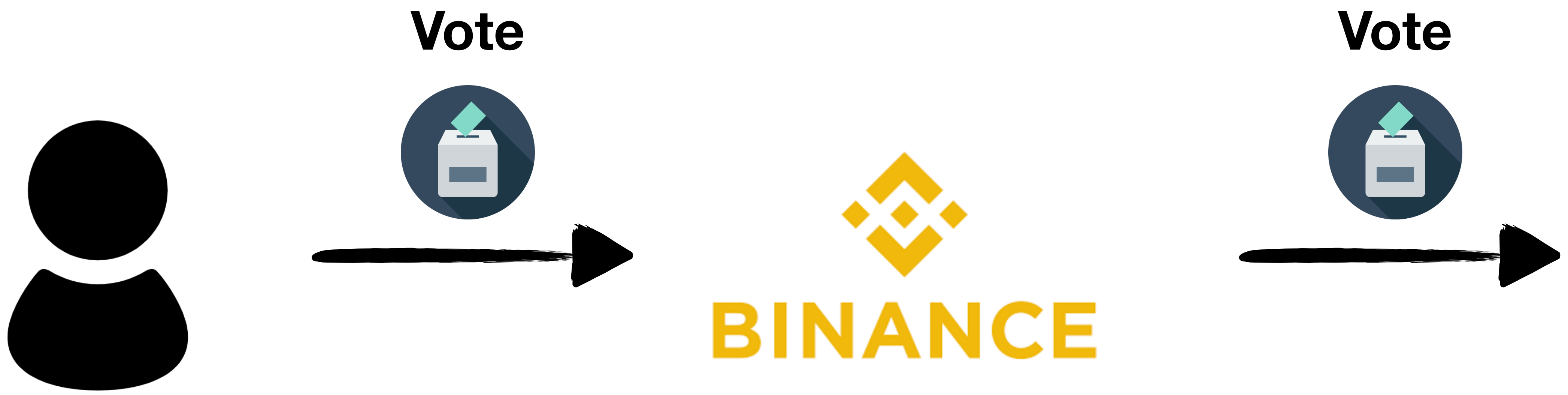
Public Markets

- Taking a real-world analogy, brokers allow users on their platform to vote



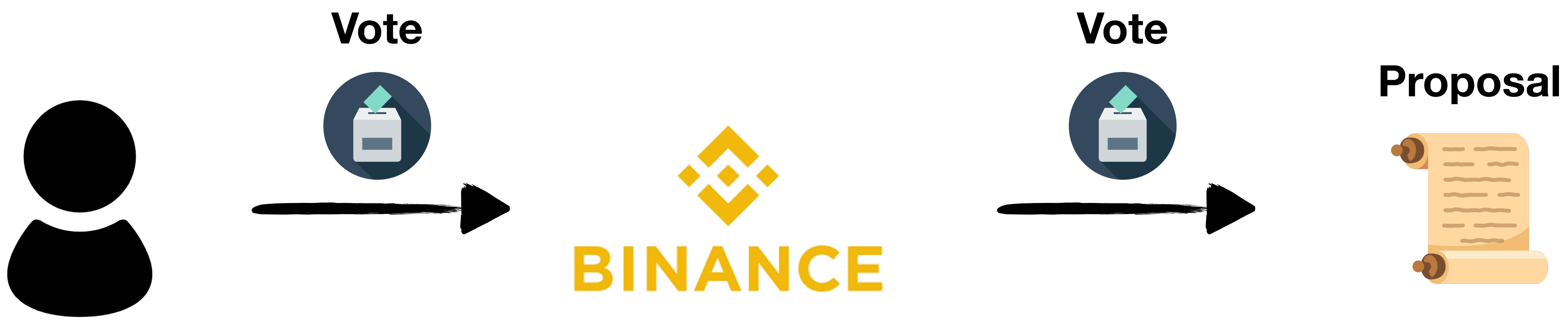
Public Markets

- Taking a real-world analogy, brokers allow users on their platform to vote



Public Markets

- Taking a real-world analogy, brokers allow users on their platform to vote

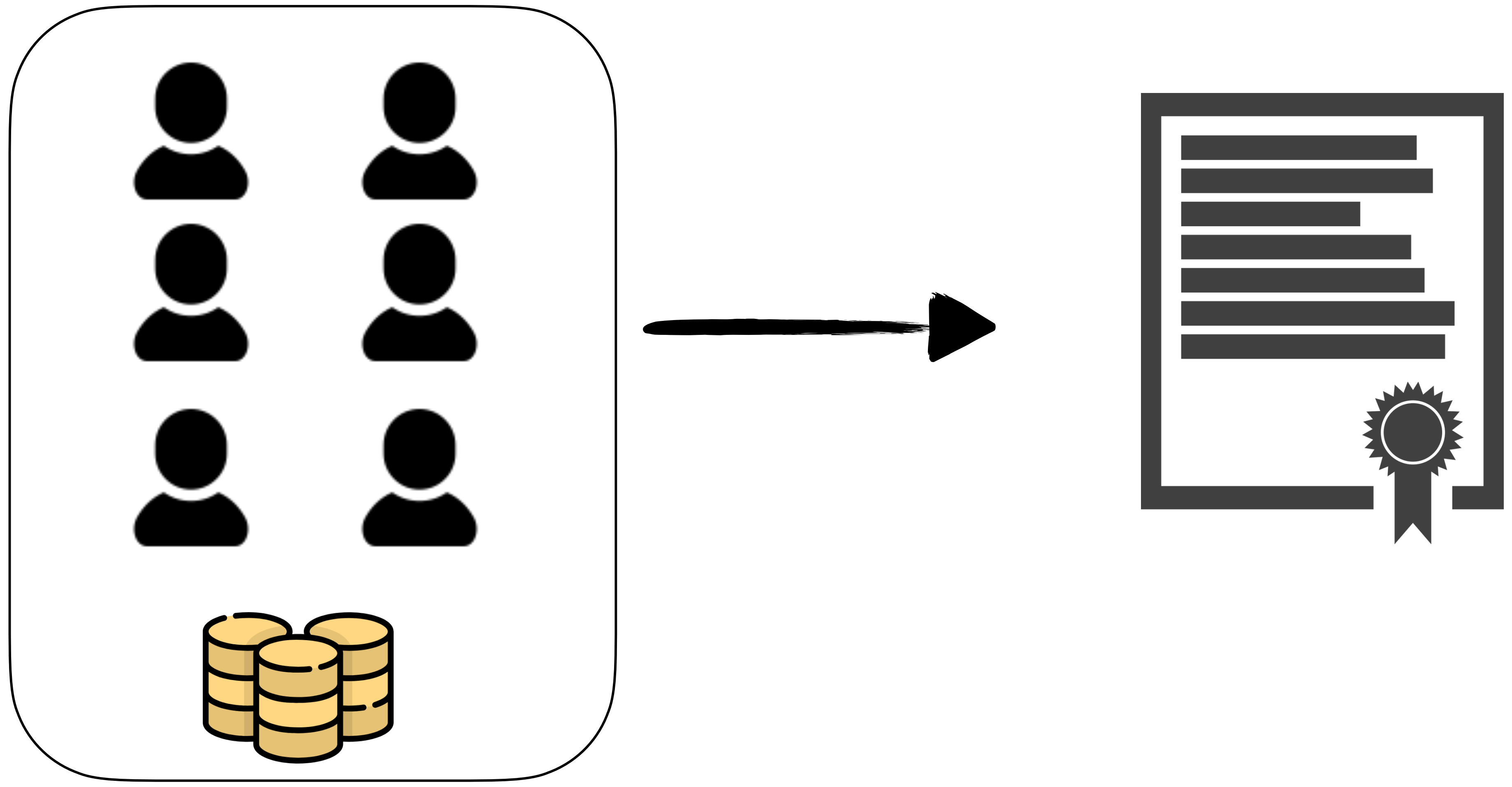


Voting via Proxies

- Direct Voting
- Delegated Voting
- Representative Voting

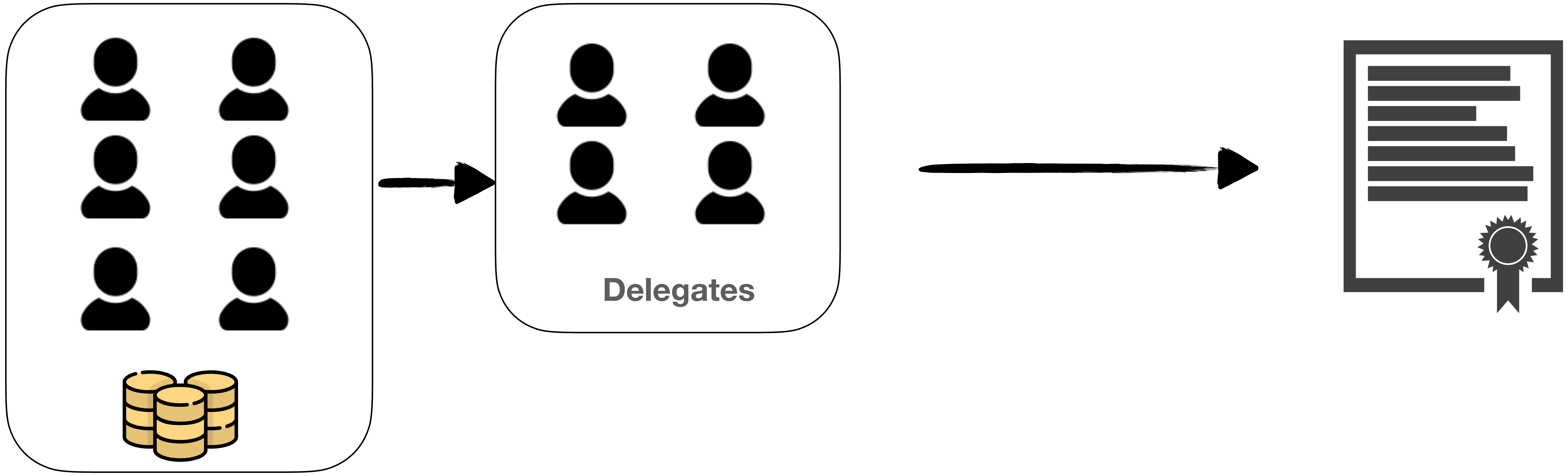
Voting via Proxies

- Direct Voting



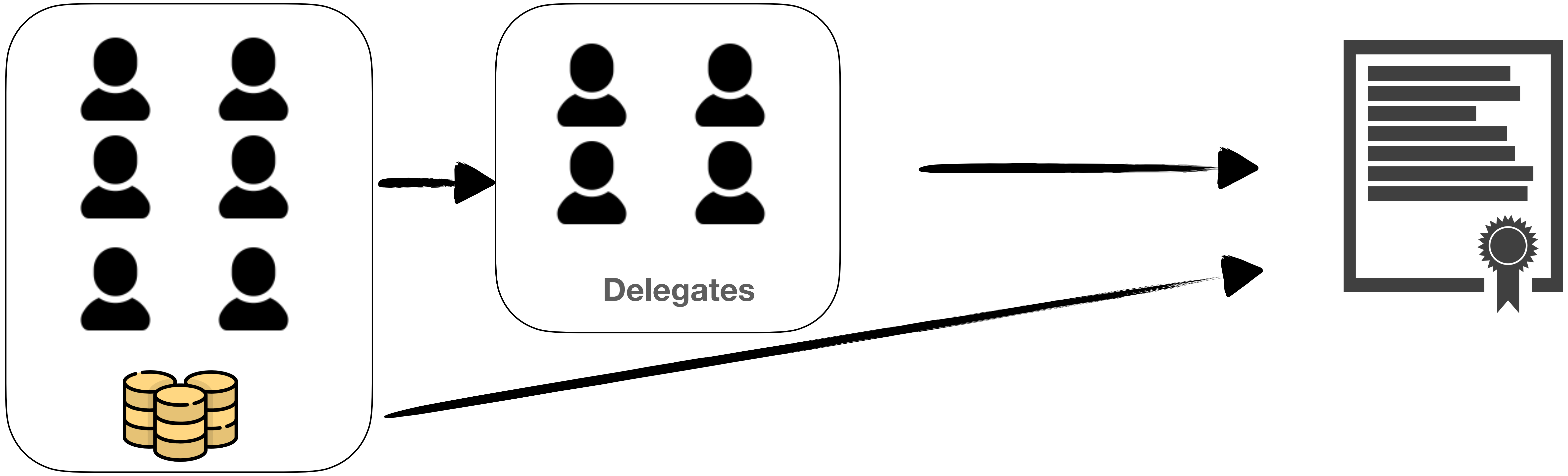
Voting via Proxies

- Delegated Voting



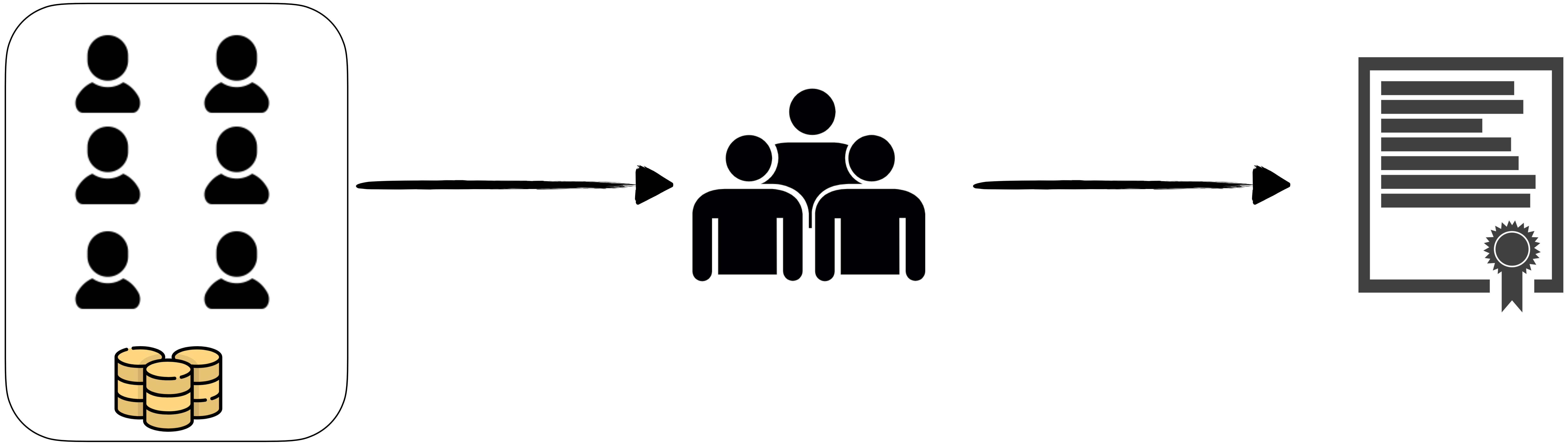
Voting via Proxies

- Most DAOs have both Direct and Delegated Voting
- Only 7 DAOs allow for only direct voting



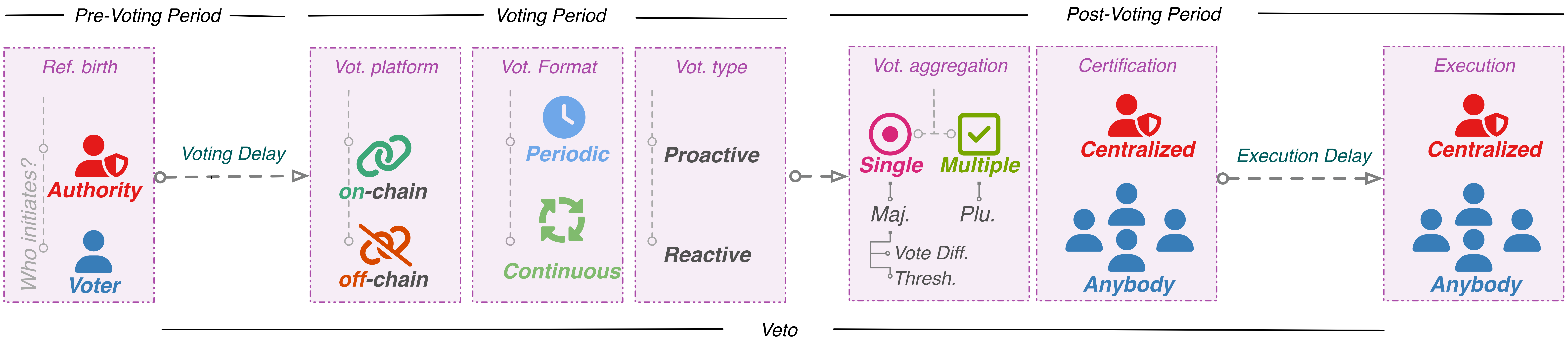
Voting via Proxies

- Representative Voting
- Only 3 DAOs use this

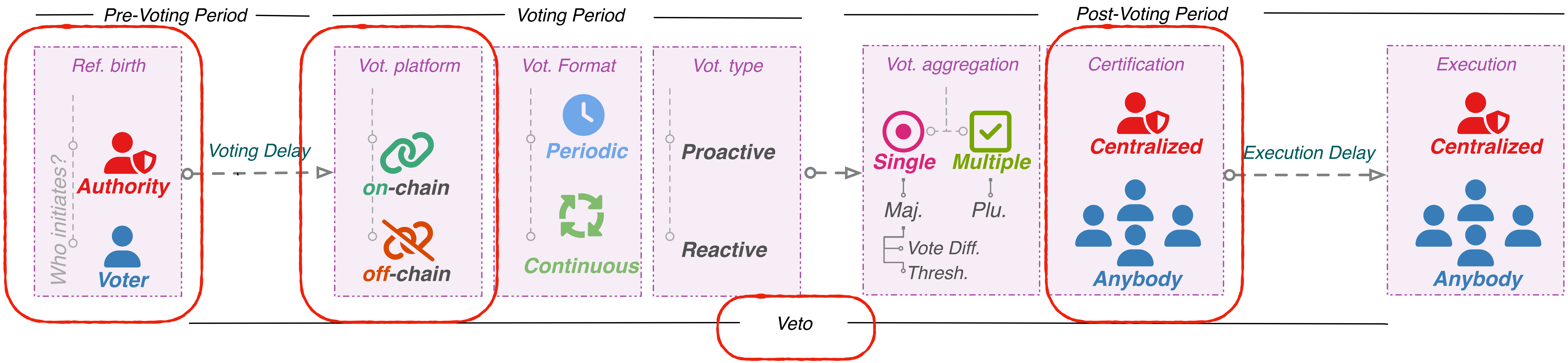


How is governance power exercised?

Lifecycle of a proposal



Lifecycle of a proposal

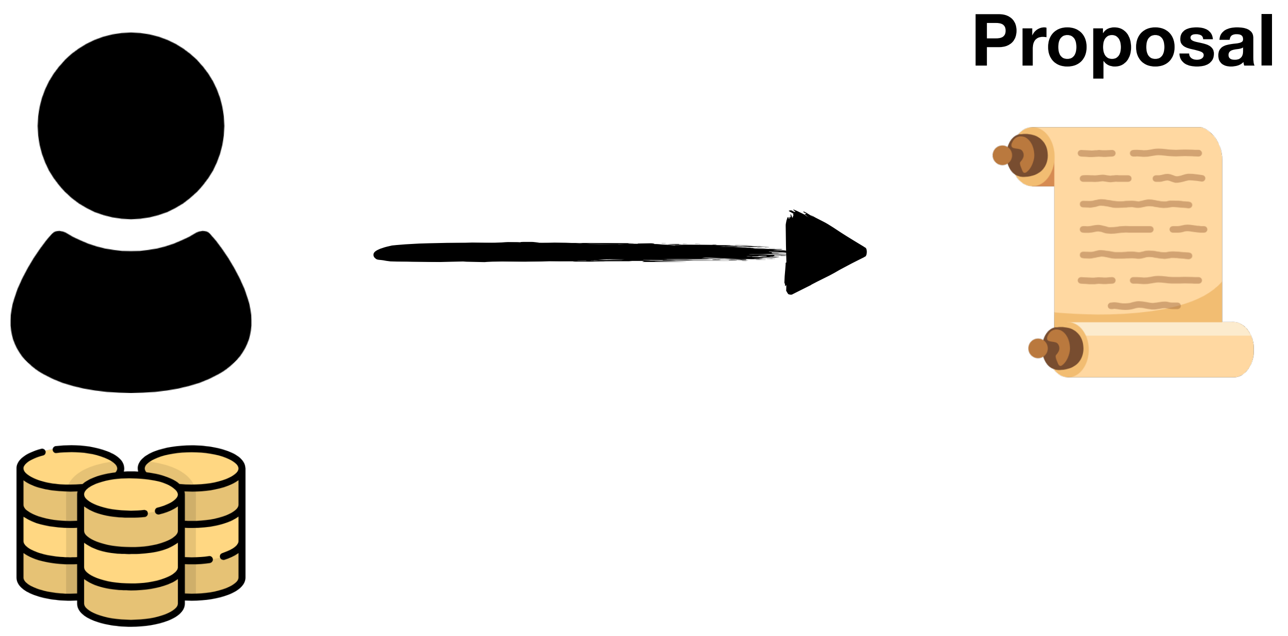


Pre-Voting Period

- Who initiates a proposal?

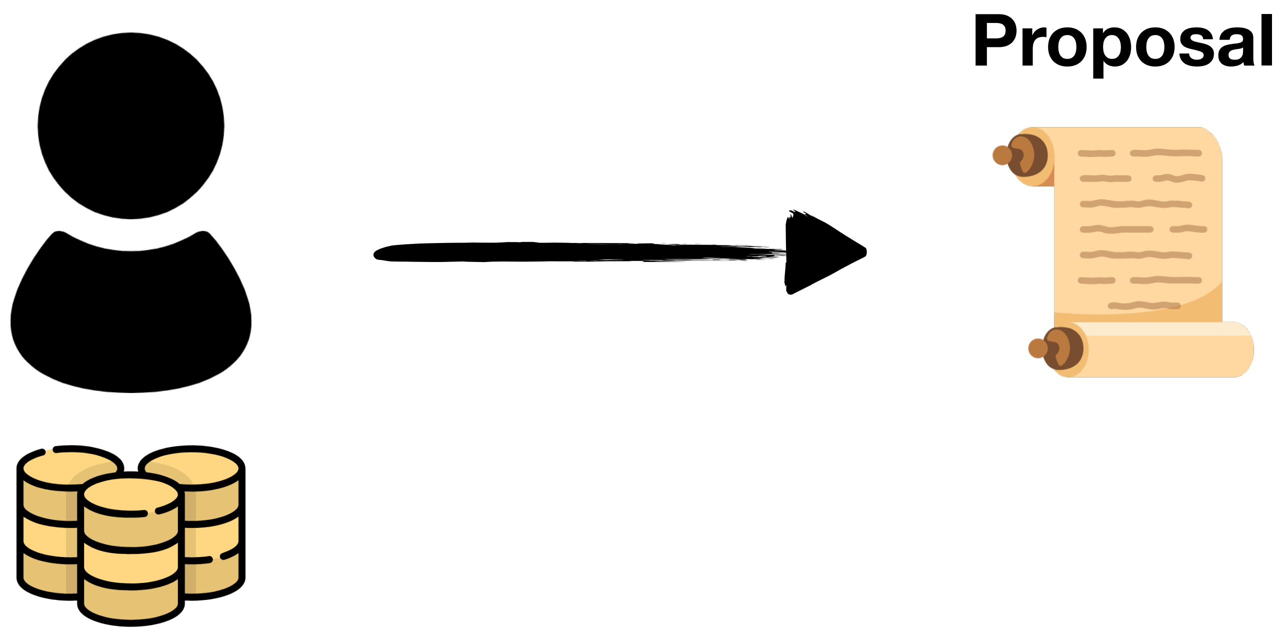
Pre-Voting Period

- Who initiates a proposal?
  - **Voter initiated proposal**



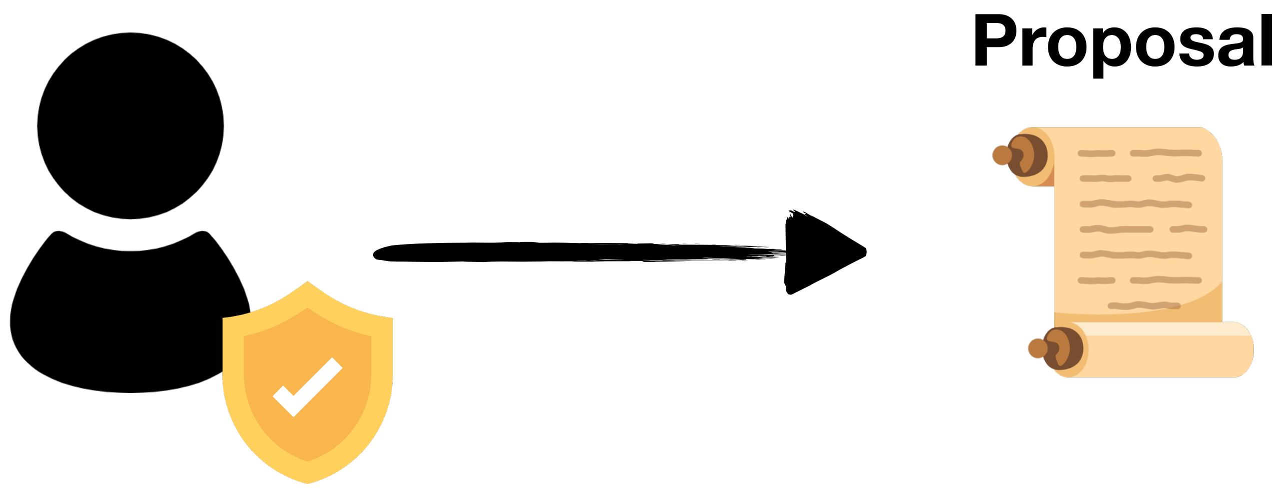
Pre-Voting Period

- Who initiates a proposal?
    - **Voter initiated proposal**
        - 19 DAOs only allow this



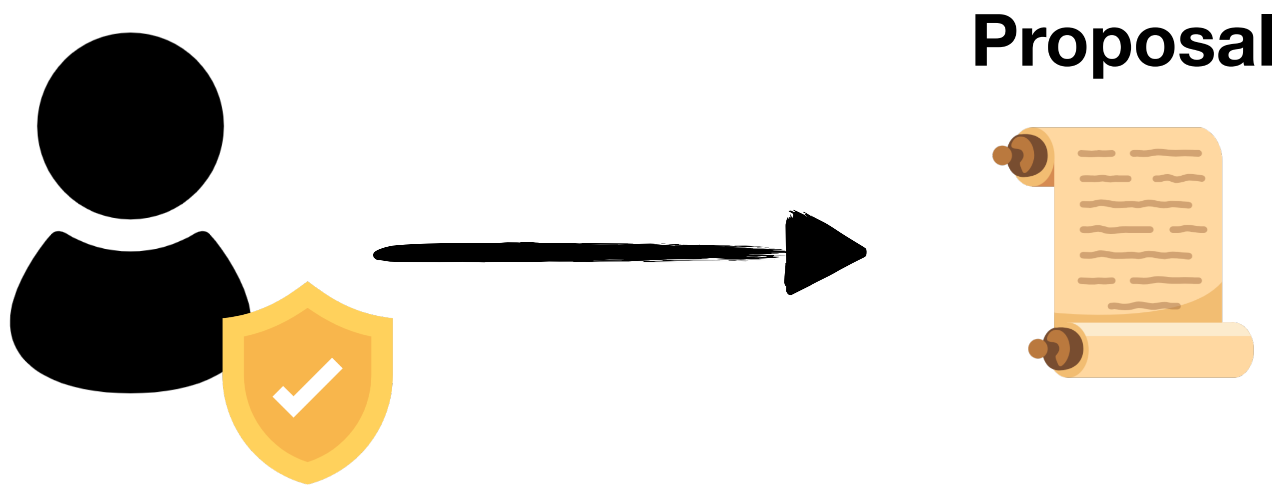
Pre-Voting Period

- Who initiates a proposal?
  - **Authority initiated proposal**



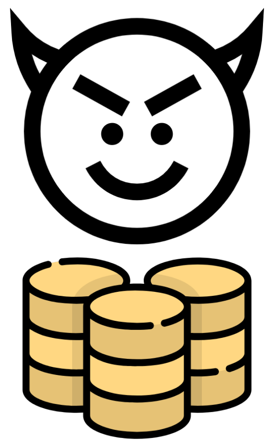
Pre-Voting Period

- Who initiates a proposal?
  - **Authority initiated proposal**
    - 14 DAOs only allow this

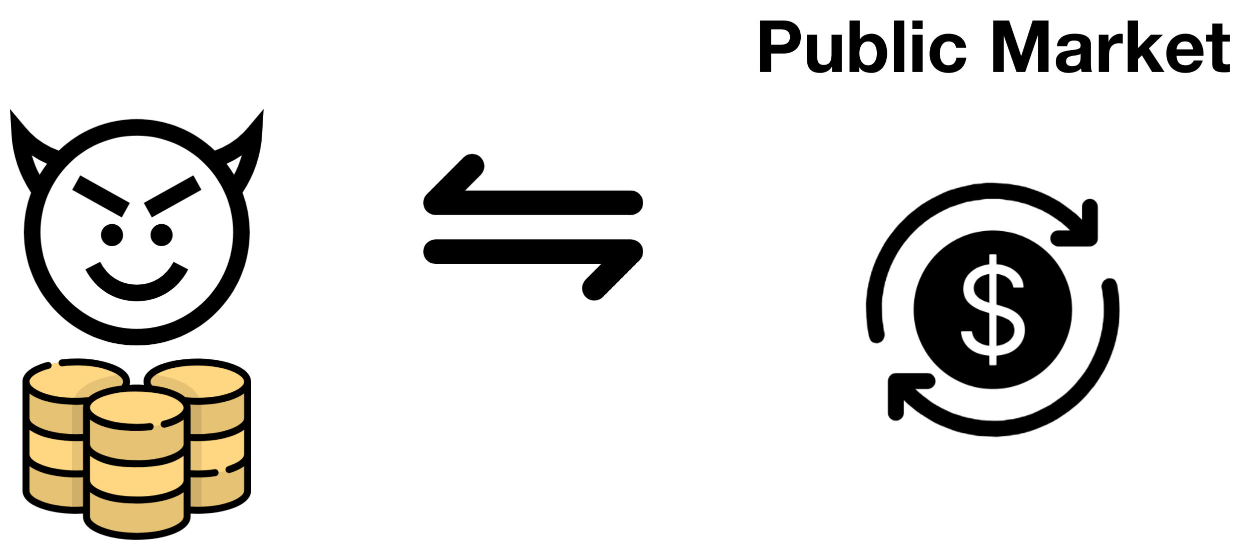


Pre-Voting Period

Pre-Voting Period

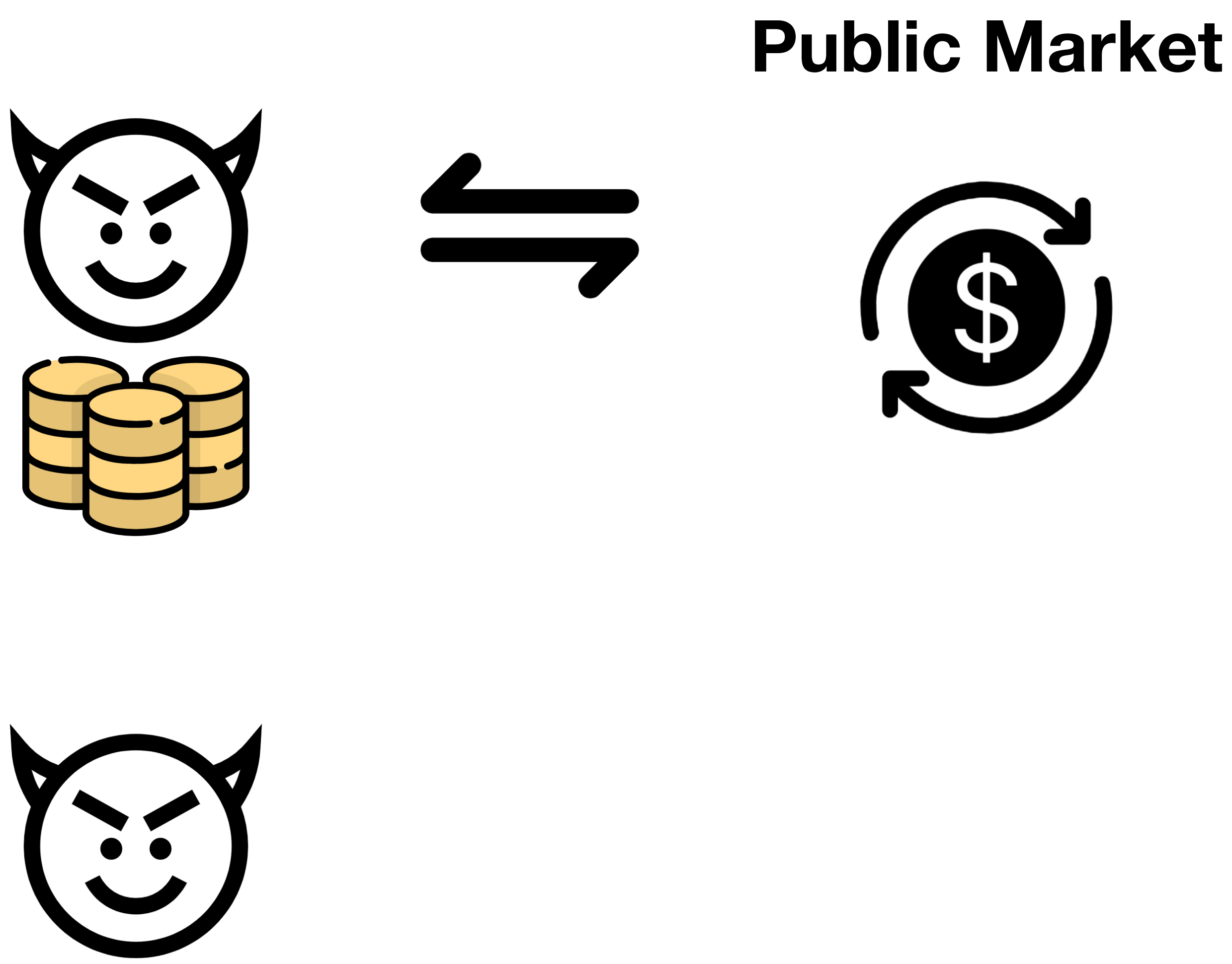


Pre-Voting Period



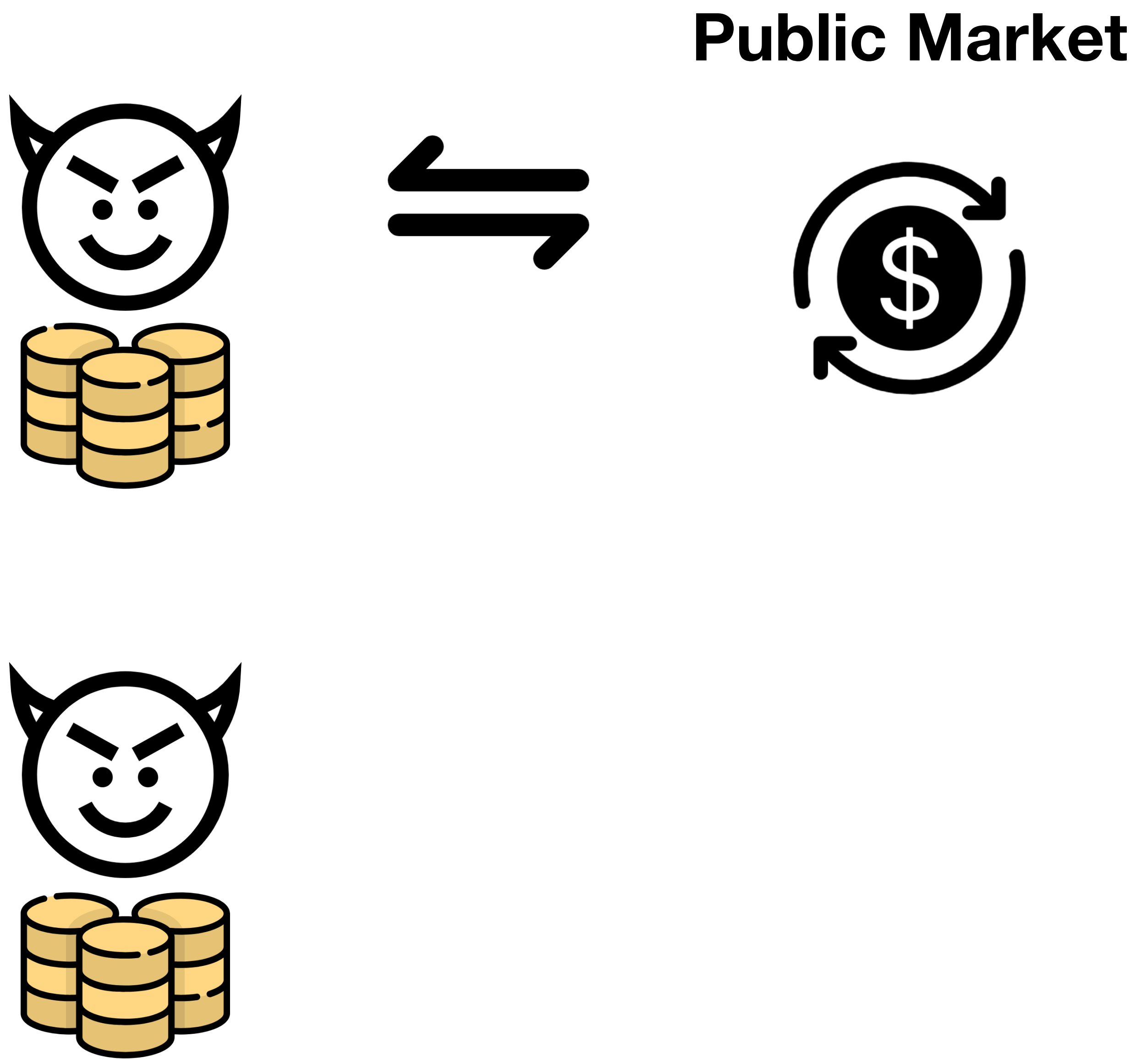
Public Market

Pre-Voting Period



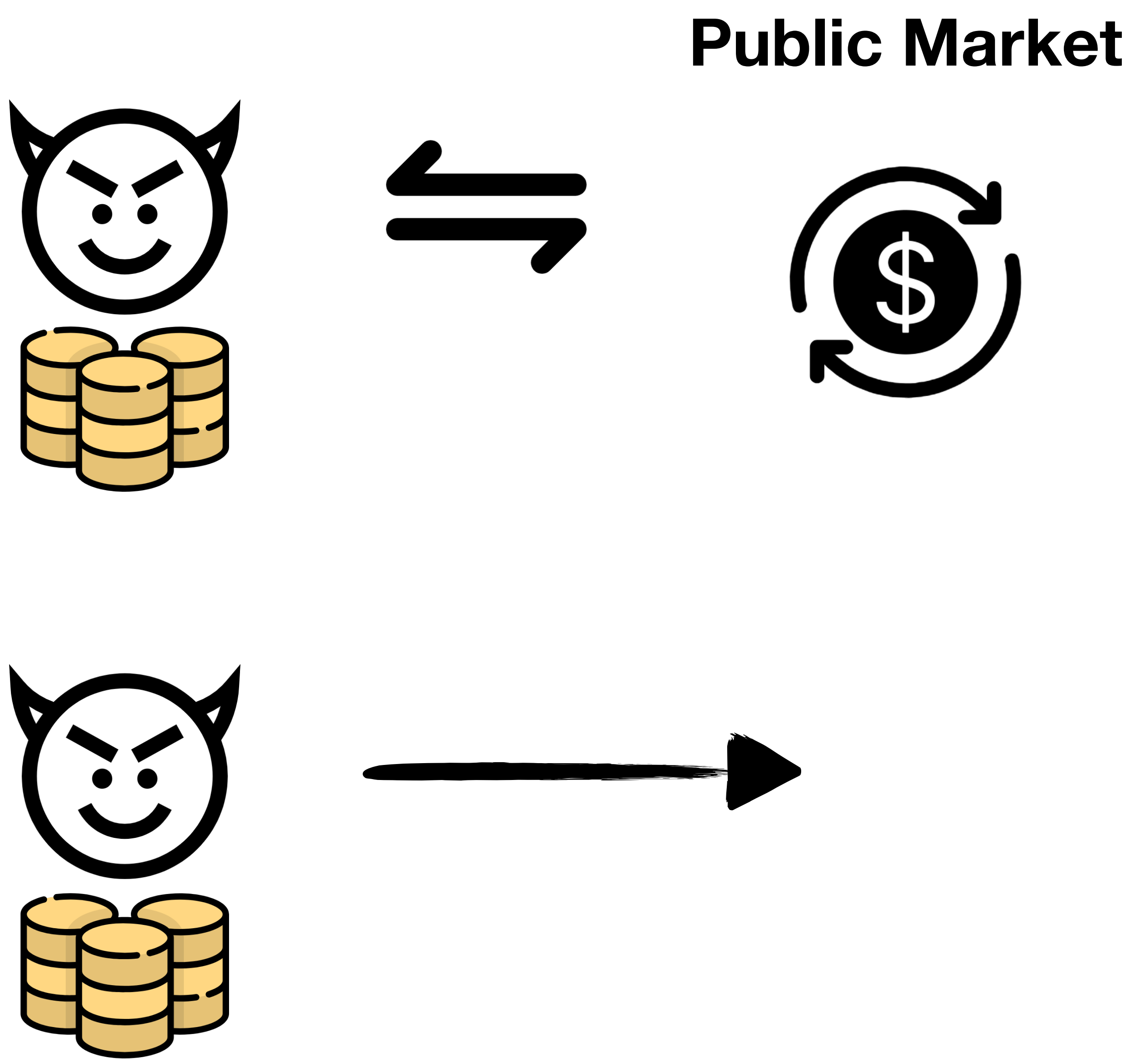
Public Market

Pre-Voting Period



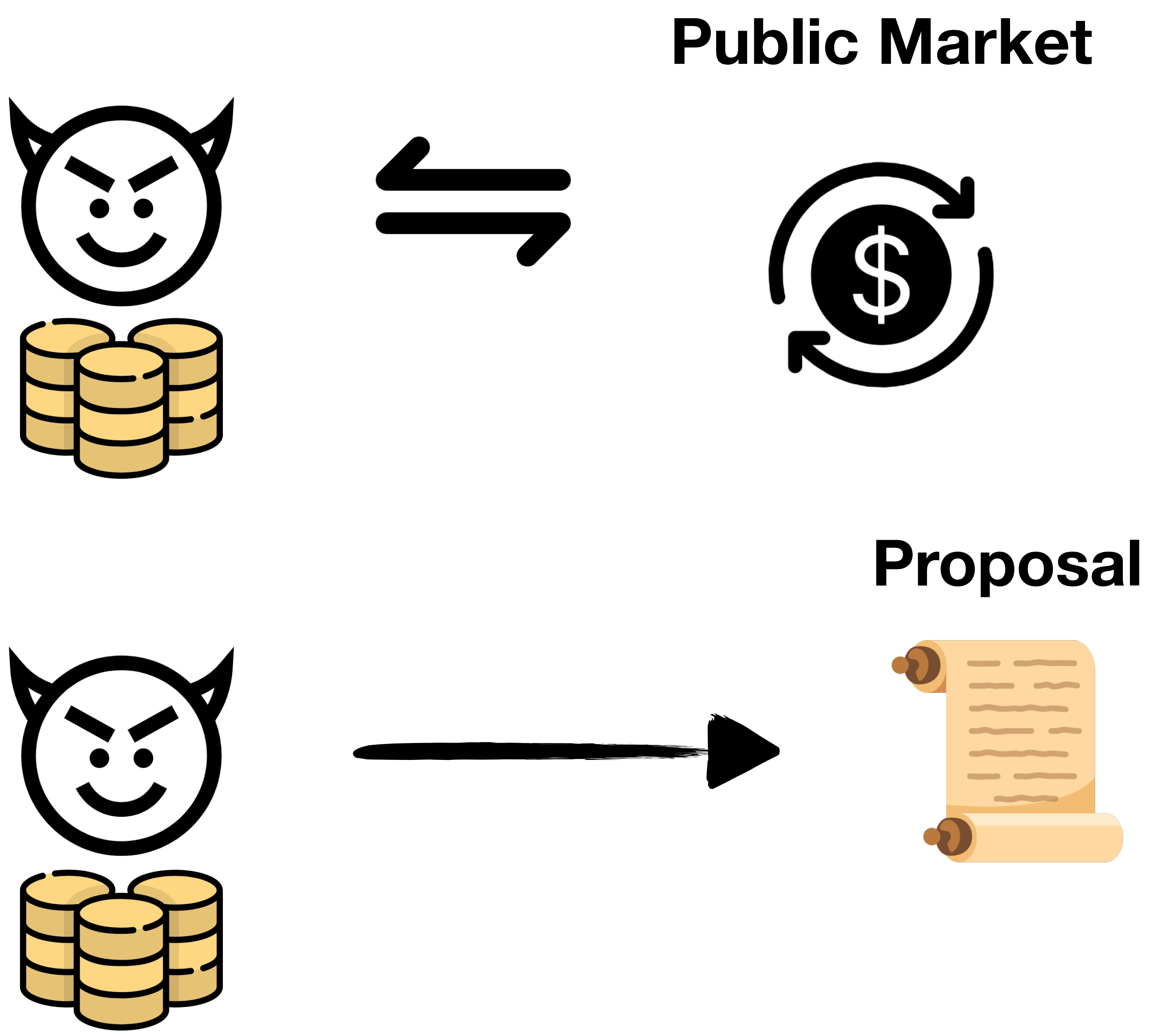
Public Market

Pre-Voting Period



Public Market

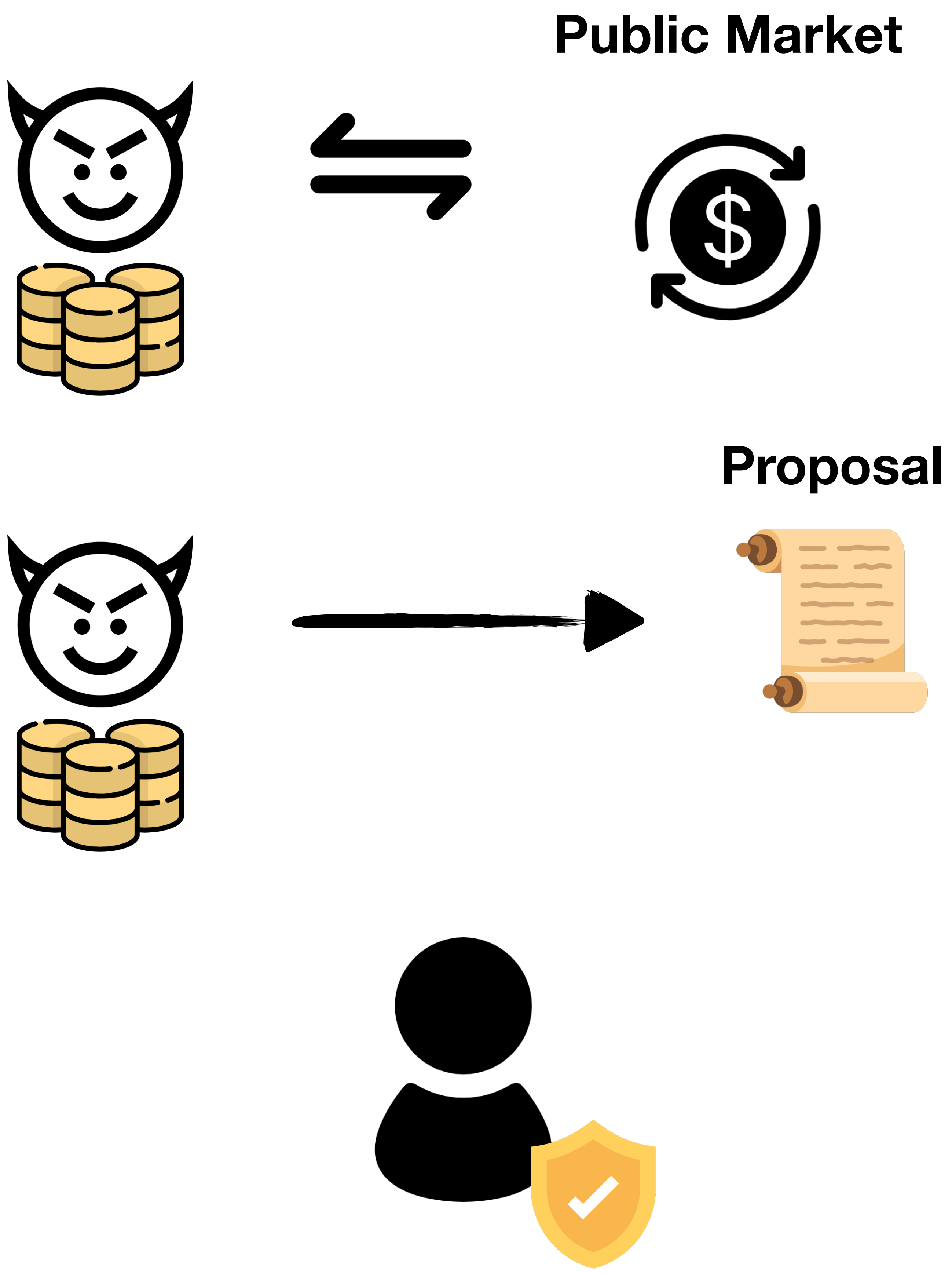
Pre-Voting Period



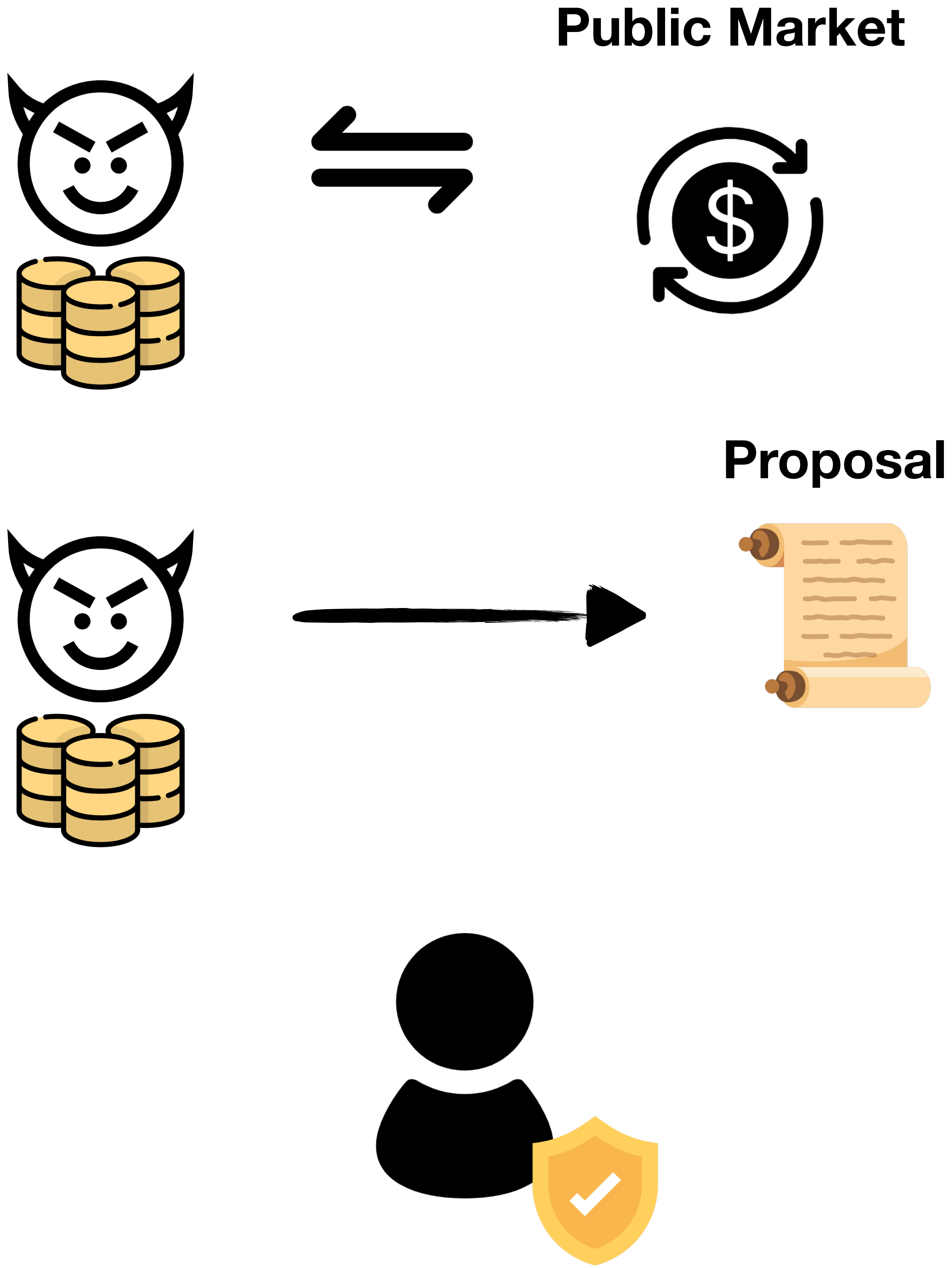
Public Market

Proposal

Pre-Voting Period



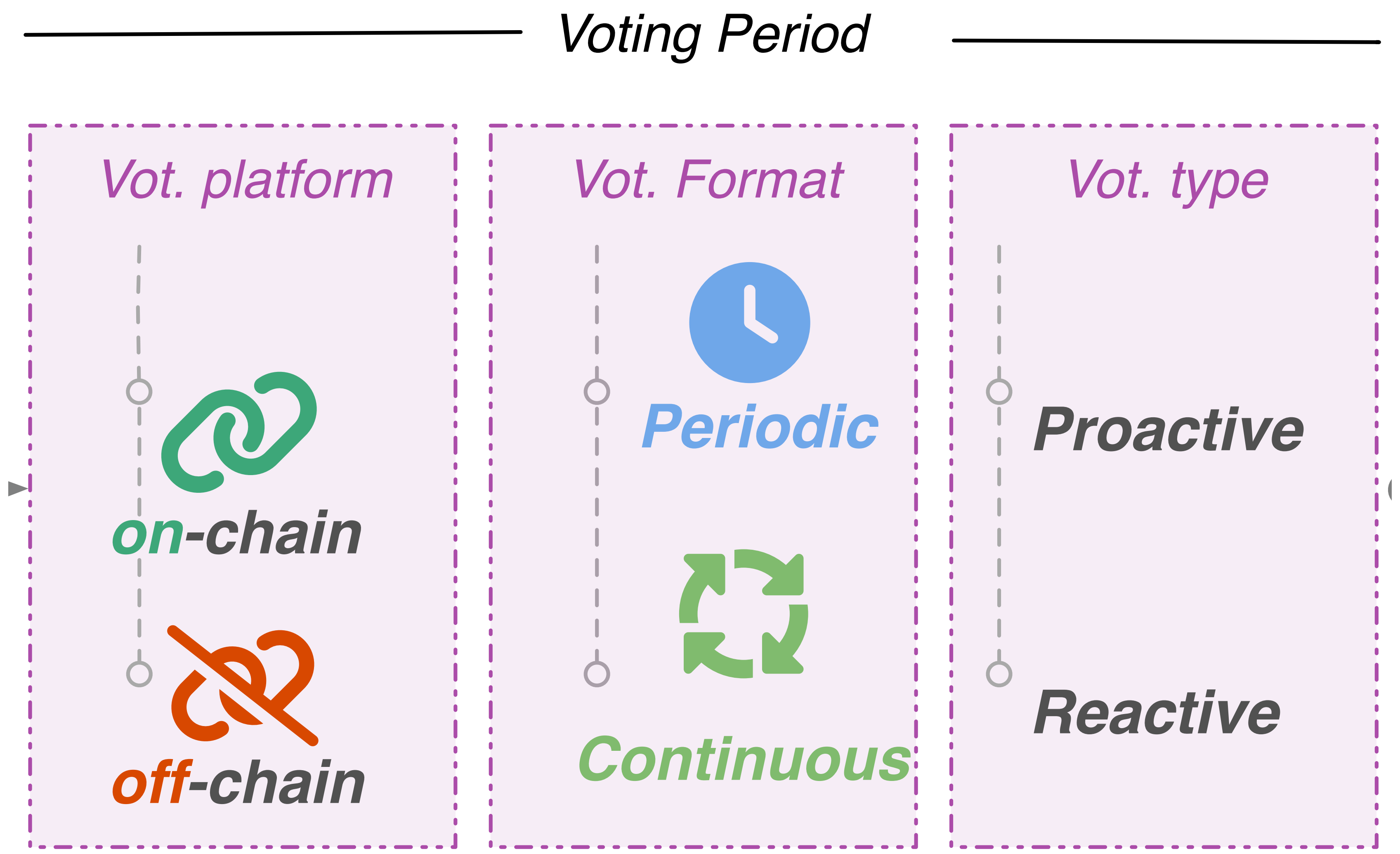
Pre-Voting Period



CENTRALIZED

Voting Period

- **Voting Platform**
- Voting Format
- Voting Type

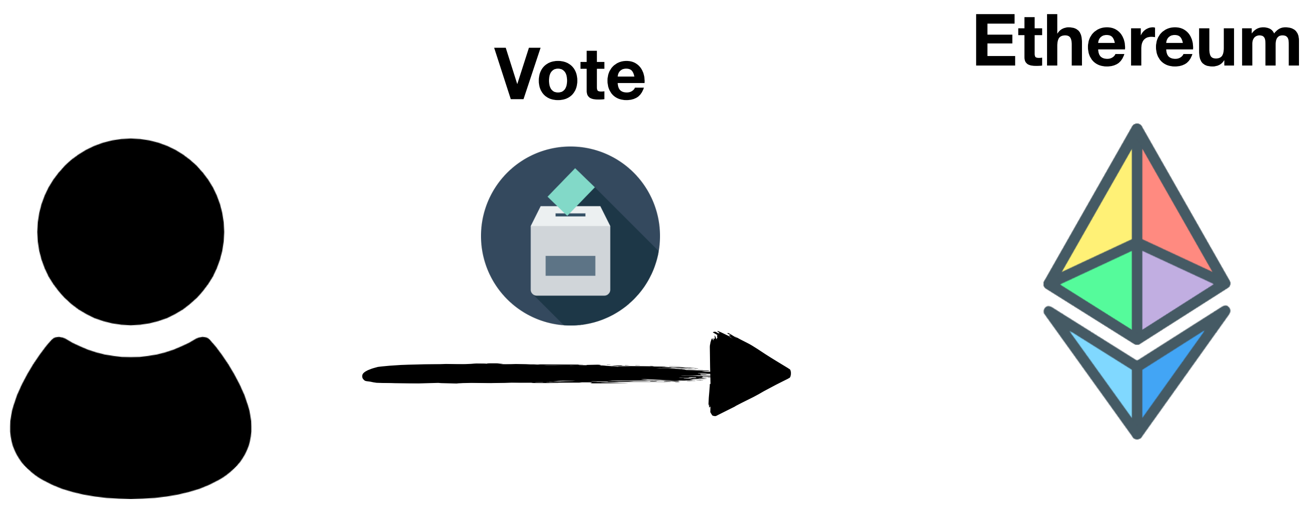


Voting Period

- **Voting Platform**
  - On-chain

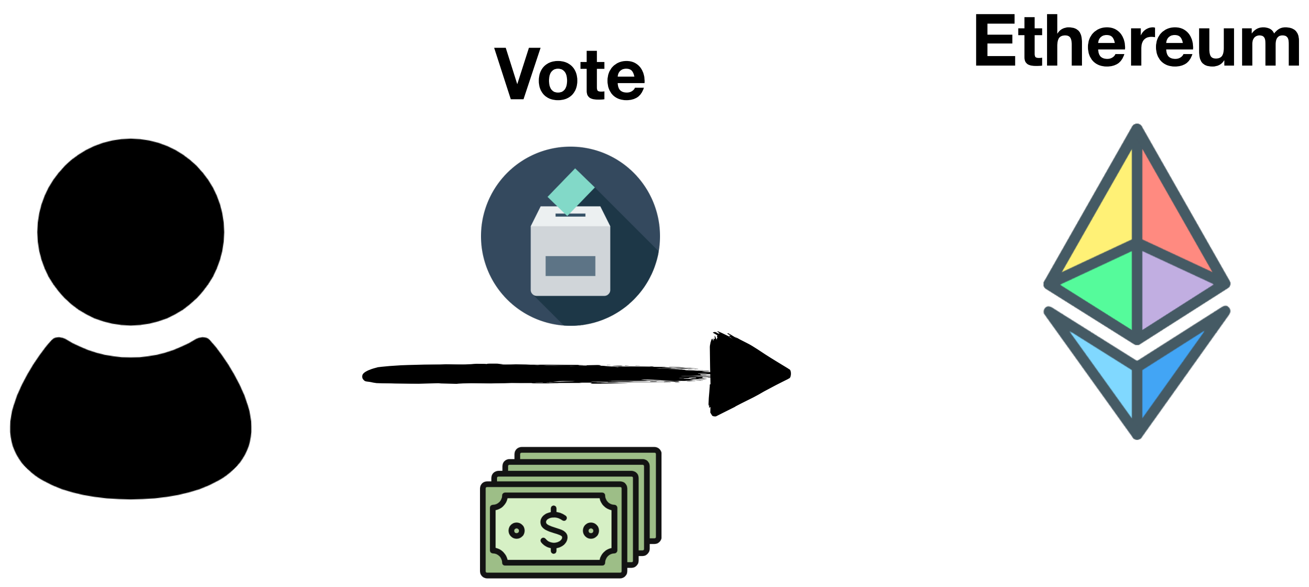
Voting Period

- **Voting Platform**
  - On-chain



Voting Period

- **Voting Platform**
  - On-chain

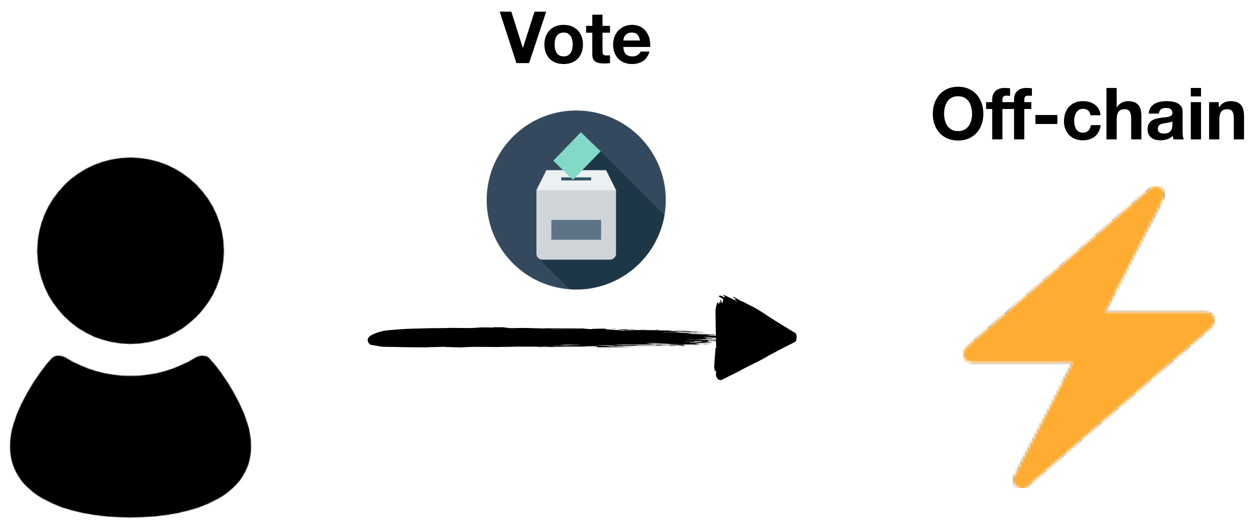


Voting Period

- **Voting Platform**
    - Off-chain

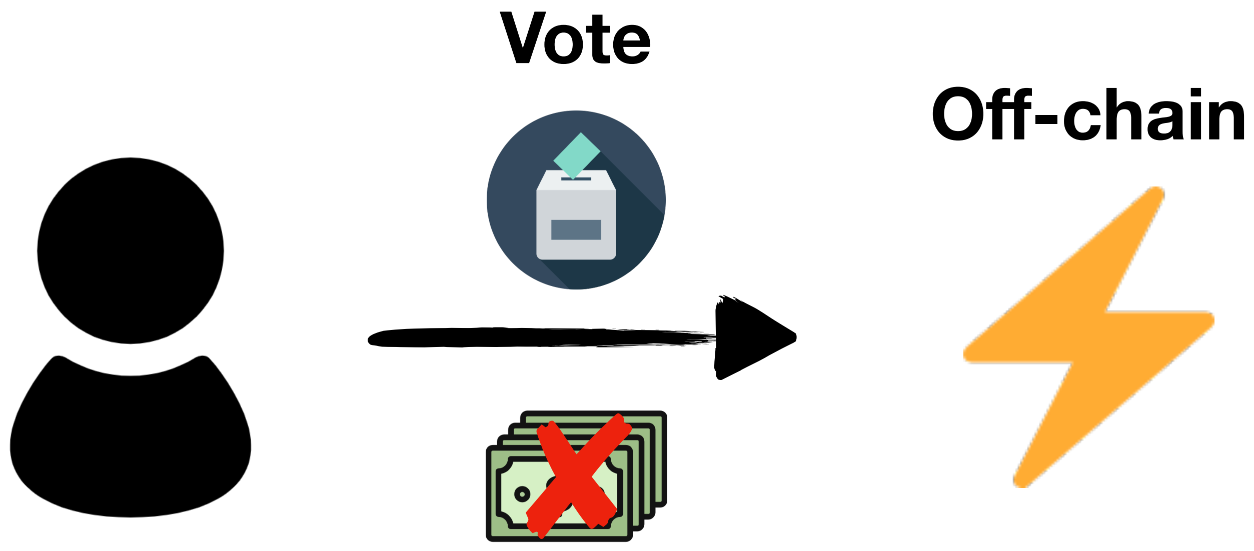
Voting Period

- **Voting Platform**
  - Off-chain



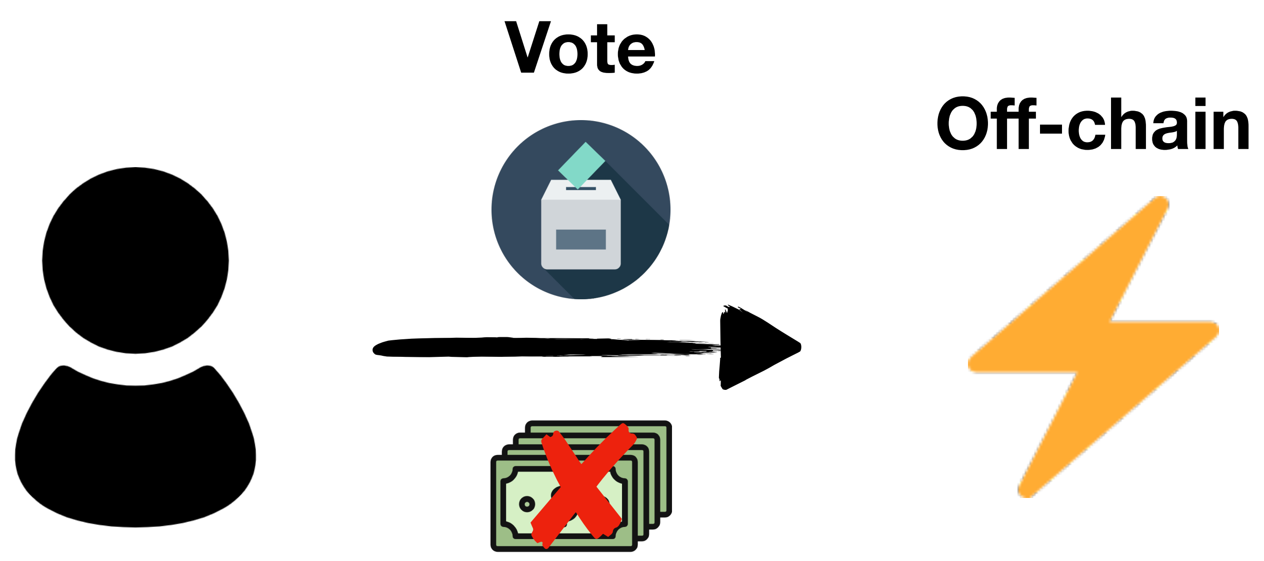
Voting Period

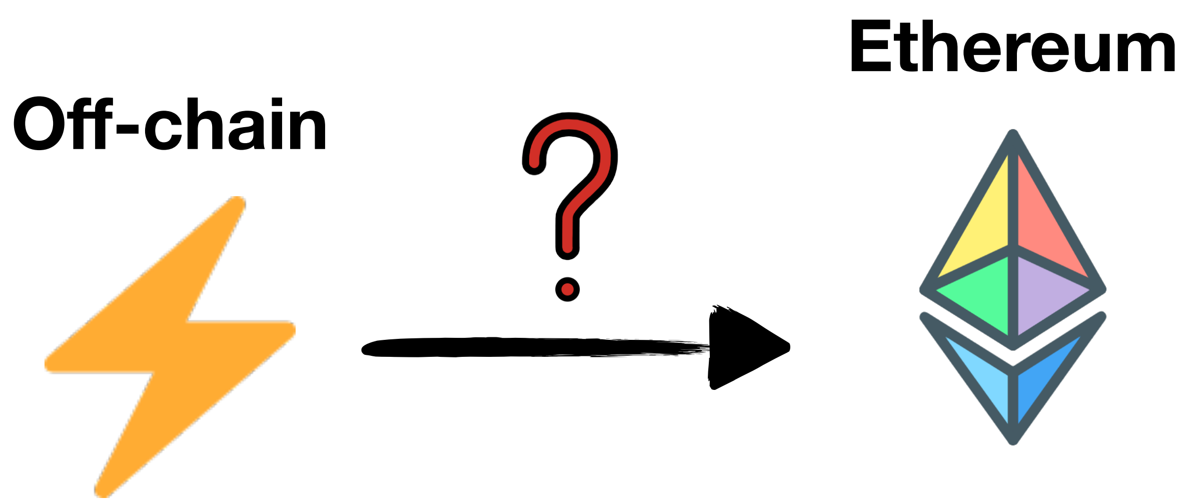
- **Voting Platform**
  - Off-chain



Voting Period

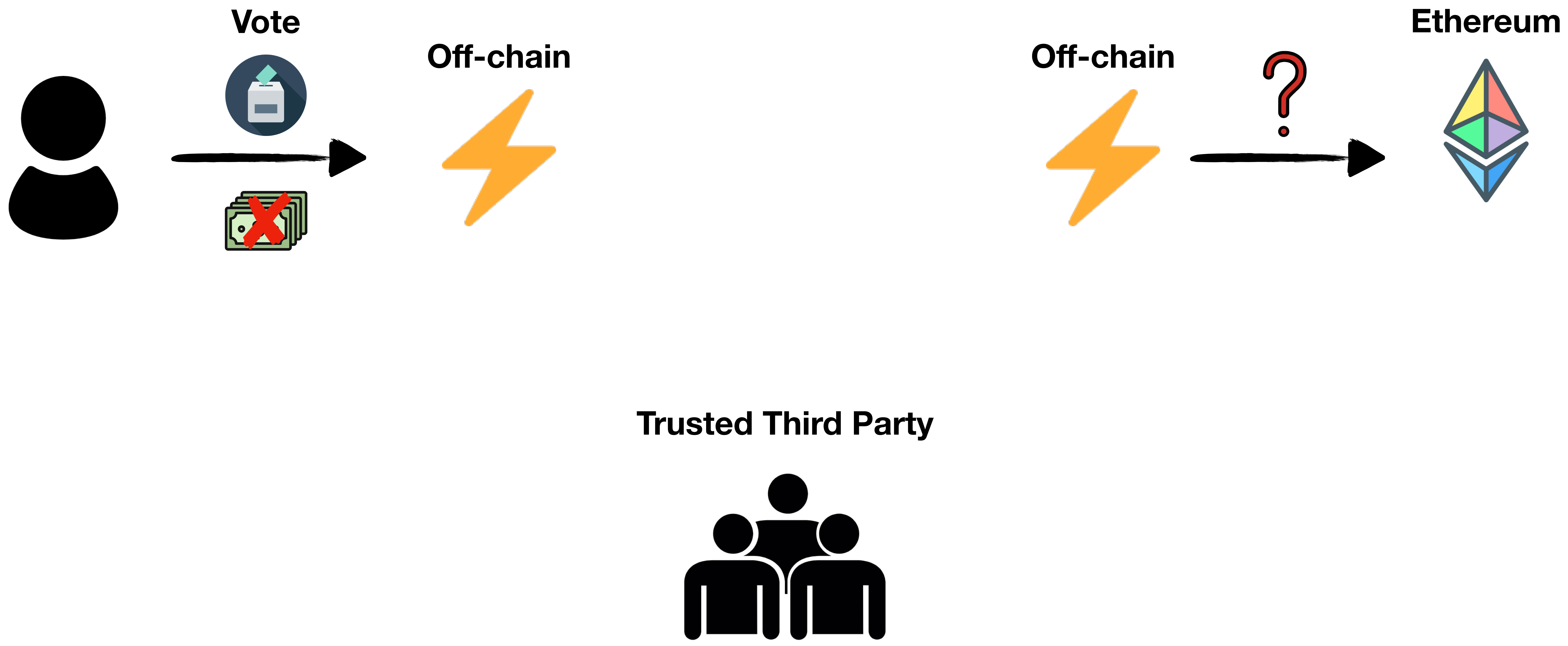
- **Voting Platform**
  - Off-chain





Voting Period

- **Voting Platform**
    - Off-chain



Vote

Off-chain

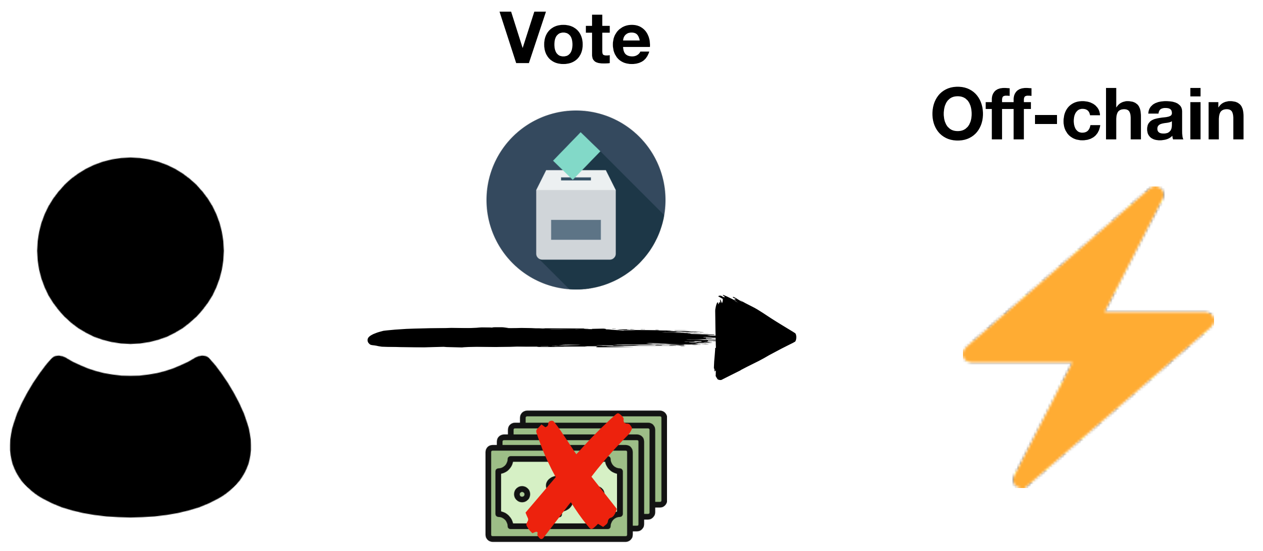
Off-chain

Ethereum

Trusted Third Party

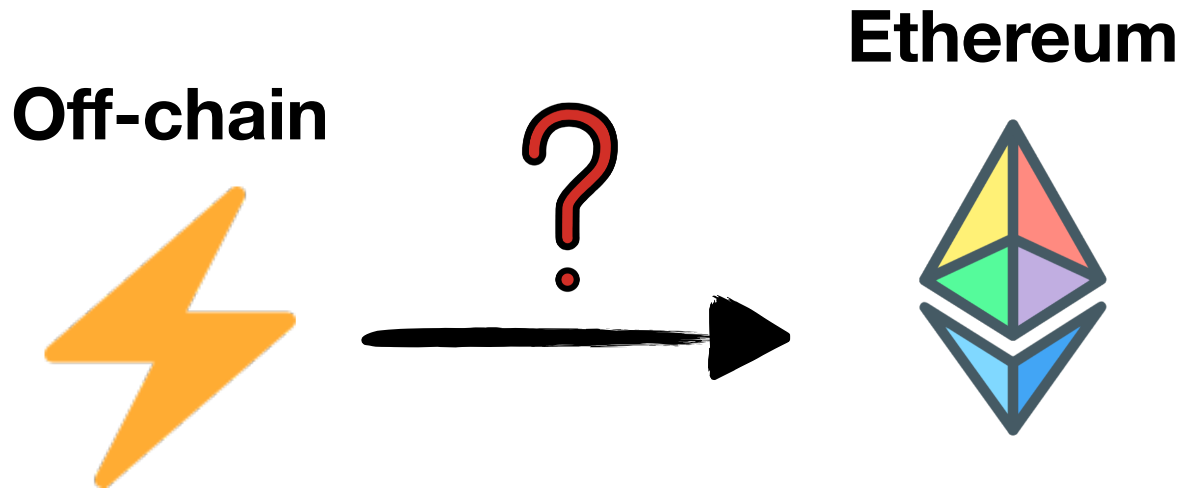
Voting Period

- **Voting Platform**
  - Off-chain



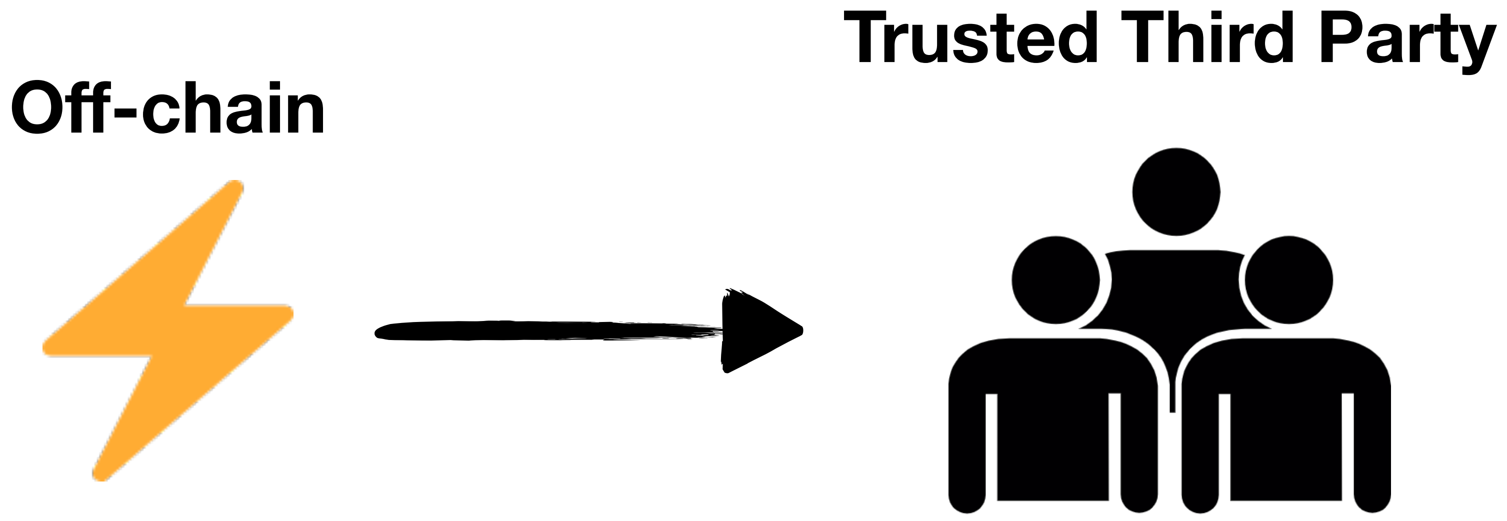
Vote

Off-chain



Off-chain

Ethereum

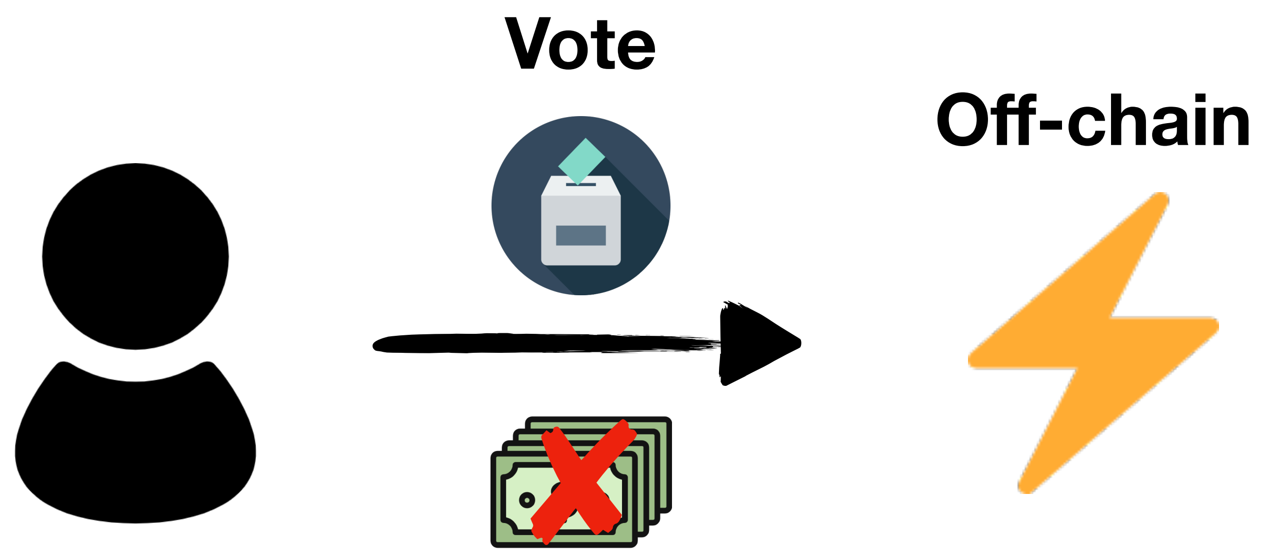


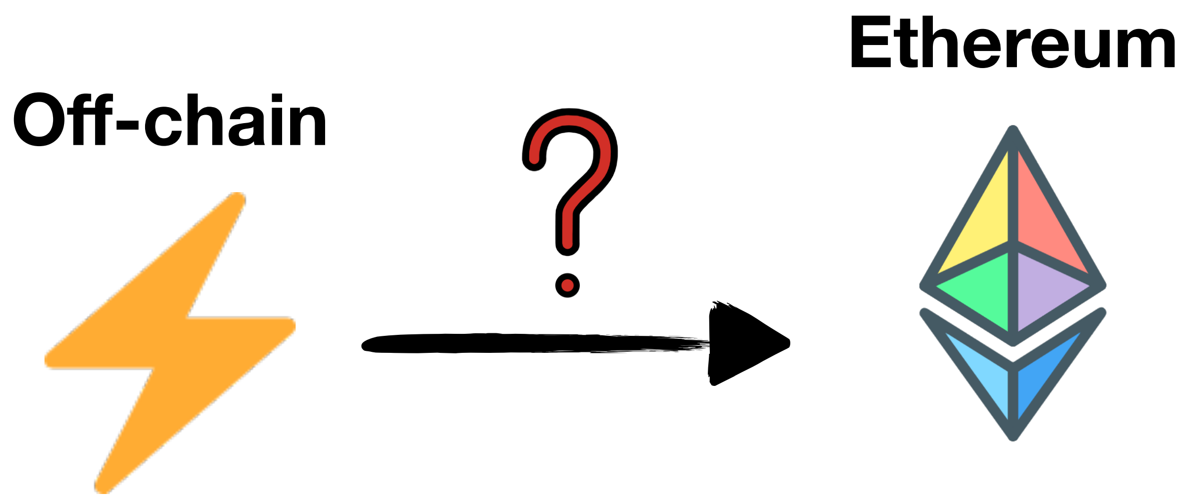
Off-chain

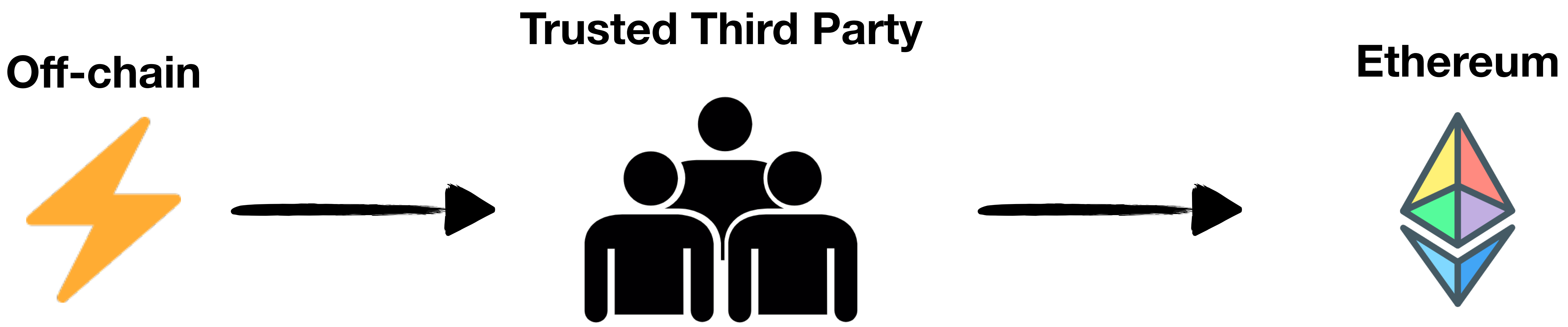
Trusted Third Party

Voting Period

- **Voting Platform**
  - Off-chain







Voting Period

- **Voting Platform**
    - On-chain Voting with pre-vote polling

Voting Period

- **Voting Platform**
  - On-chain Voting with pre-vote polling

Proposal 📜 Off-chain ⚡

Voting Period

- **Voting Platform**
  - On-chain Voting with pre-vote polling

Proposal 📜 **Off-chain** ⚡✓

Voting Period

- **Voting Platform**
  - On-chain Voting with pre-vote polling

Proposal Off-chain

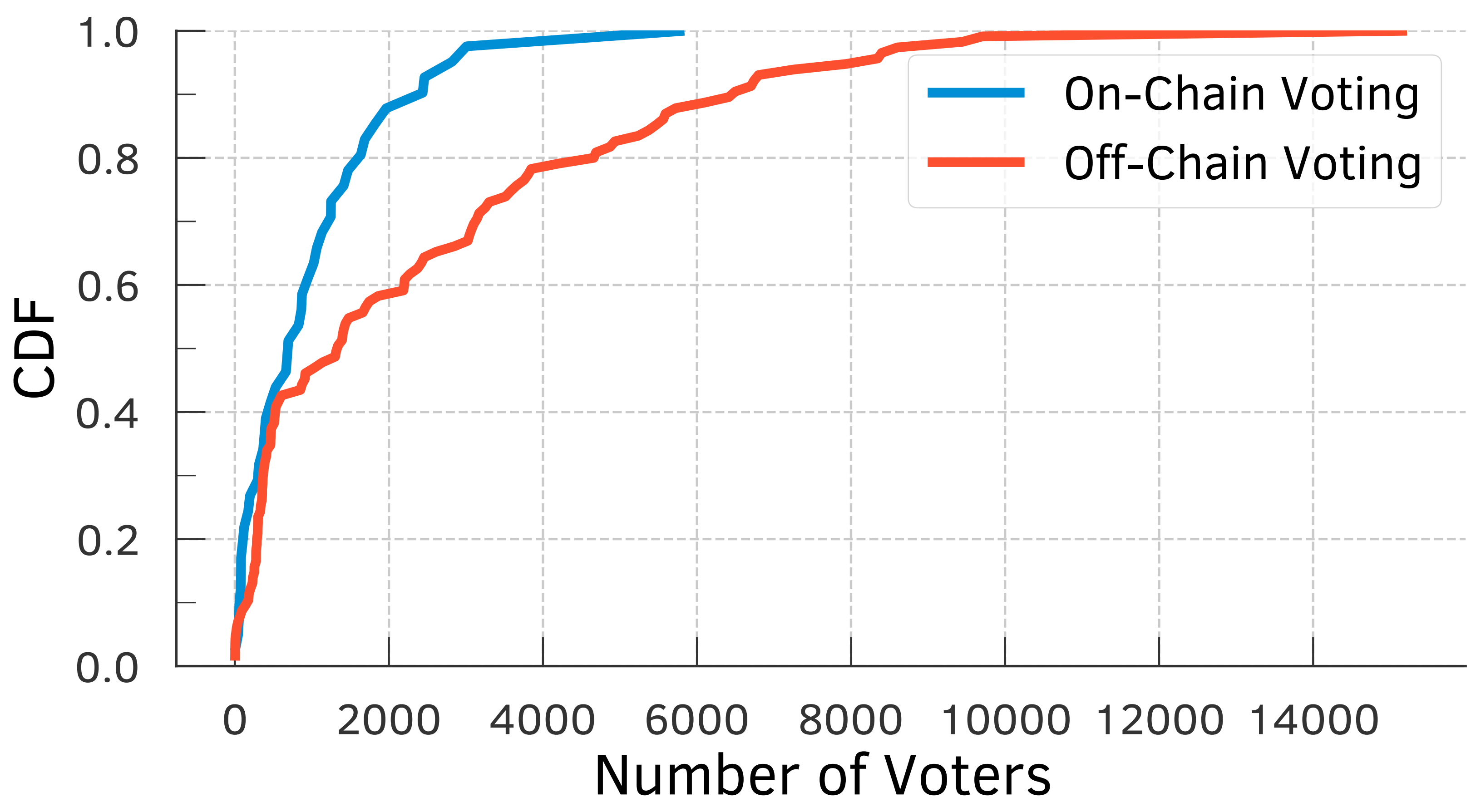
Proposal Ethereum

Voting Period

- **Voting Platform**
  - On-chain Voting with pre-vote polling

Proposal Off-chain

Proposal Ethereum

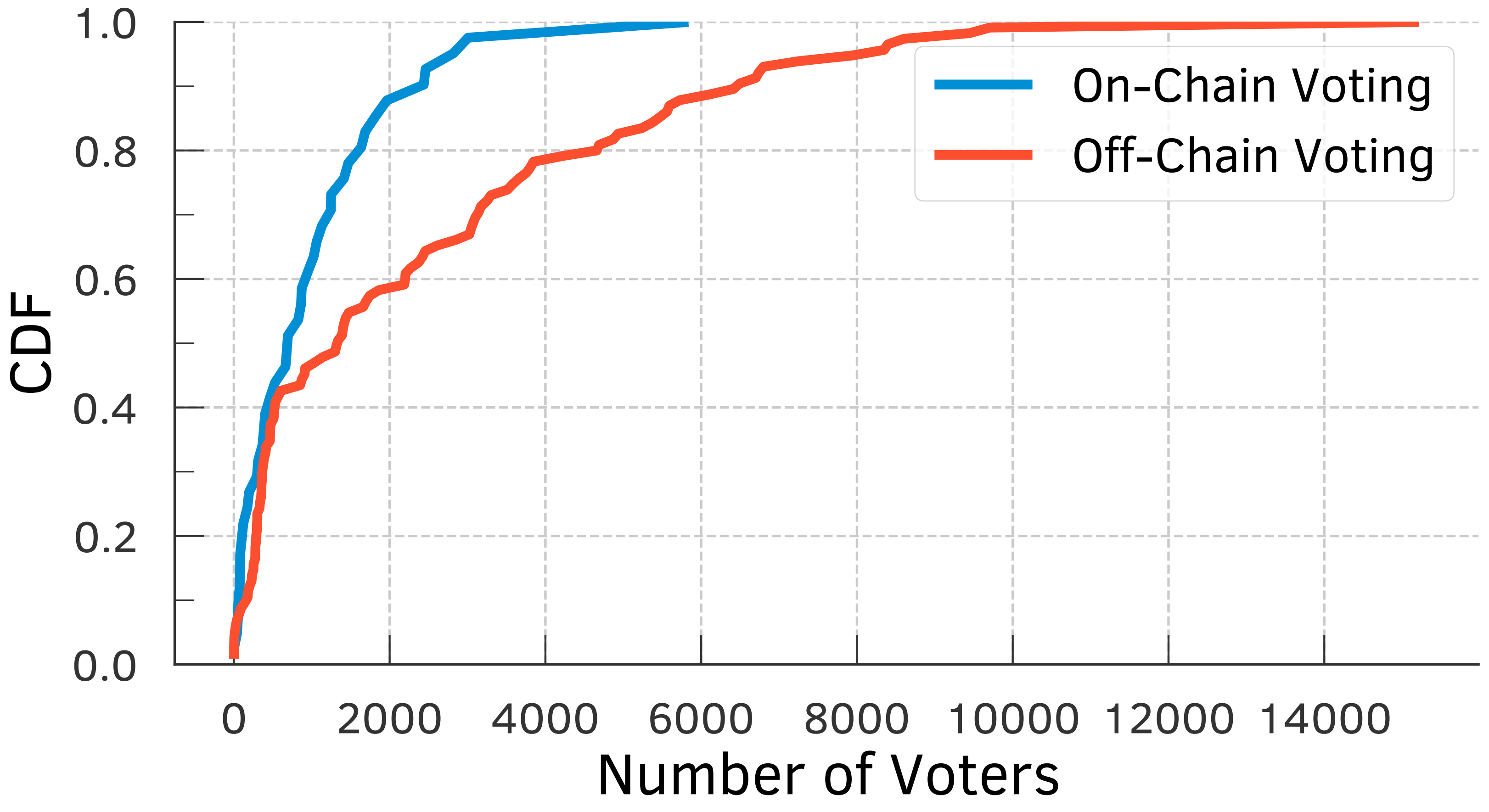


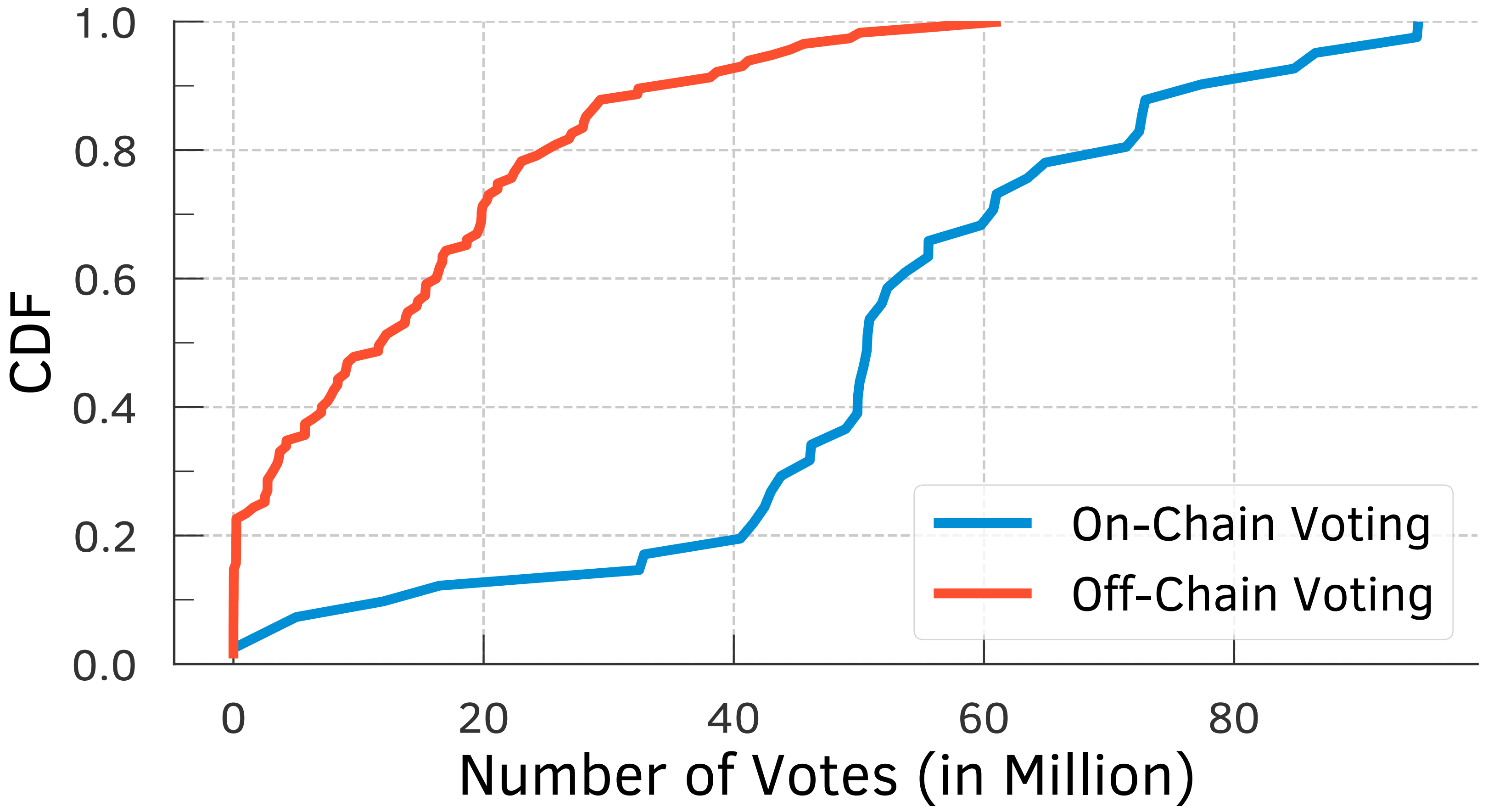
Voting Period

- **Voting Platform**
  - On-chain Voting with pre-vote polling

Proposal Off-chain

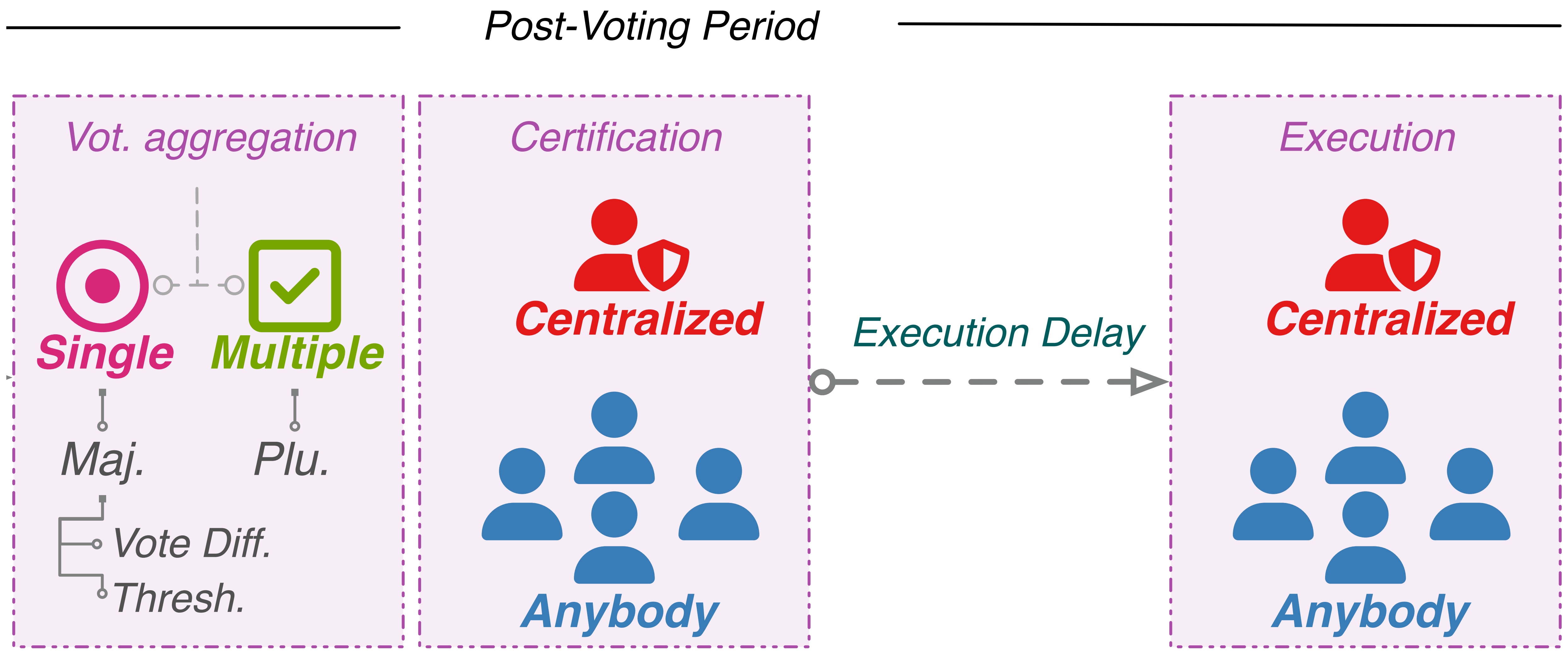
Proposal Ethereum





Post-Voting Period

- Voting Aggregation
- **Certification**
- Execution

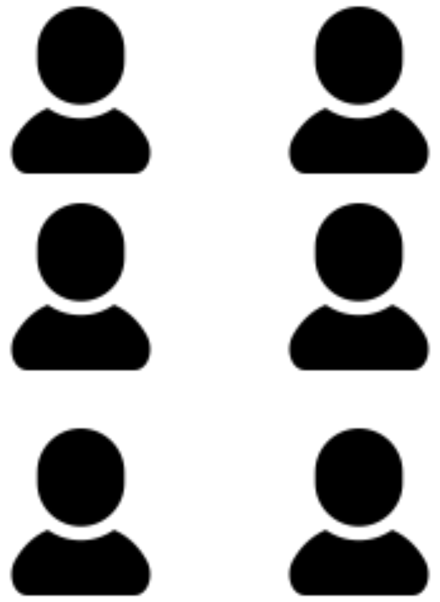


Post-Voting Period

- **Certification**
  - **Anybody**
    - Generally for DAOs with on-chain voting

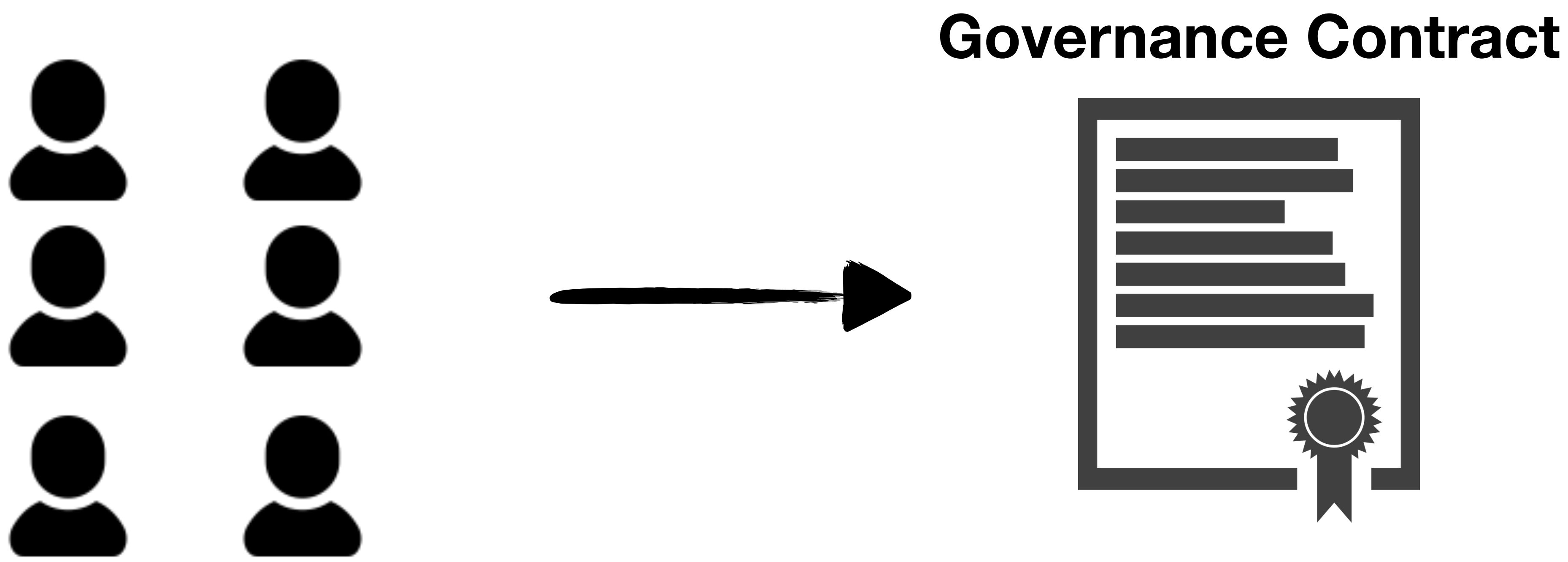
Post-Voting Period

- **Certification**
  - **Anybody**
    - Generally for DAOs with on-chain voting



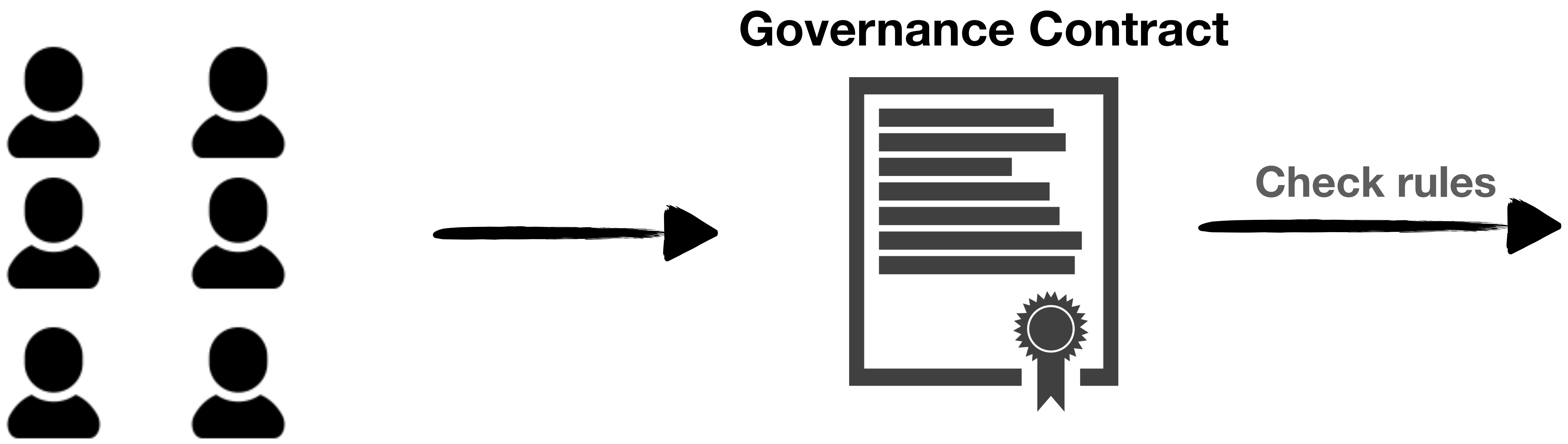
Post-Voting Period

- **Certification**
  - **Anybody**
    - Generally for DAOs with on-chain voting



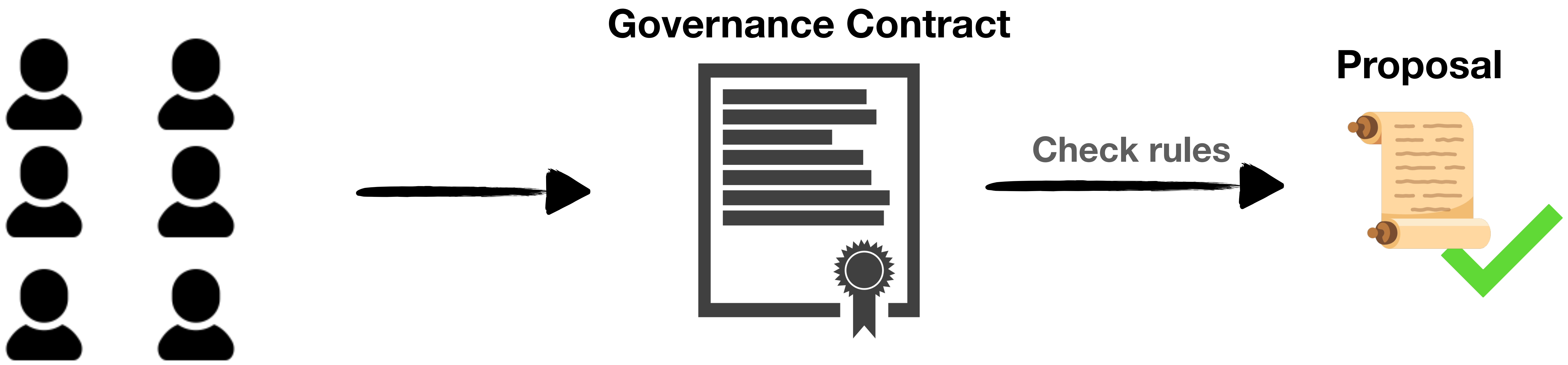
Post-Voting Period

- **Certification**
  - **Anybody**
    - Generally for DAOs with on-chain voting



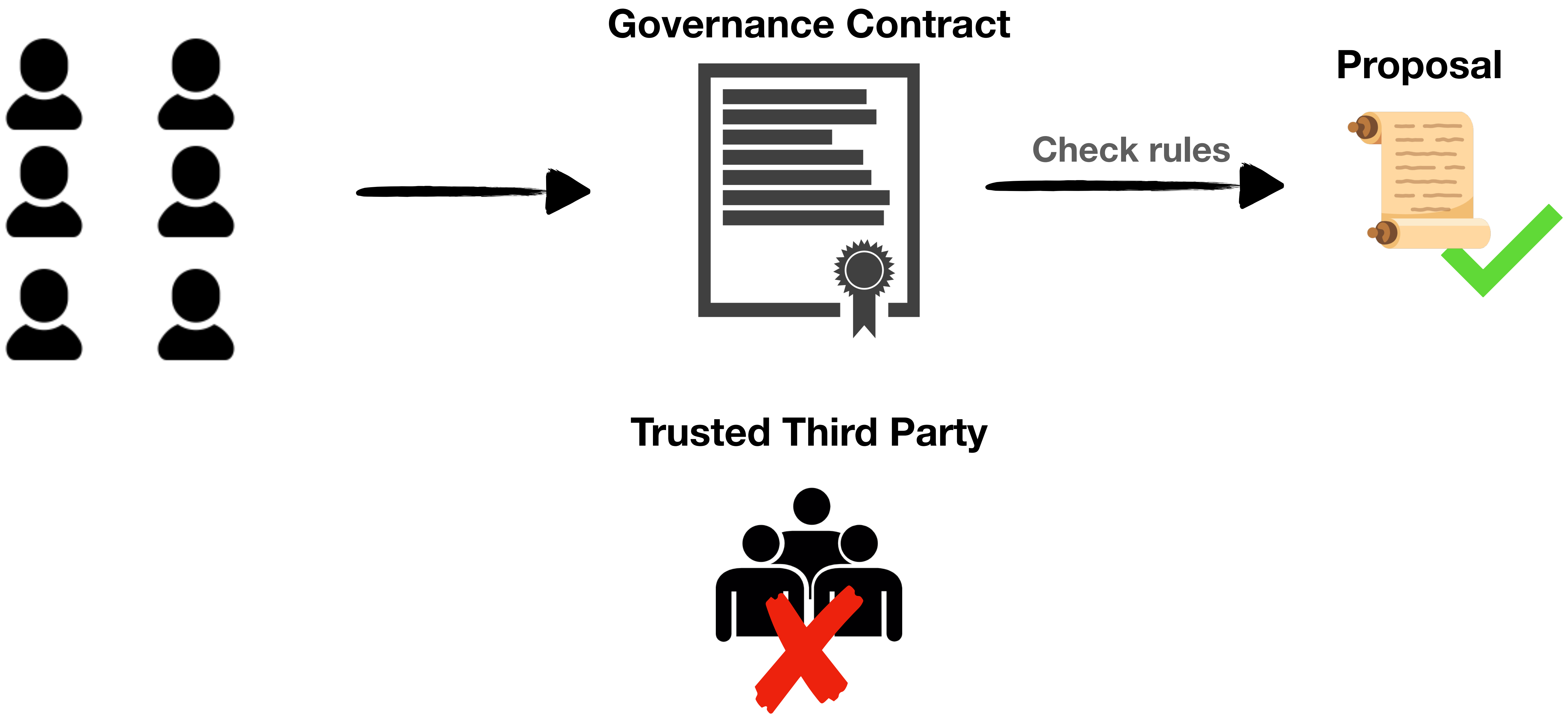
Post-Voting Period

- **Certification**
  - **Anybody**
    - Generally for DAOs with on-chain voting



Post-Voting Period

- **Certification**
  - **Anybody**
    - Generally for DAOs with on-chain voting



Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting

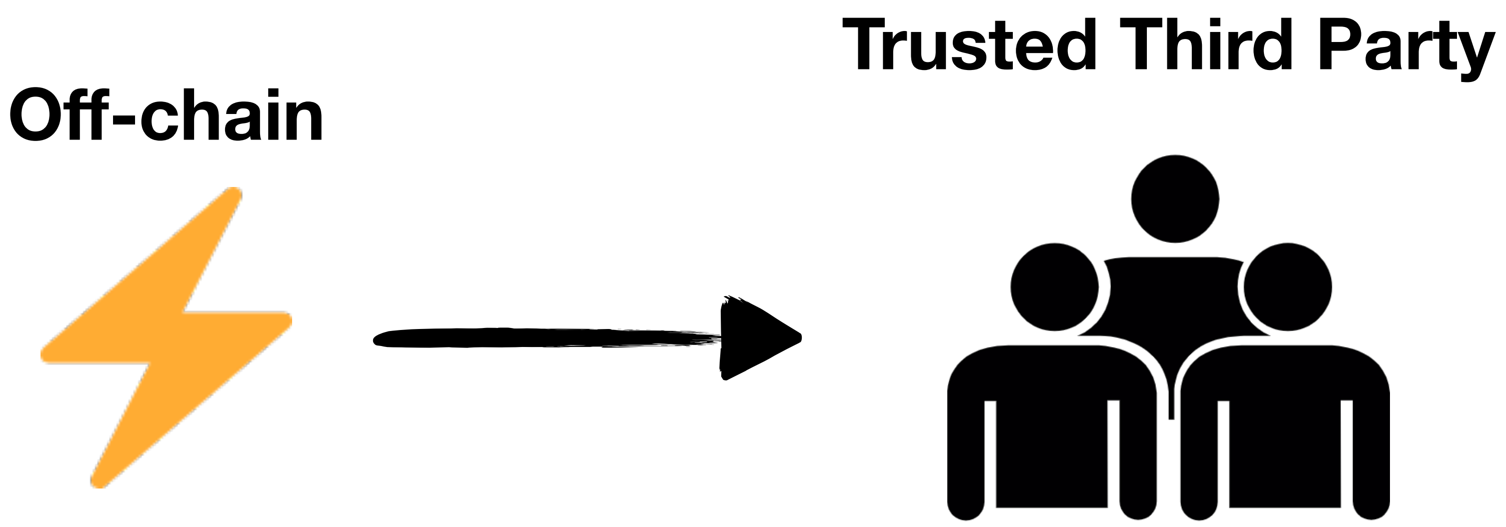
Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting

Trusted Third Party

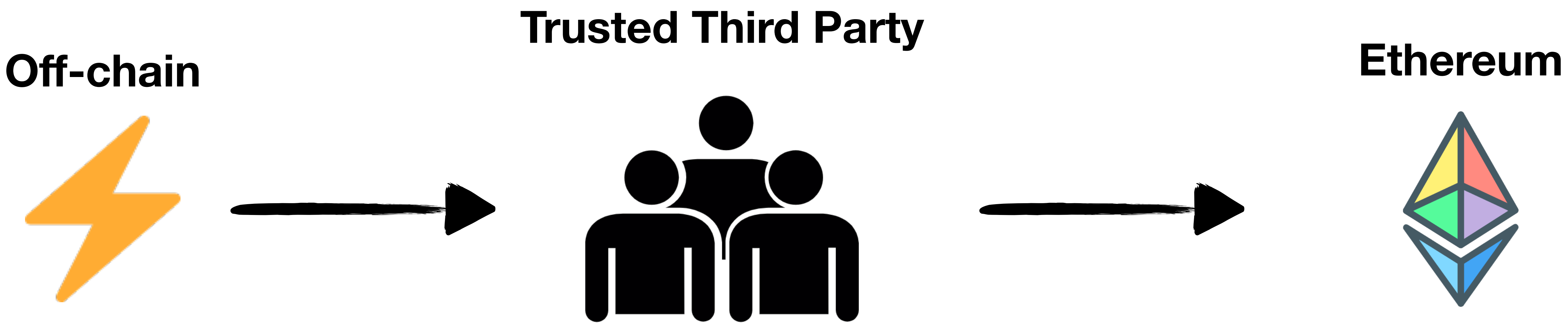
Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting



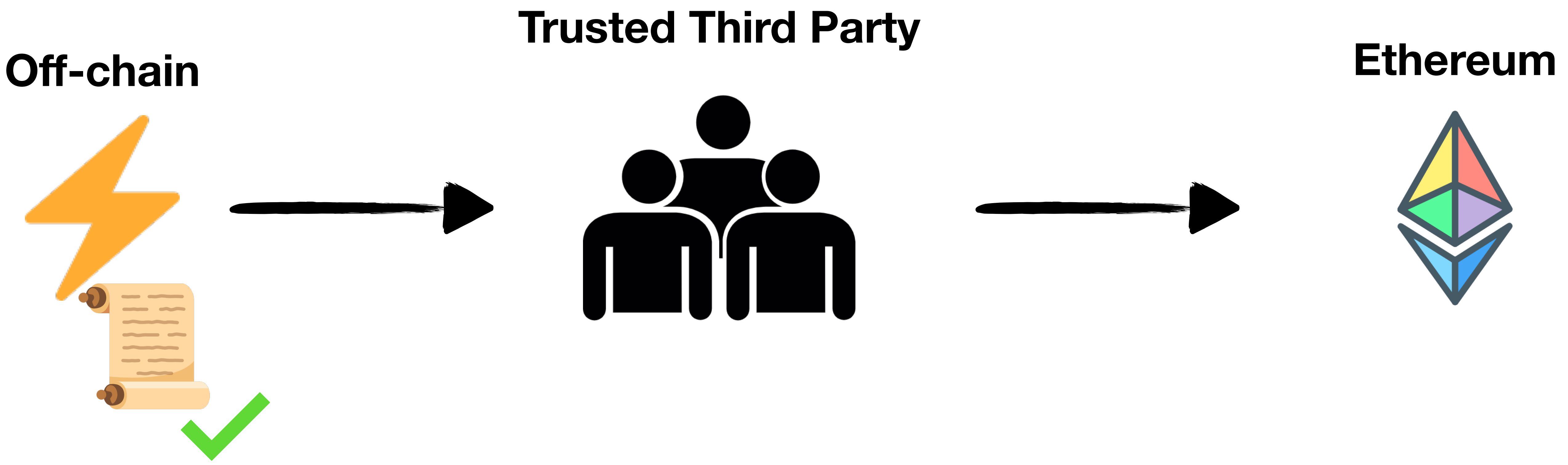
Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting



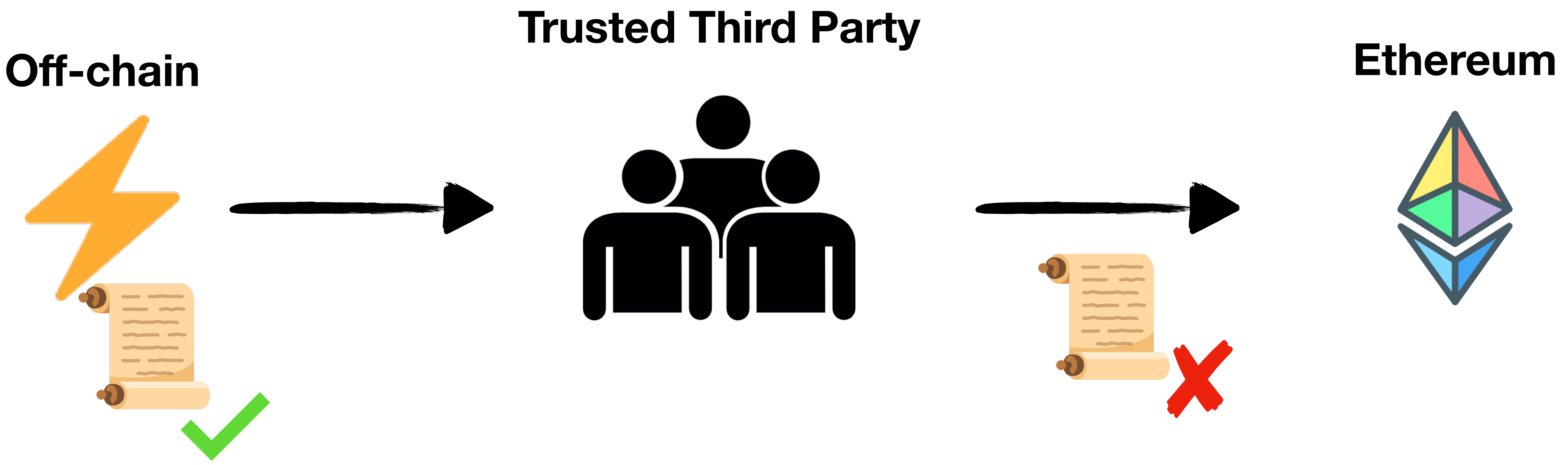
Post-Voting Period

- **Certification**
  - **Centralised**
    - Generally for DAOs with off-chain voting



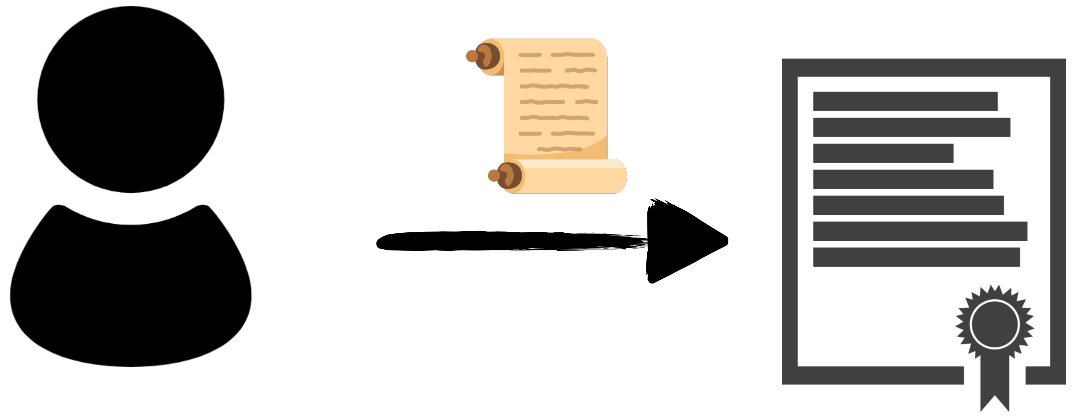
Post-Voting Period

- **Certification**
    - **Centralised**
        - Generally for DAOs with off-chain voting

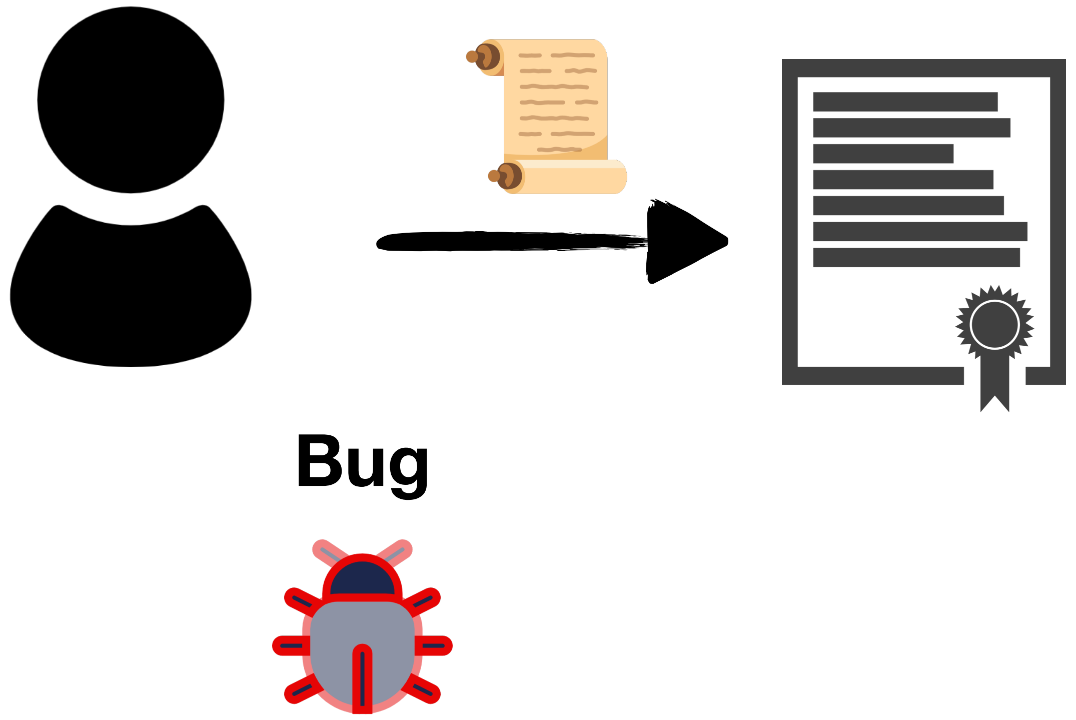


Veto

Veto

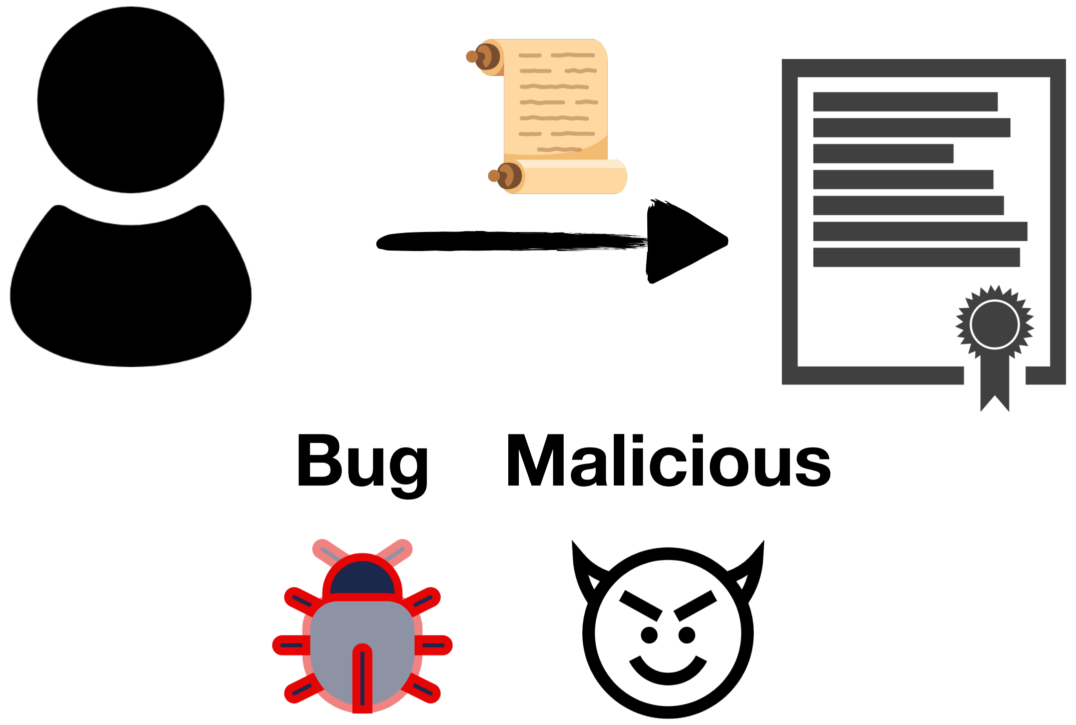


Veto

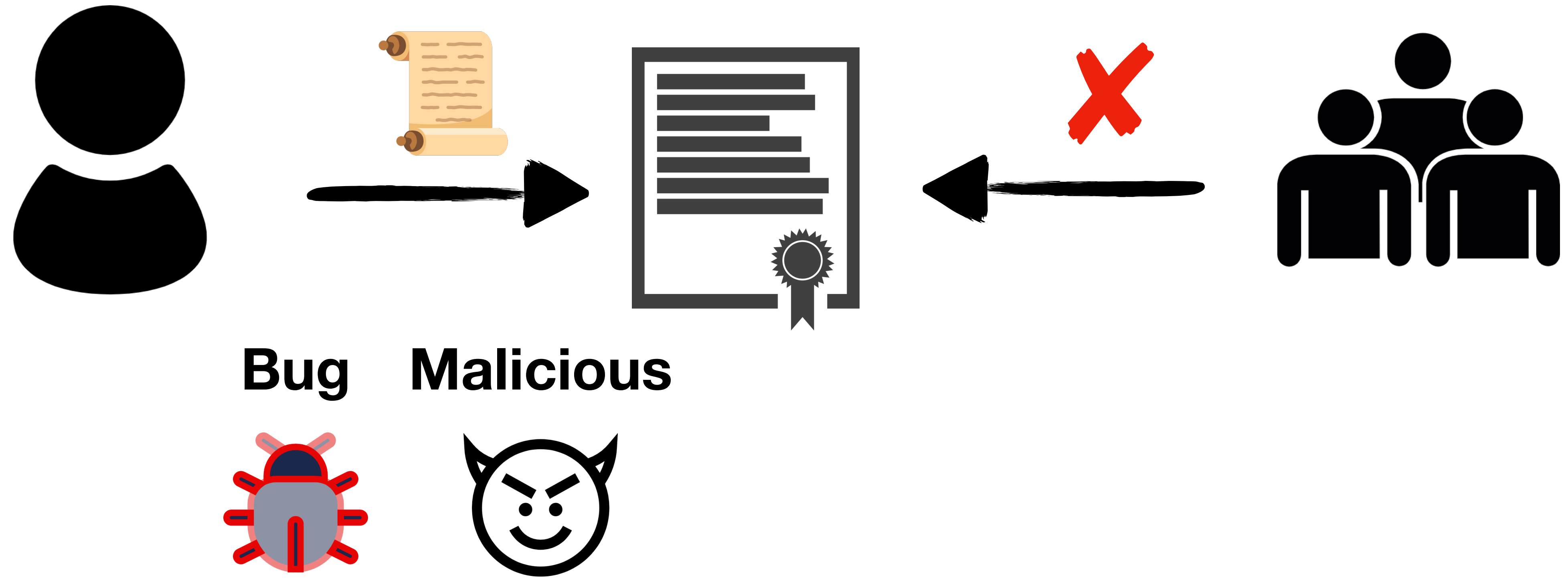


Bug

Veto



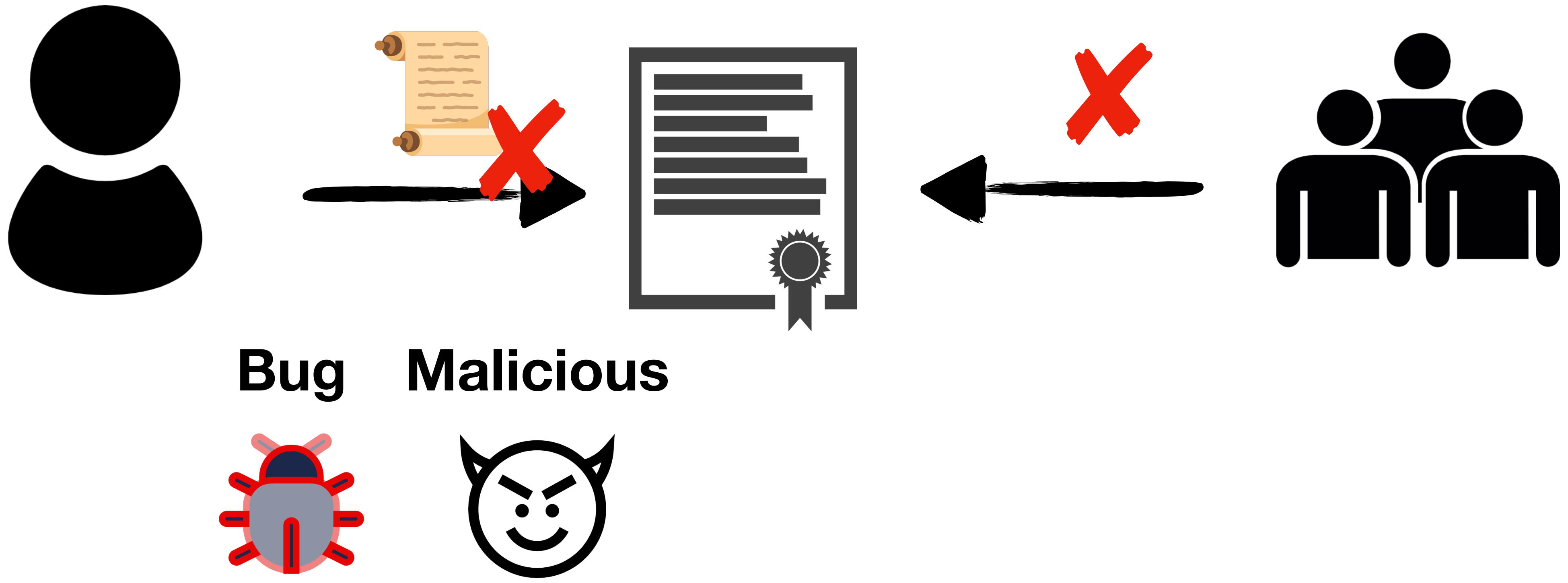
Veto



Bug

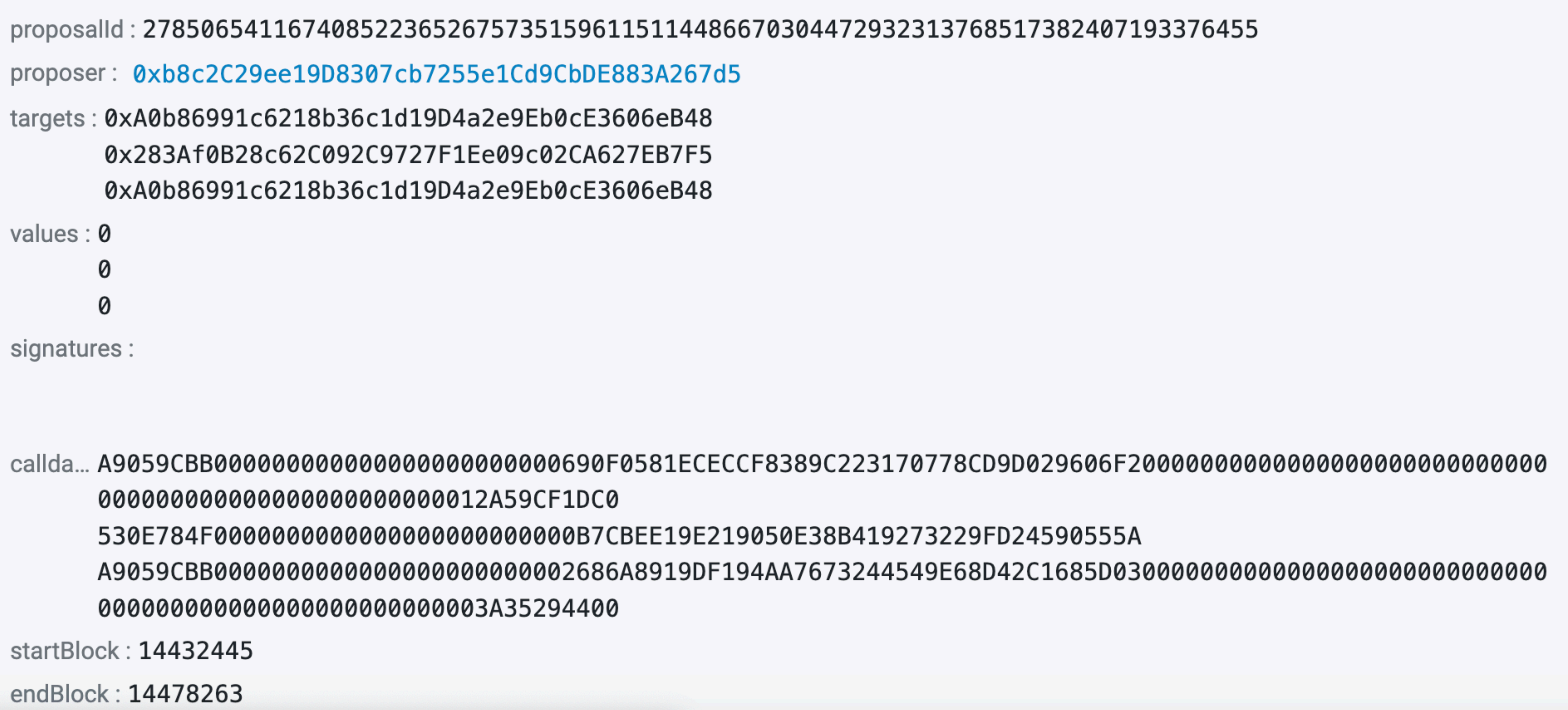
Malicious

Veto



Veto

- **Veto is needed !!!**



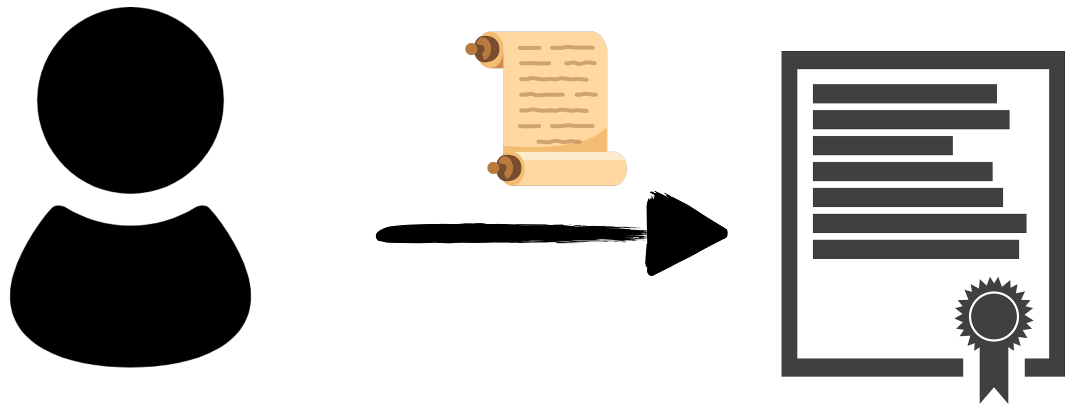
```
proposalId : 27850654116740852236526757351596115114486670304472932313768517382407193376455
proposer :  0xb8c2C29ee19D8307cb7255e1Cd9CbDE883A267d5
targets : 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
          0x283Af0B28c62C092C9727F1Ee09c02CA627EB7F5
          0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
values : 0
         0
         0
signatures :



callda… A9059CBB000000000000000000000000690F0581ECECCF8389C223170778CD9D029606F20000000000000000000000000000
        00000000000000000000000000012A59CF1DC0
        530E784F0000000000000000000000000B7CBEE19E219050E38B419273229FD24590555A
        A9059CBB0000000000000000000000002686A8919DF194AA7673244549E68D42C1685D030000000000000000000000000000
        0000000000000000000000000003A35294400
startBlock : 14432445
endBlock : 14478263
```

Veto

- **Vote Initiator**
    - The initiator of the vote can cancel the proposal

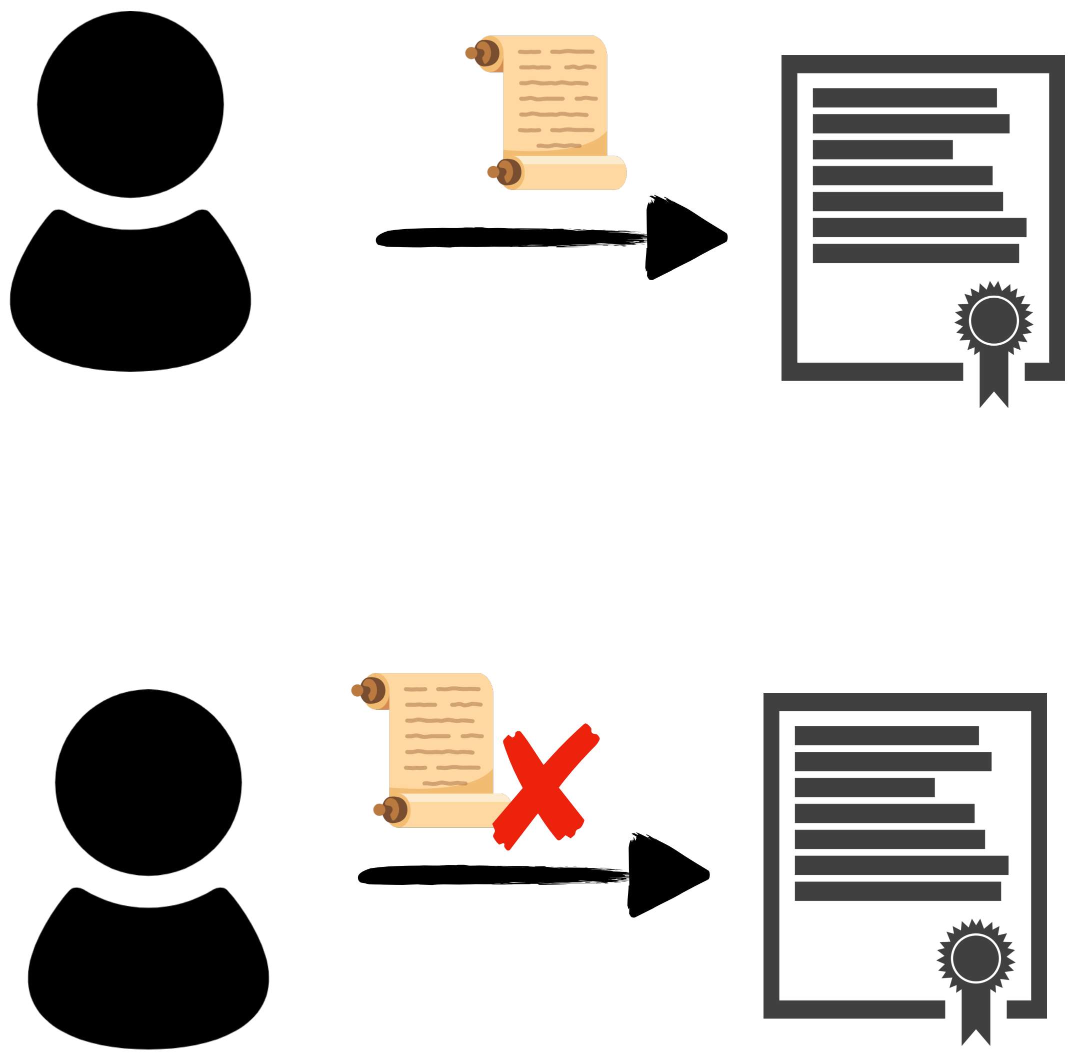
Veto

- **Vote Initiator**
    - The initiator of the vote can cancel the proposal



Veto

- **Vote Initiator**
  - The initiator of the vote can cancel the proposal

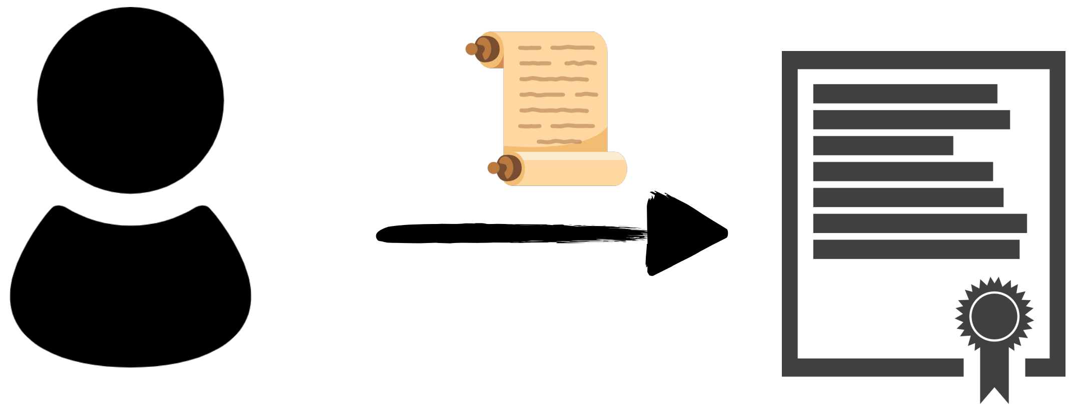


Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal

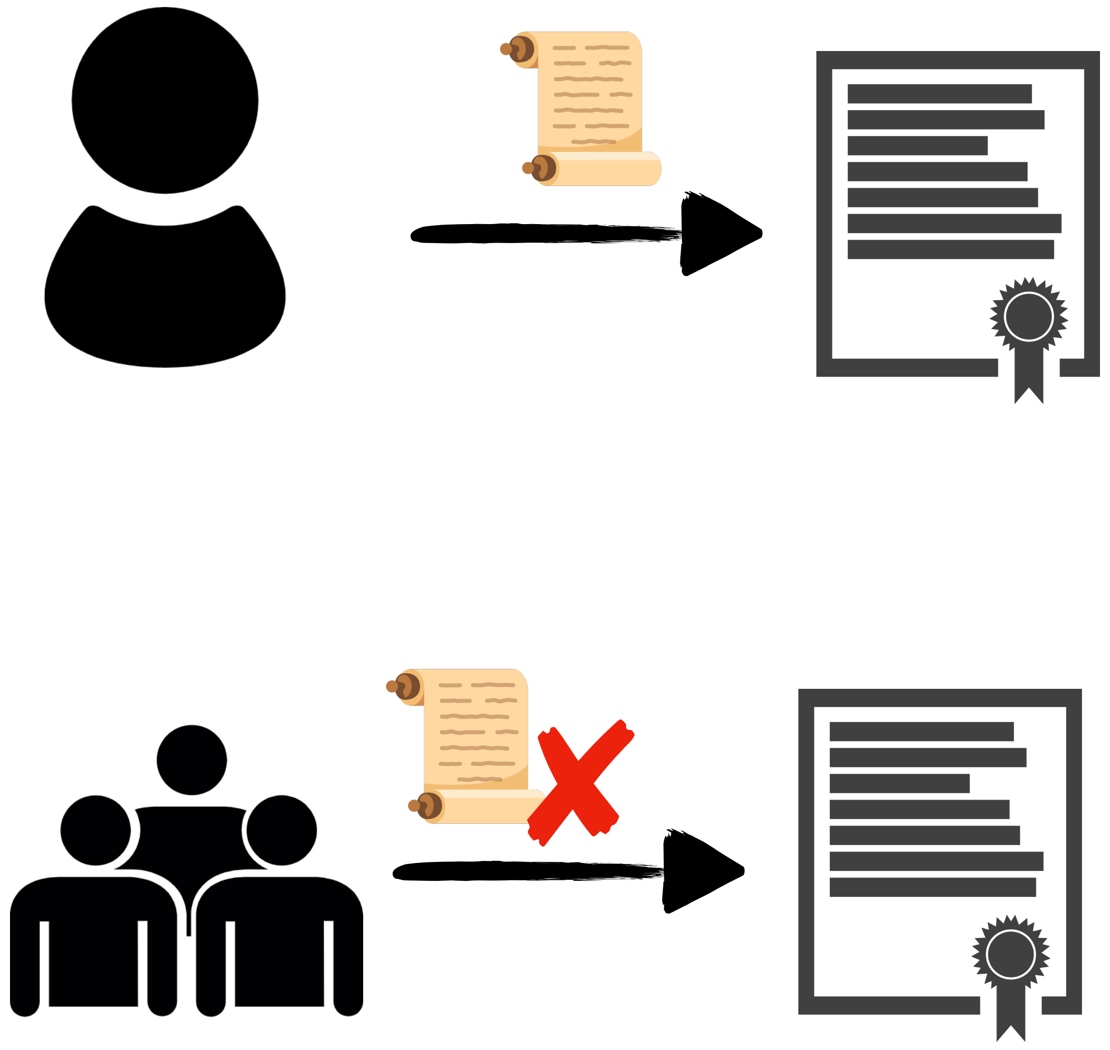
Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



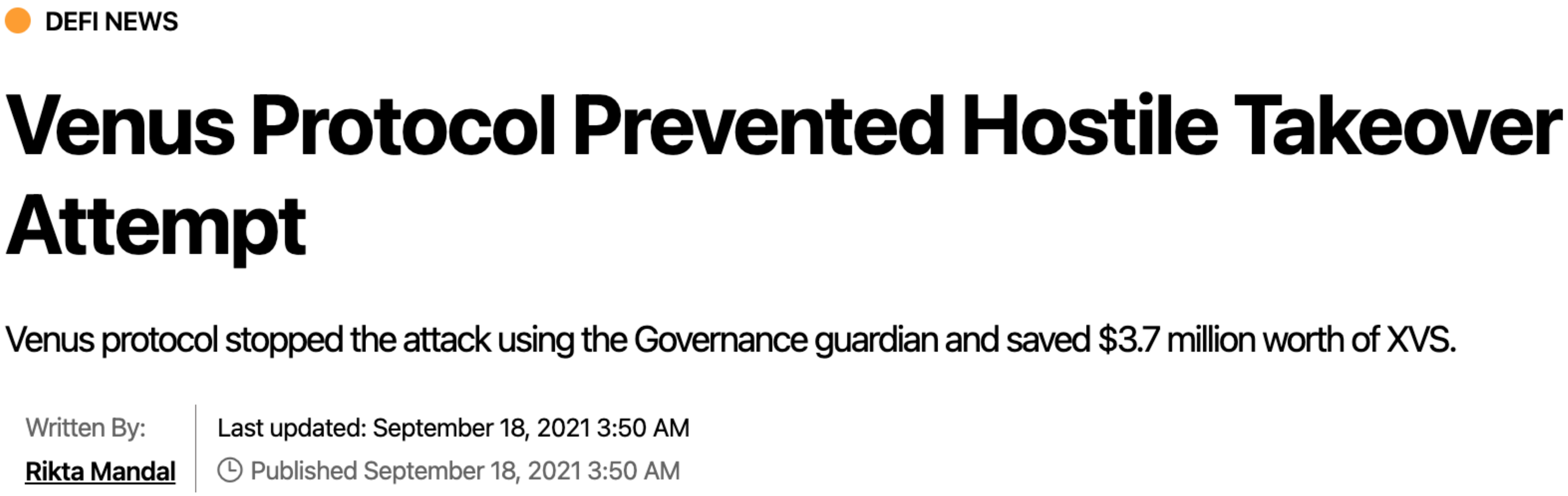
Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



DEFI NEWS

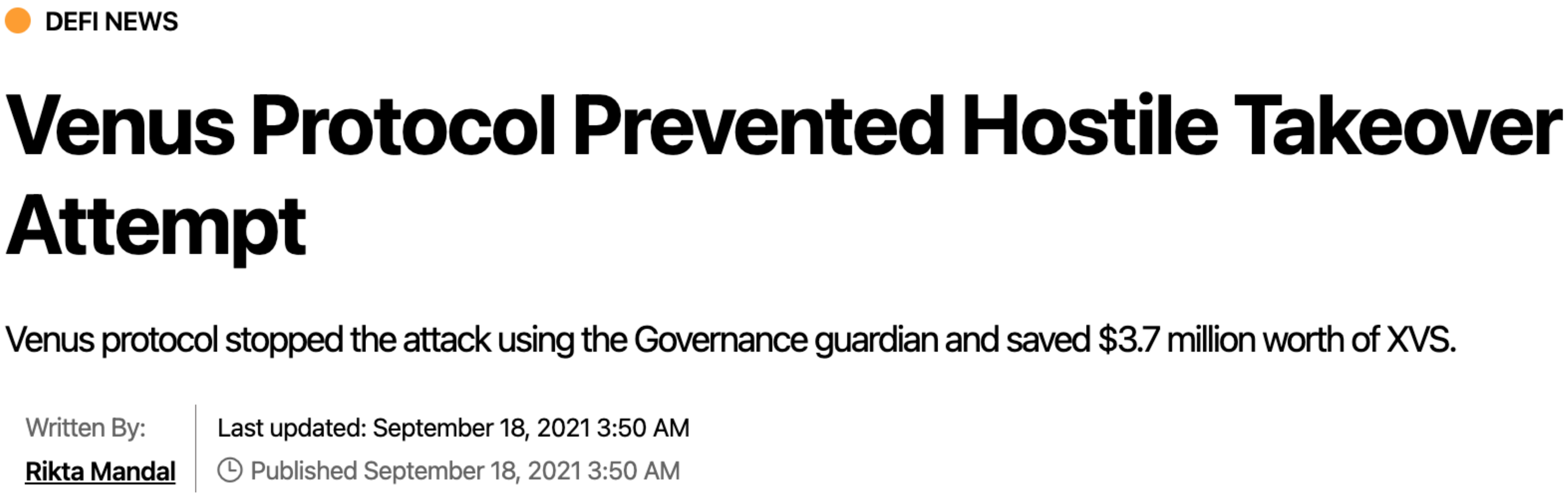
Venus Protocol Prevented Hostile Takeover Attempt

Venus protocol stopped the attack using the Governance guardian and saved $3.7 million worth of XVS.

Written By: Rikta Mandal | Last updated: September 18, 2021 3:50 AM
Published September 18, 2021 3:50 AM

Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



DEFI NEWS

Venus Protocol Prevented Hostile Takeover Attempt

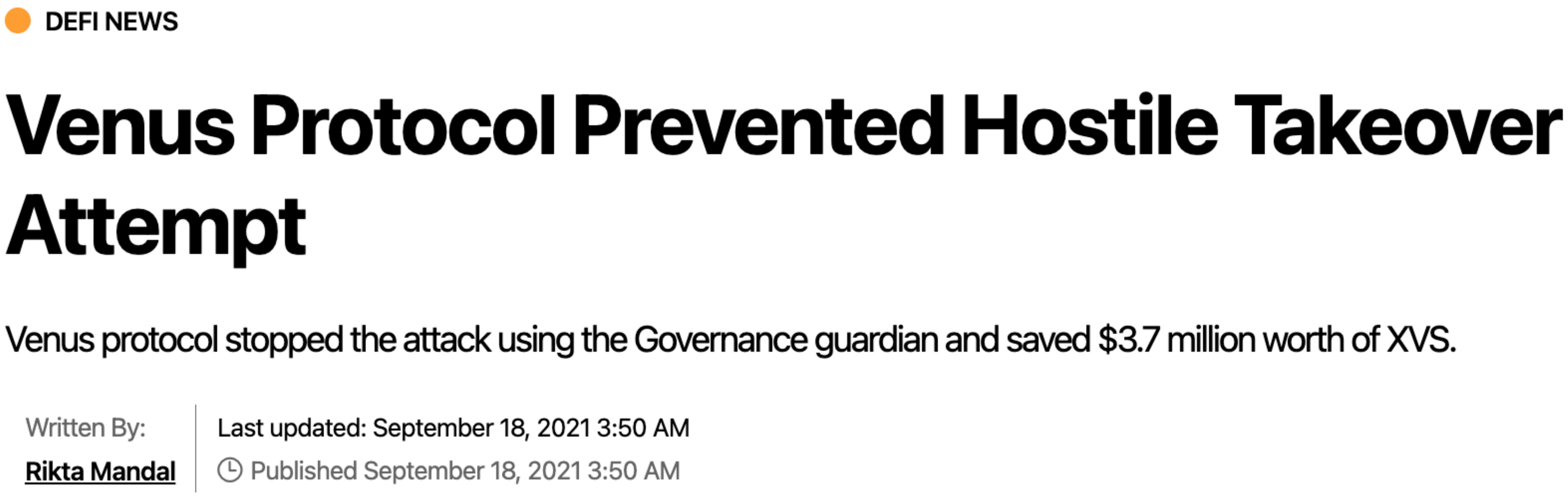
Venus protocol stopped the attack using the Governance guardian and saved $3.7 million worth of XVS.

Written By:
Rikta Mandal

Last updated: September 18, 2021 3:50 AM
Published September 18, 2021 3:50 AM

Veto

- **Veto Authority**
  - Specific authority has the power to veto any proposal



● DEFI NEWS

Venus Protocol Prevented Hostile Takeover Attempt

Venus protocol stopped the attack using the Governance guardian and saved $3.7 million worth of XVS.

Written By: Rikta Mandal | Last updated: September 18, 2021 3:50 AM
Published September 18, 2021 3:50 AM

Compound Case Study

- We can characterise what can go wrong
- Real-attack on Compound protocol to take approx. **$25 million**

Attack Timeline

Date	Amount to be taken	Votes For	Votes Against	Succeeded ?
May 6th	92,000 COMP	95.865	710.978	✗
July 15th	92,000 COMP	116.530	578.664	✗
July 24th	499,000 COMP	682.191	633.636	✓

Attack Timeline

Date	Amount to be taken	Votes For	Votes Against	Succeeded ?
May 6th	92,000 COMP	95.865	710.978	✗
July 15th	**92,000 COMP**	**116.530**	**578.664**	✗
July 24th	499,000 COMP	682.191	633.636	✓

Attack Timeline

Date	Amount to be taken	Votes For	Votes Against	Succeeded ?
May 6th	92,000 COMP	95.865	710.978	✗
July 15th	92,000 COMP	116.530	578.664	✗
July 24th	**499,000 COMP**	**682.191**	**633.636**	✓

Compound Case Study

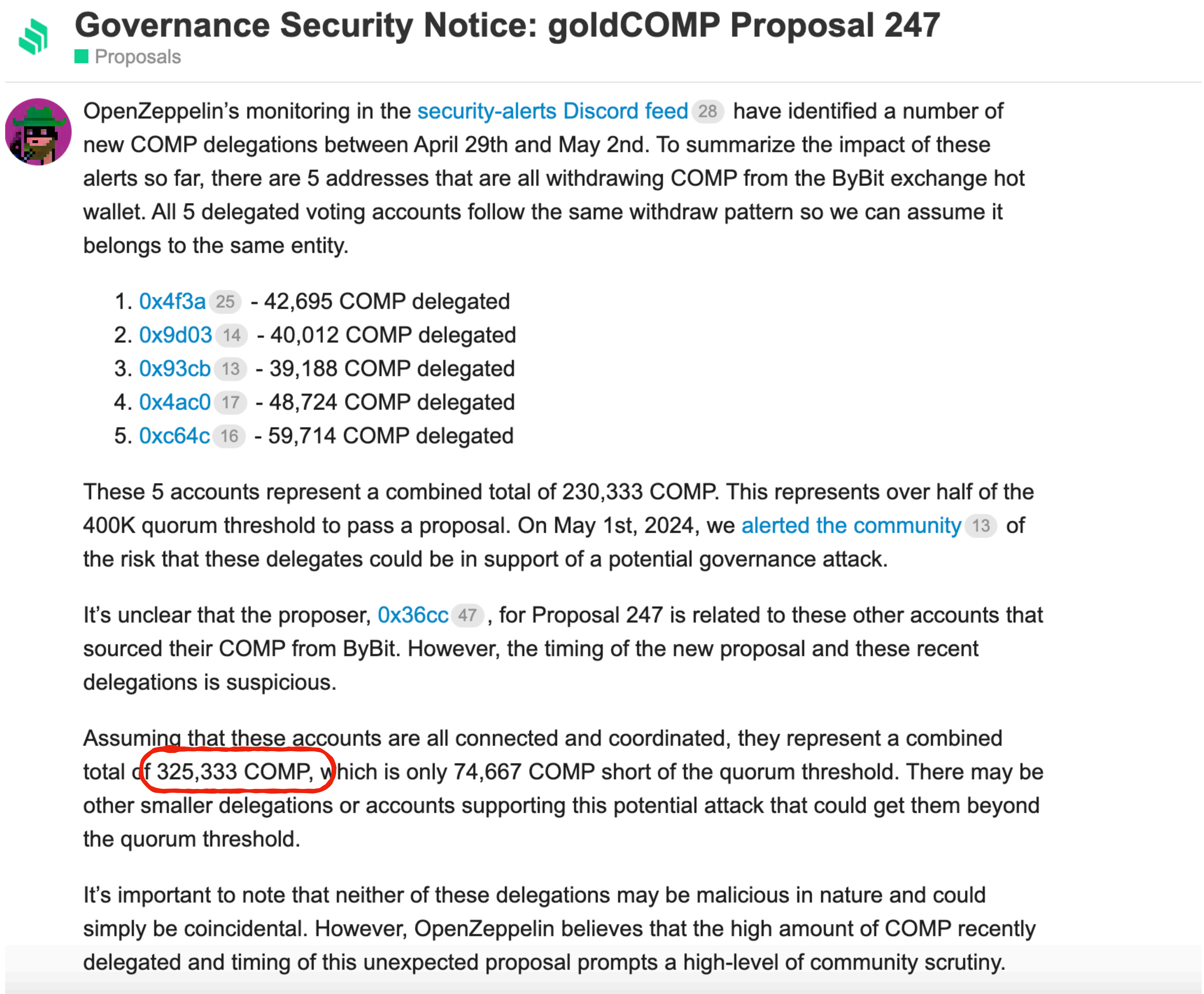
- Exploit 3 critical vulnerabilities:
    - Anonymous Registration
    - Voter Apathy and Vote Sniping
    - Lack of Oversight

Vulnerabilities

- Exploit 3 critical vulnerabilities
  - **Anonymous Registration**
  - Voter Apathy and Vote Sniping
  - Lack of Oversight

Anonymous Registration

- Nobody knew how large the malicious party was !!!



Governance Security Notice: goldCOMP Proposal 247

Proposals

OpenZeppelin's monitoring in the security-alerts Discord feed 28 have identified a number of new COMP delegations between April 29th and May 2nd. To summarize the impact of these alerts so far, there are 5 addresses that are all withdrawing COMP from the ByBit exchange hot wallet. All 5 delegated voting accounts follow the same withdraw pattern so we can assume it belongs to the same entity.

1. 0x4f3a 25 - 42,695 COMP delegated
2. 0x9d03 14 - 40,012 COMP delegated
3. 0x93cb 13 - 39,188 COMP delegated
4. 0x4ac0 17 - 48,724 COMP delegated
5. 0xc64c 16 - 59,714 COMP delegated

These 5 accounts represent a combined total of 230,333 COMP. This represents over half of the 400K quorum threshold to pass a proposal. On May 1st, 2024, we alerted the community 13 of the risk that these delegates could be in support of a potential governance attack.

It's unclear that the proposer, 0x36cc 47 , for Proposal 247 is related to these other accounts that sourced their COMP from ByBit. However, the timing of the new proposal and these recent delegations is suspicious.

Assuming that these accounts are all connected and coordinated, they represent a combined total of 325,333 COMP, which is only 74,667 COMP short of the quorum threshold. There may be other smaller delegations or accounts supporting this potential attack that could get them beyond the quorum threshold.

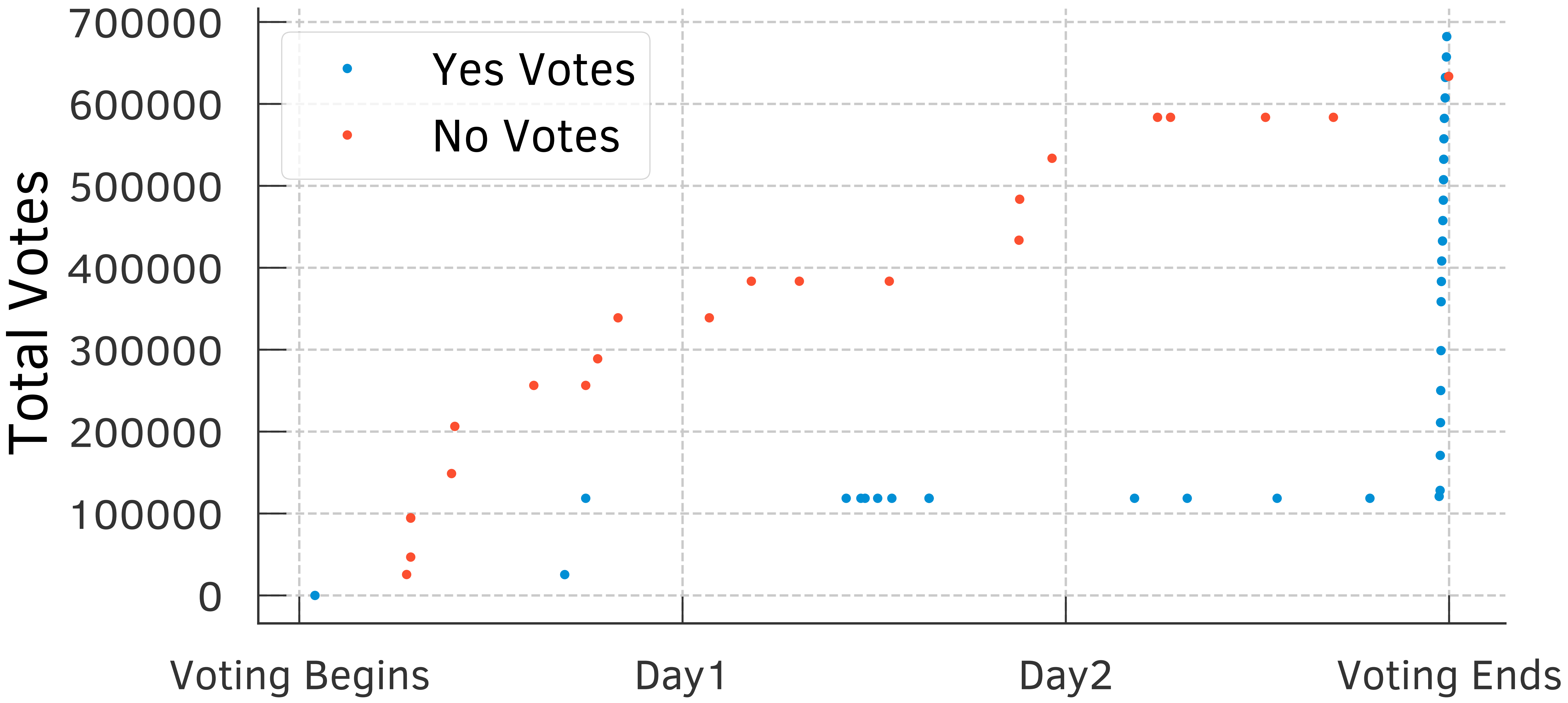
It's important to note that neither of these delegations may be malicious in nature and could simply be coincidental. However, OpenZeppelin believes that the high amount of COMP recently delegated and timing of this unexpected proposal prompts a high-level of community scrutiny.

Vulnerabilities

- Exploit 3 critical vulnerabilities
  - Anonymous Registration
  - **Voter Apathy and Vote Sniping**
  - Lack of Oversight

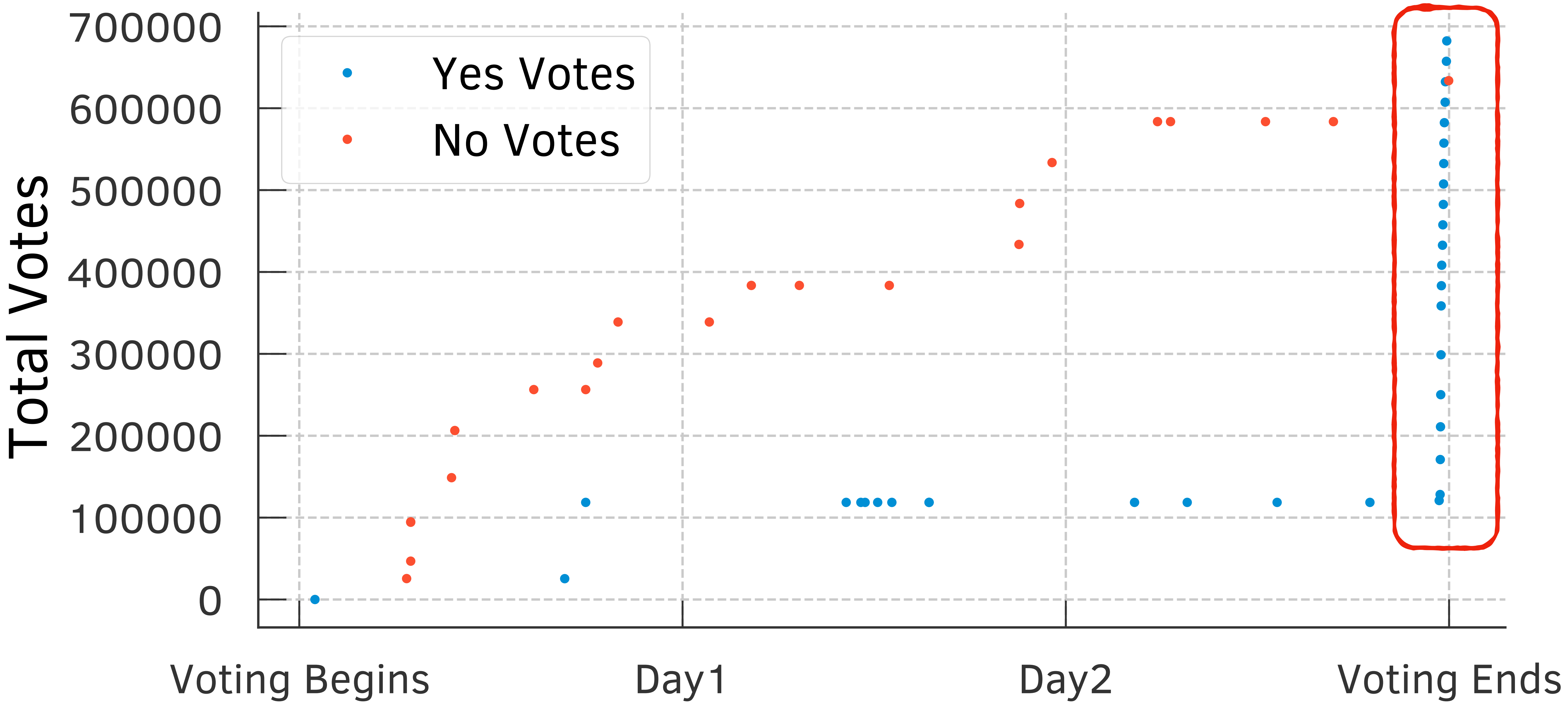
Voter Apathy and Vote Sniping

- On-chain voting has a cost
- Over **582,000 Votes (over 82%)** were cast in the last 30 minutes



Voter Apathy and Vote Sniping

- On-chain voting has a cost
- Over **582,000 Votes (over 82%)** were cast in the last 30 minutes



Vulnerabilities

- Exploit 3 critical vulnerabilities
  - Anonymous Registration
  - Voter Apathy and Vote Sniping
  - **Lack of Oversight**

Lack of Oversight

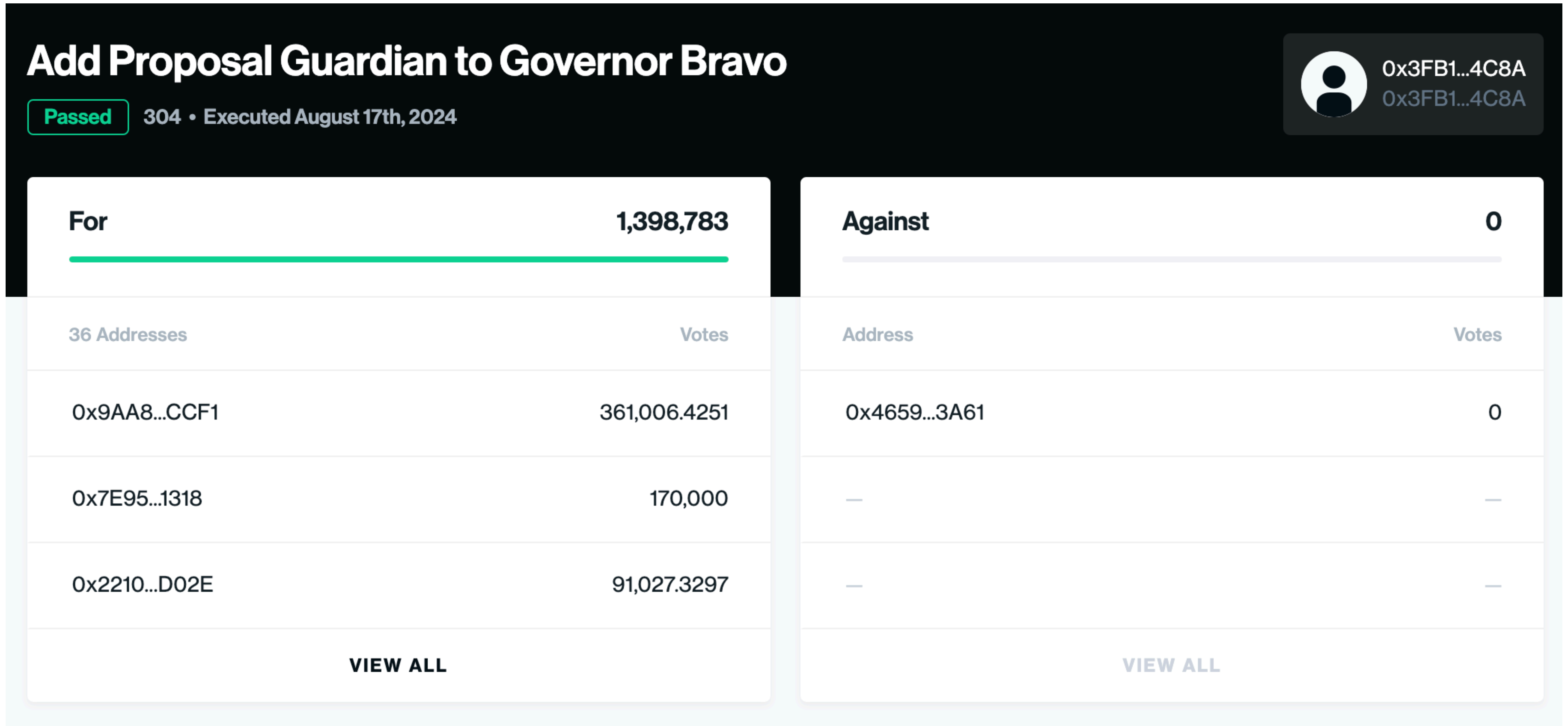
- **No Veto Authority !!!**

Lack of Oversight

- **No Veto Authority !!!**
- In response, Compound added a vetoer.

Lack of Oversight

- **No Veto Authority !!!**
- In response, Compound added a vetoer.



Add Proposal Guardian to Governor Bravo

Passed 304 • Executed August 17th, 2024

0x3FB1...4C8A
0x3FB1...4C8A

For	1,398,783
36 Addresses	Votes
0x9AA8...CCF1	361,006.4251
0x7E95...1318	170,000
0x2210...D02E	91,027.3297

VIEW ALL

Against	0
Address	Votes
0x4659...3A61	0
—	—
—	—

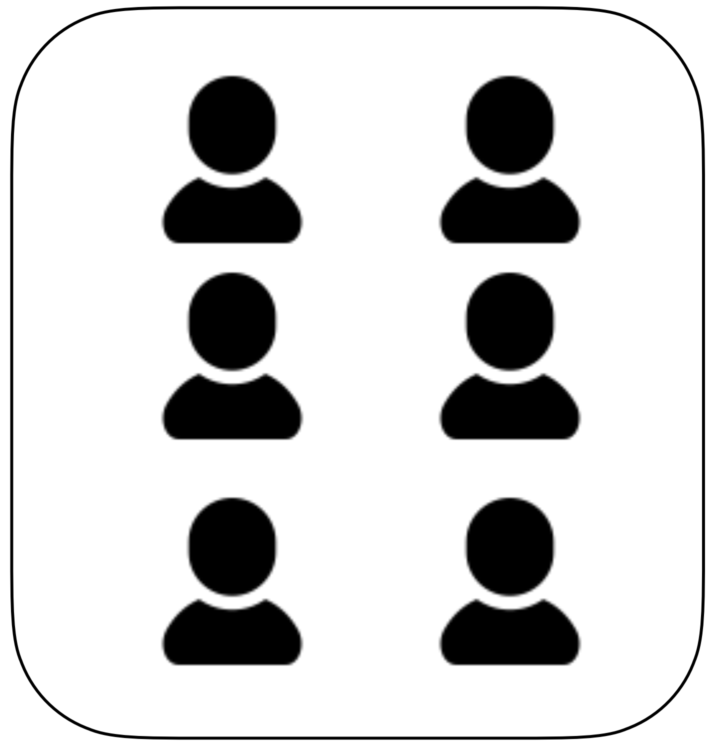
VIEW ALL

Conclusion

- Classified DAOs along different security critical dimensions
  - Decentralisation vs Security

Conclusion

- Classified DAOs along different security critical dimensions
    - Decentralisation vs Security

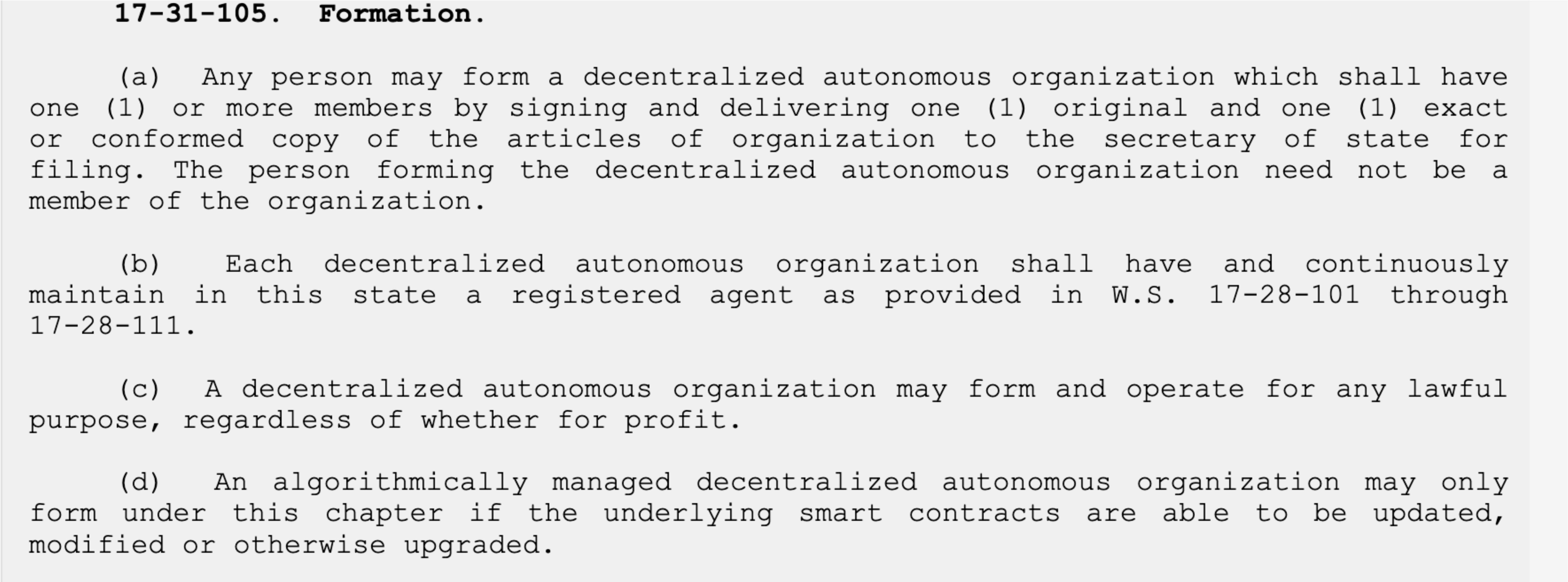


Conclusion

- Classified DAOs along different security critical dimensions
    - Decentralisation vs Security

Conclusion

- *“An algorithmically managed decentralized autonomous organisation may only form under this chapter if the underlying smart contracts are able to be updated, modified or otherwise upgraded”*



17-31-105. Formation.

(a) Any person may form a decentralized autonomous organization which shall have one (1) or more members by signing and delivering one (1) original and one (1) exact or conformed copy of the articles of organization to the secretary of state for filing. The person forming the decentralized autonomous organization need not be a member of the organization.

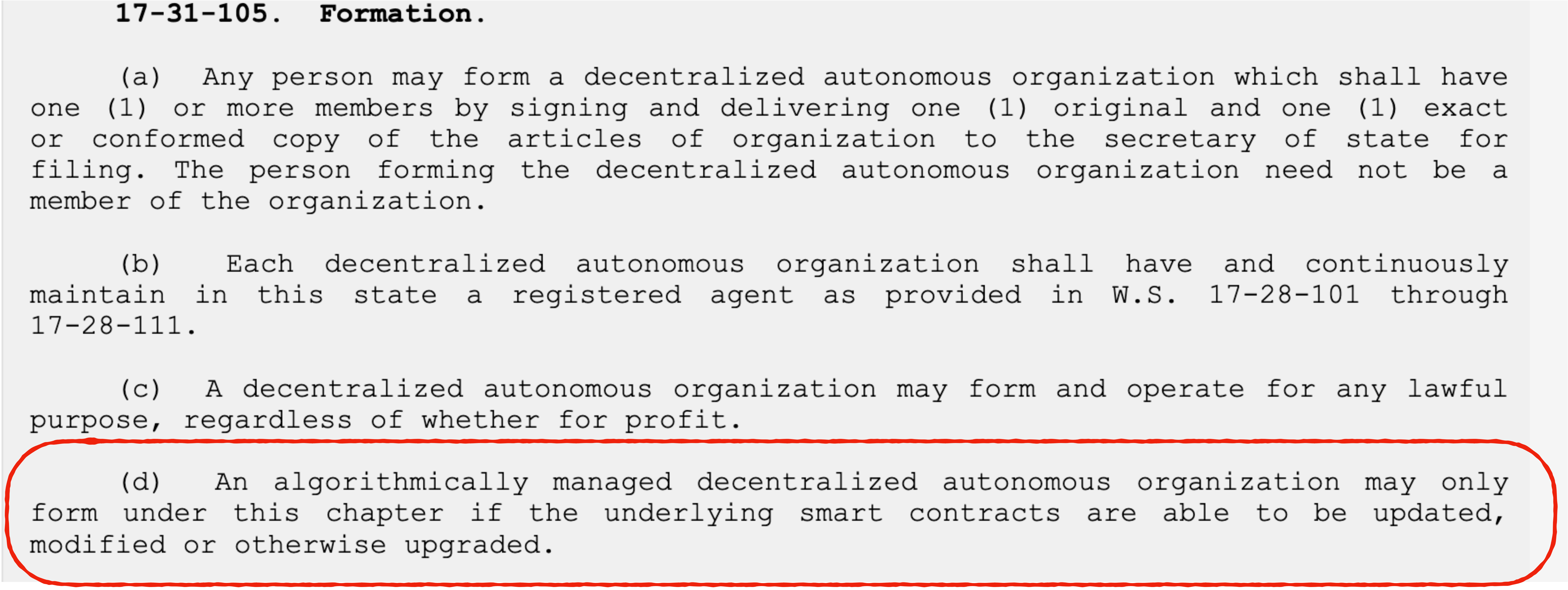
(b) Each decentralized autonomous organization shall have and continuously maintain in this state a registered agent as provided in W.S. 17-28-101 through 17-28-111.

(c) A decentralized autonomous organization may form and operate for any lawful purpose, regardless of whether for profit.

(d) An algorithmically managed decentralized autonomous organization may only form under this chapter if the underlying smart contracts are able to be updated, modified or otherwise upgraded.

Conclusion

- *"An algorithmically managed decentralized autonomous organisation may only form under this chapter if the underlying smart contracts are able to be updated, modified or otherwise upgraded"*



17-31-105. Formation.

(a) Any person may form a decentralized autonomous organization which shall have one (1) or more members by signing and delivering one (1) original and one (1) exact or conformed copy of the articles of organization to the secretary of state for filing. The person forming the decentralized autonomous organization need not be a member of the organization.

(b) Each decentralized autonomous organization shall have and continuously maintain in this state a registered agent as provided in W.S. 17-28-101 through 17-28-111.

(c) A decentralized autonomous organization may form and operate for any lawful purpose, regardless of whether for profit.

(d) An algorithmically managed decentralized autonomous organization may only form under this chapter if the underlying smart contracts are able to be updated, modified or otherwise upgraded.