# AStERISK: Auction-based Shared Economy ResolutIon System for blocKchain

Alberto Sonnino, Michał Król, Argyrios Tasiopoulos, Ioannis Psaras

University College London

# Cloud Computing

# Cloud Computing

privacy issues

SPOF

position abuse

## Cloud Computing

privacy issues

SPOF

position abuse

## Sharing Economy

## Cloud Computing

privacy issues

SPOF

position abuse

## Sharing Economy

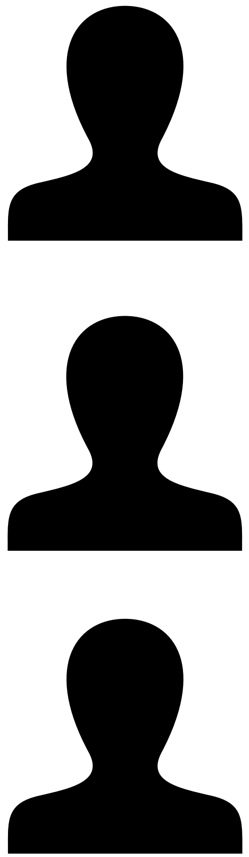
computation

storage

content

# Assignment problem

# Assignment problem

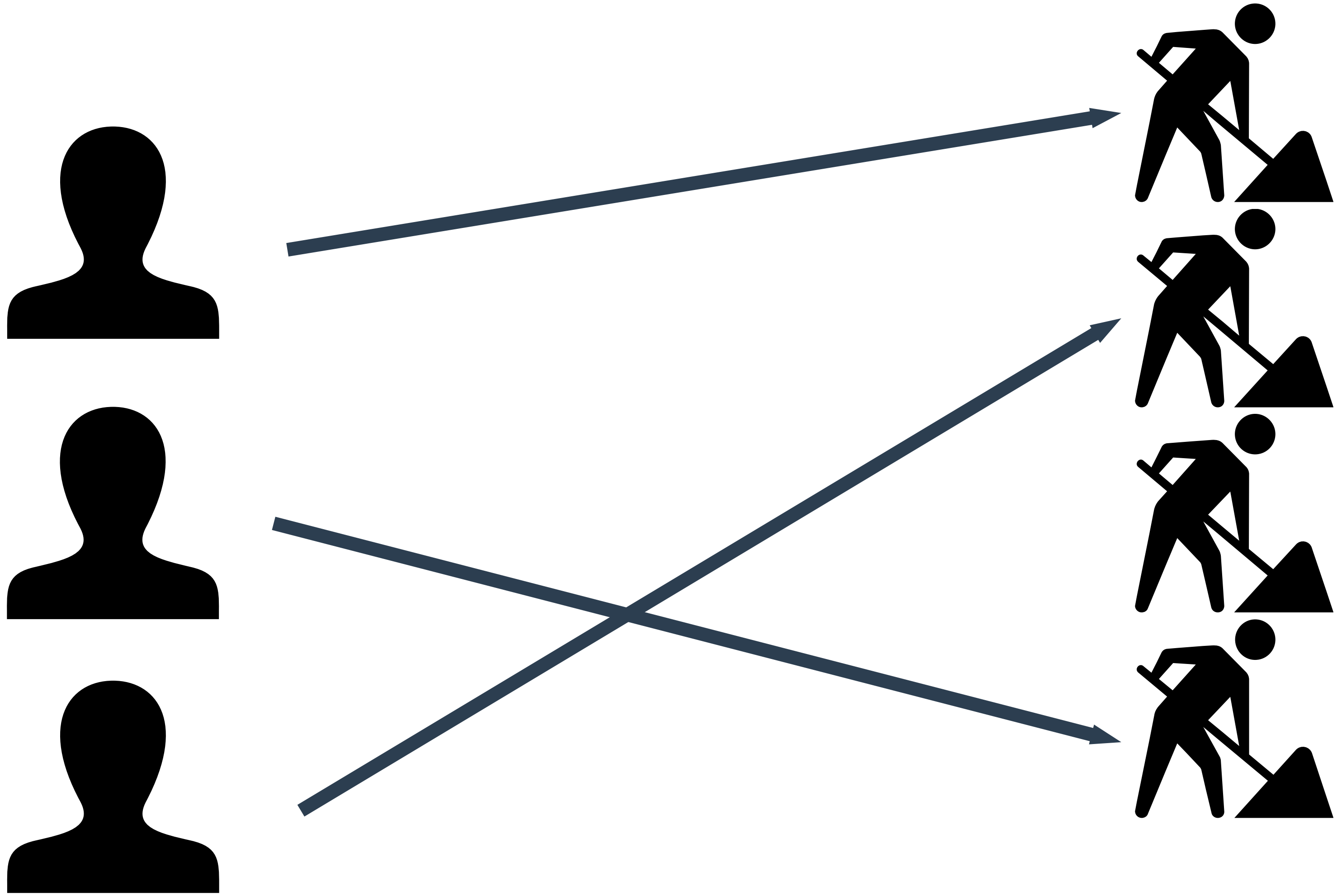


# Assignment problem

requesters

workers

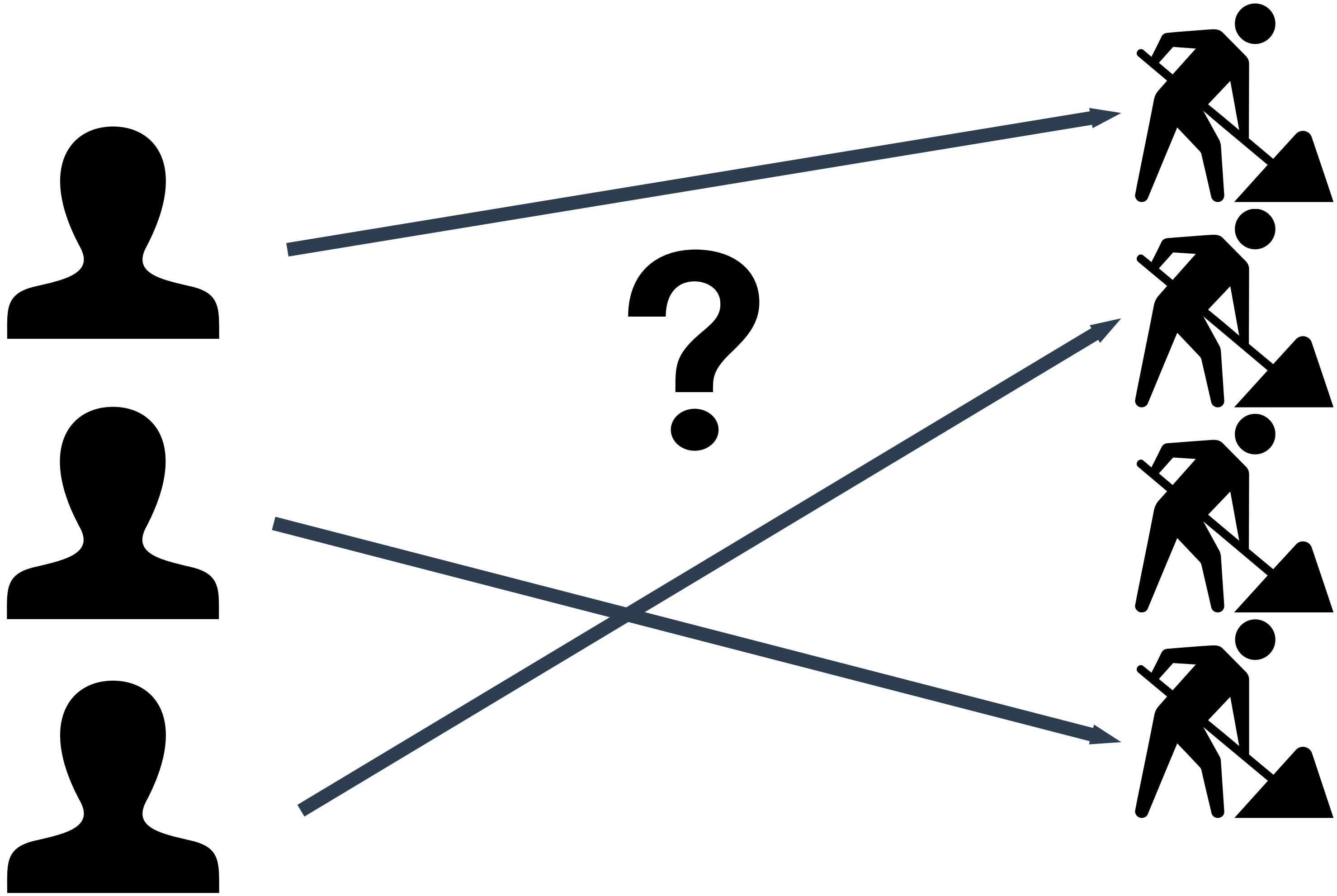
# Assignment problem



requesters

workers

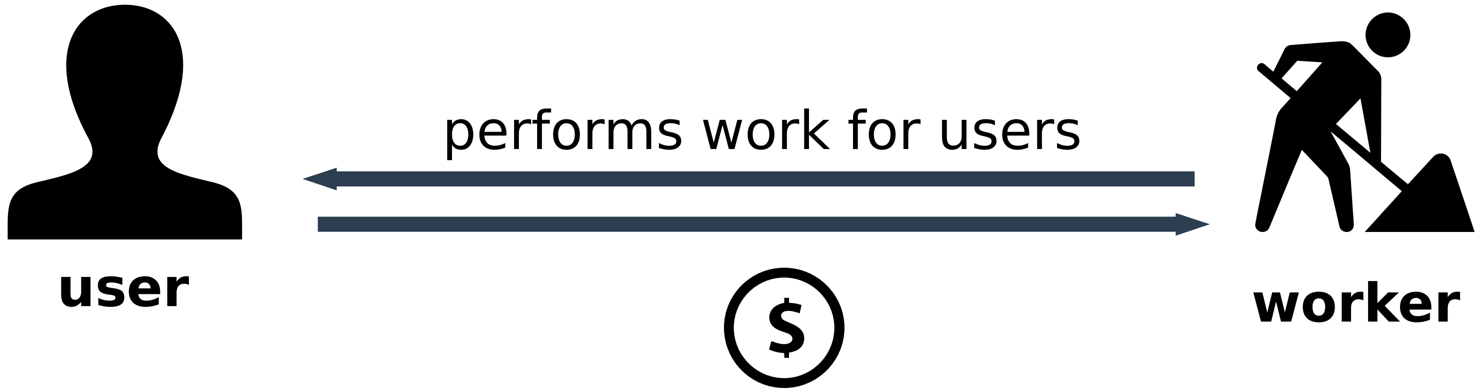
# Assignment problem



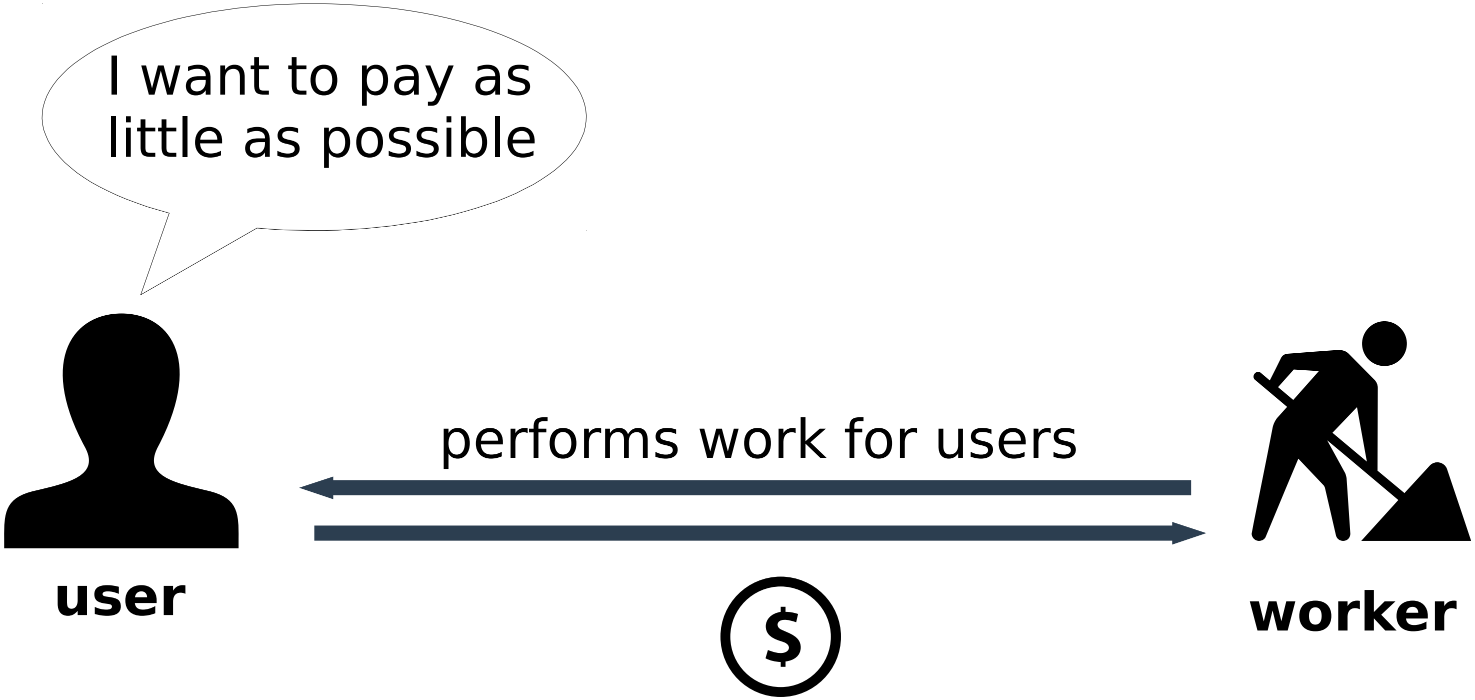
requesters

workers

# Optimal price determination



# Optimal price determination



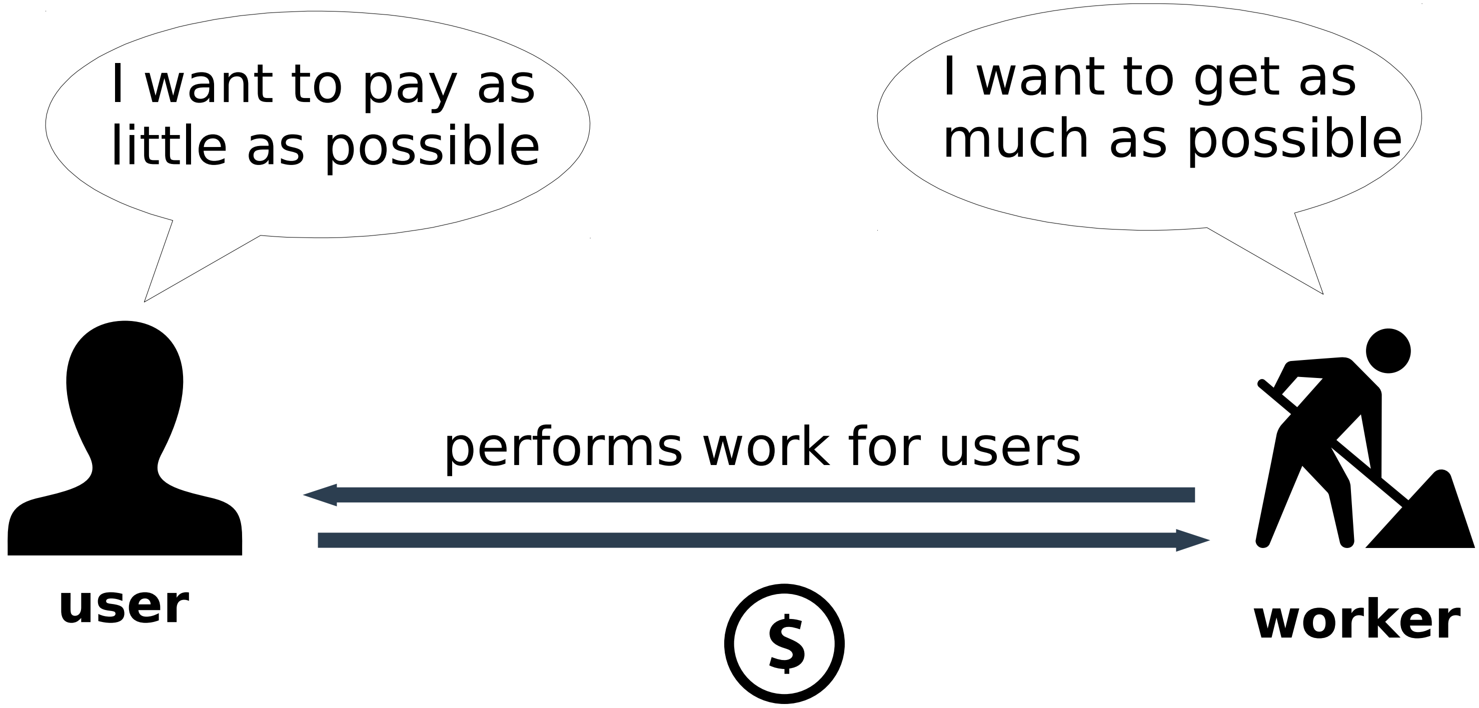
I want to pay as little as possible

performs work for users

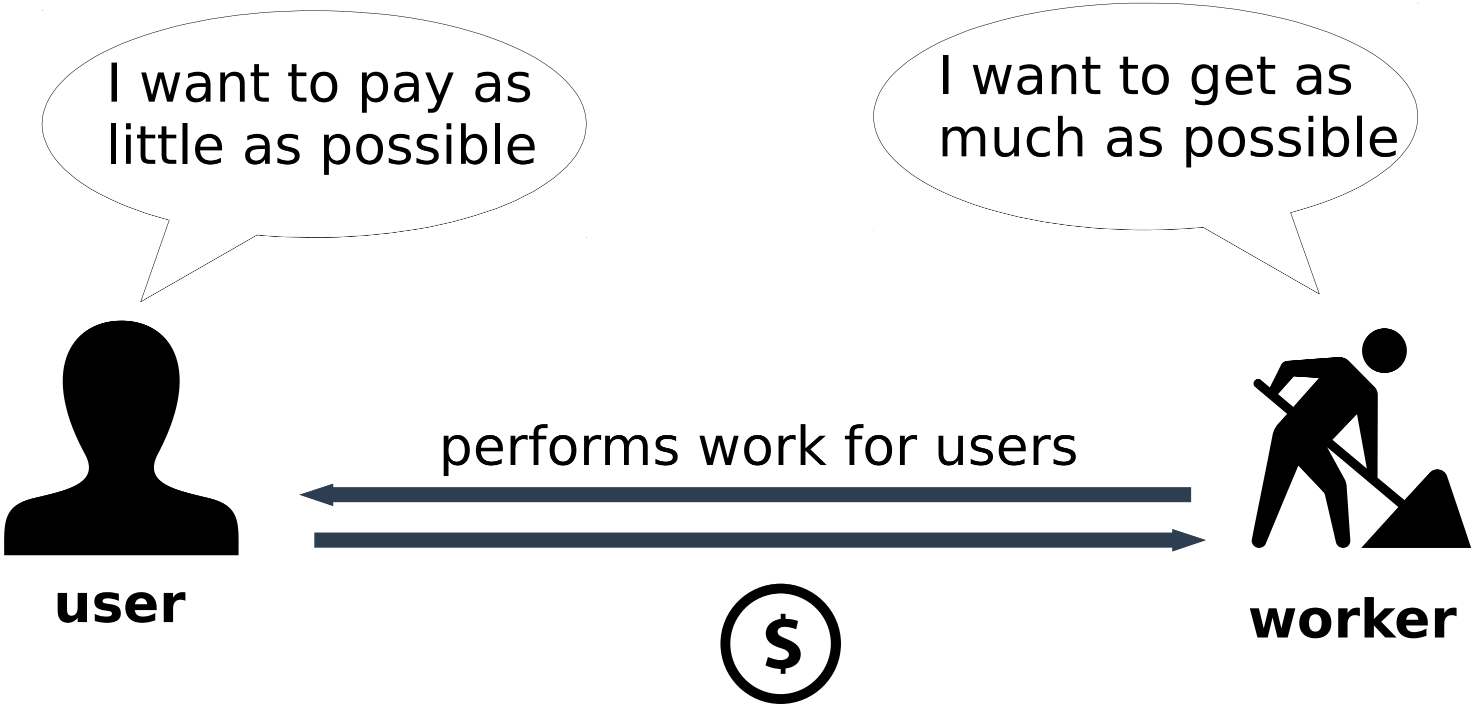
user

worker

# Optimal price determination


I want to pay as little as possible
I want to get as much as possible
performs work for users
user
$
worker

# Optimal price determination



I want to pay as little as possible

I want to get as much as possible

performs work for users

user

worker

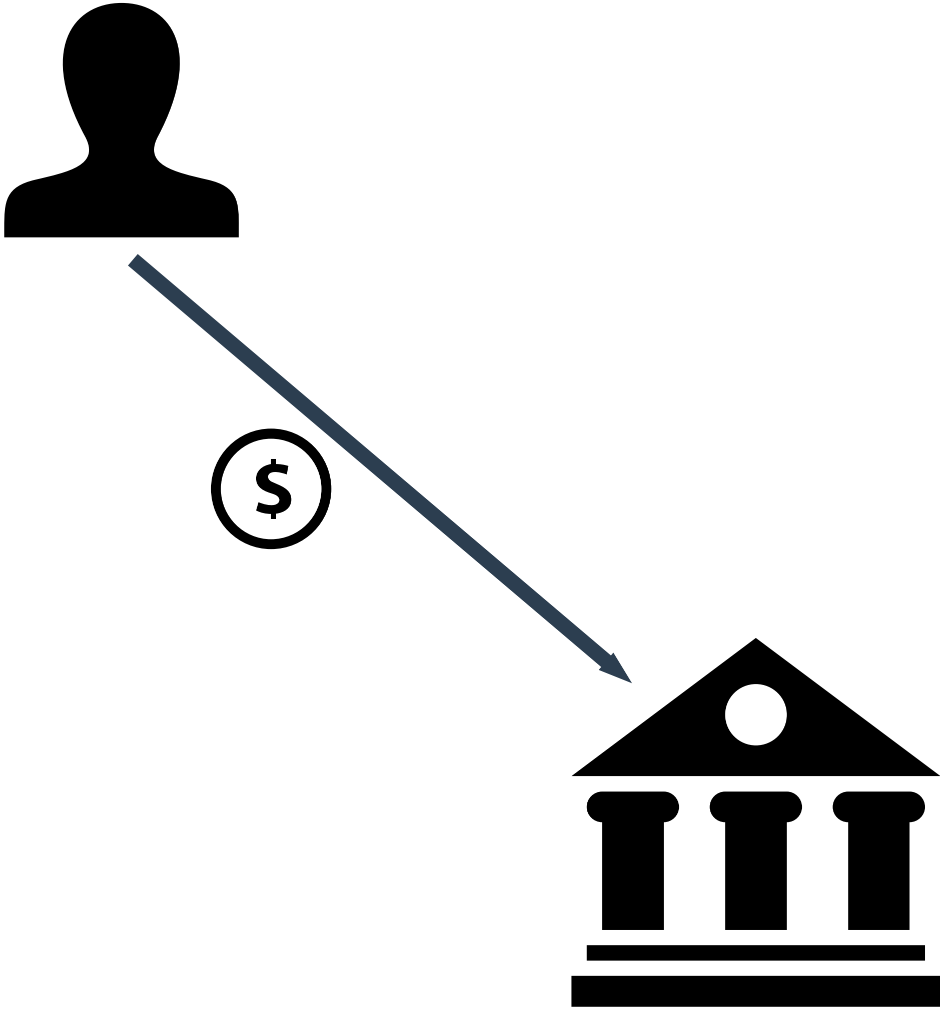
Why not run a distributed auction?!

# Auctions on Blockchain

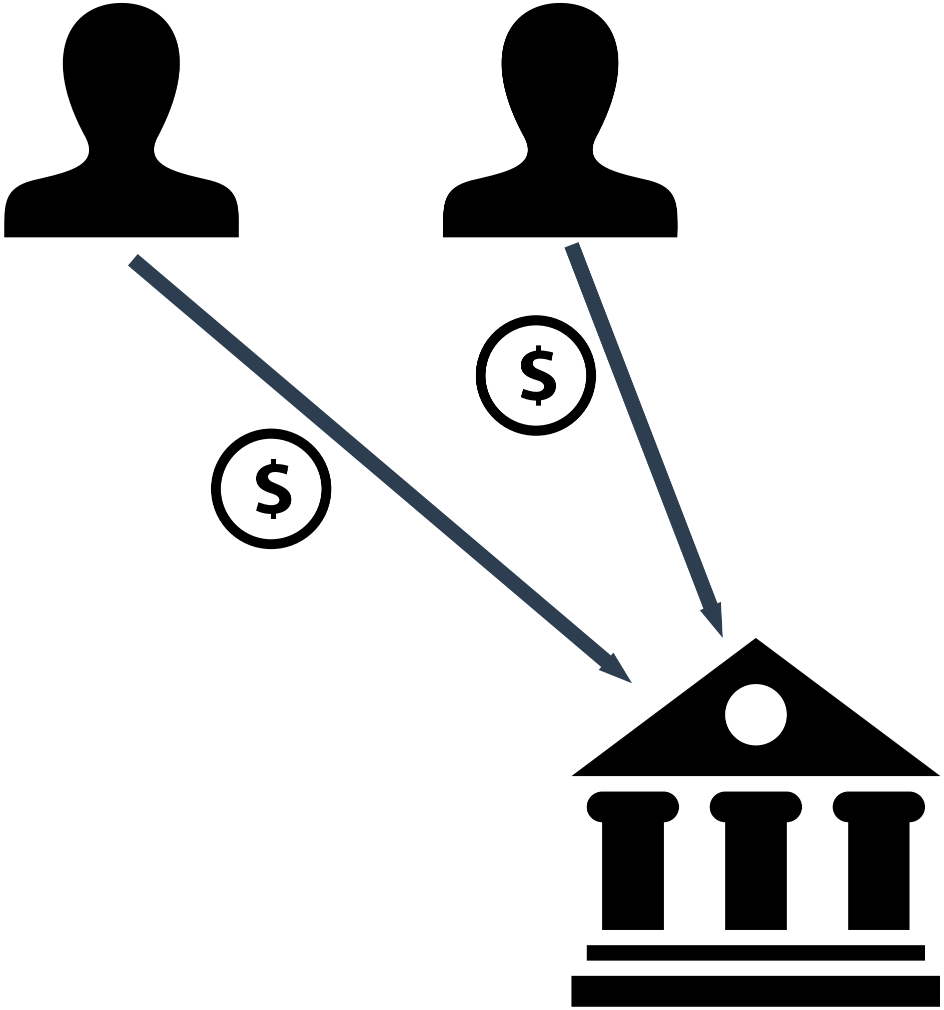
- Inherit security guarantees from the underlying blockchain
- No single 3rd trusted party
- Data submitted to the blockchain automatically becomes public

# Bids privacy

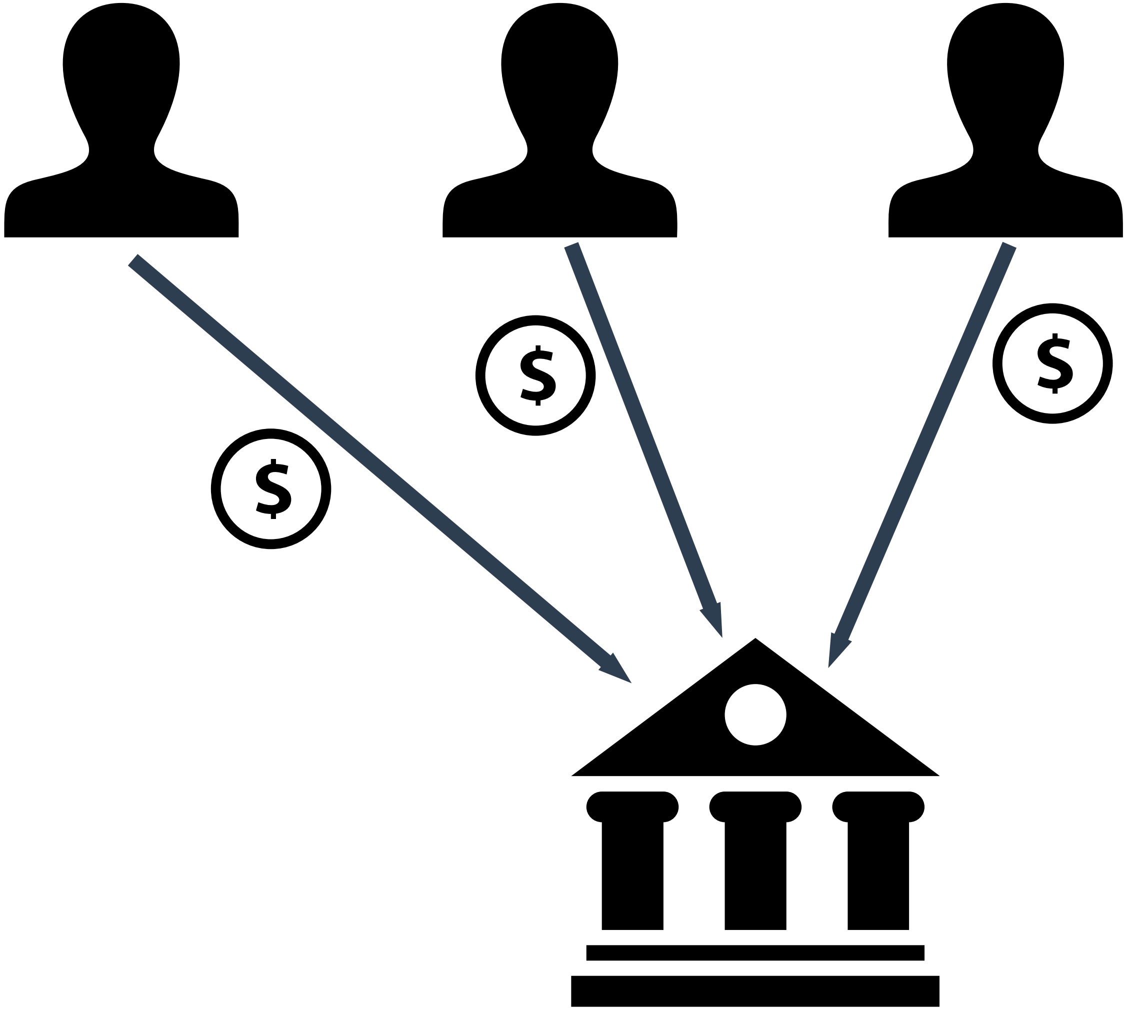
# Bids privacy



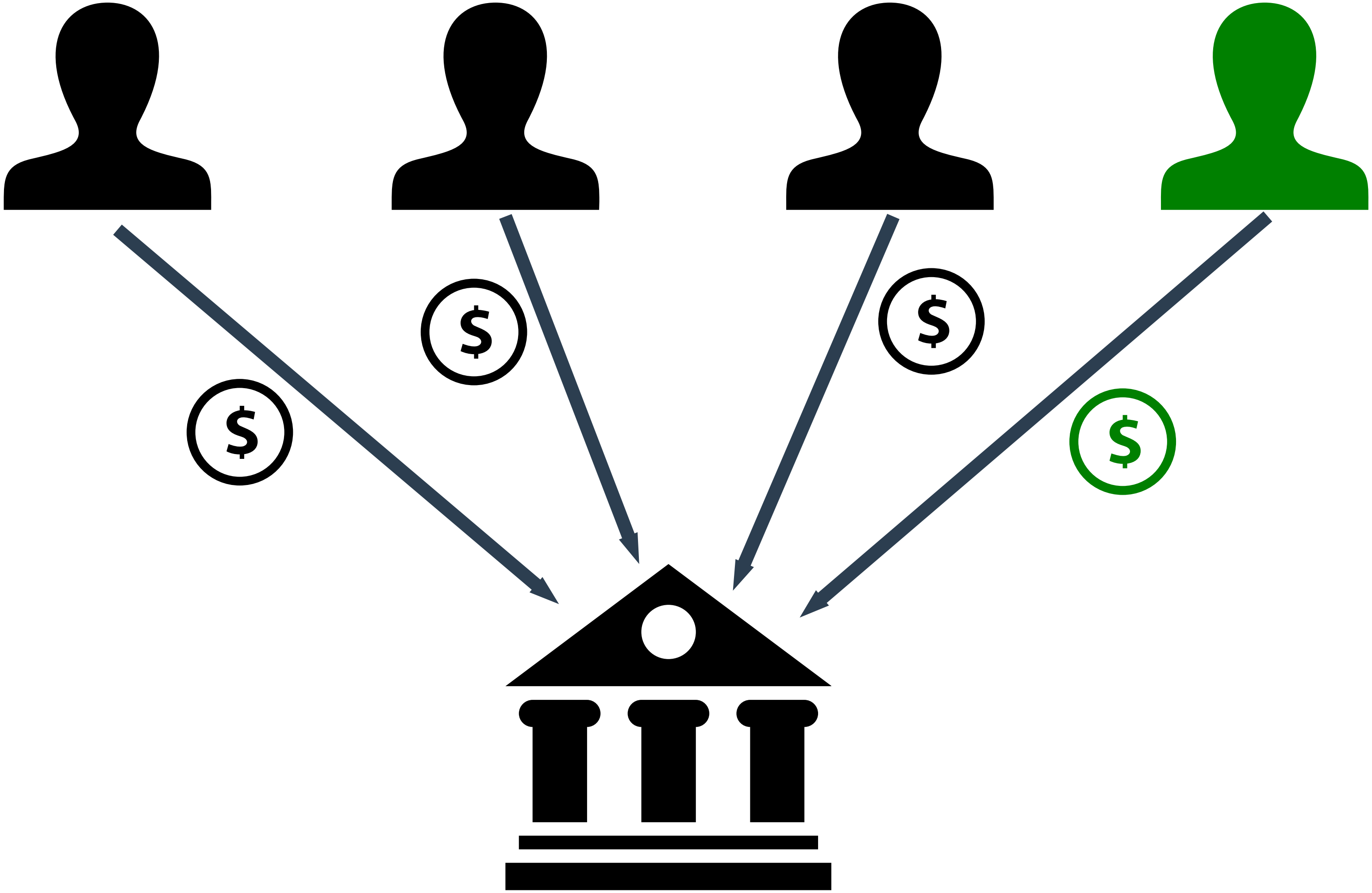
# Bids privacy



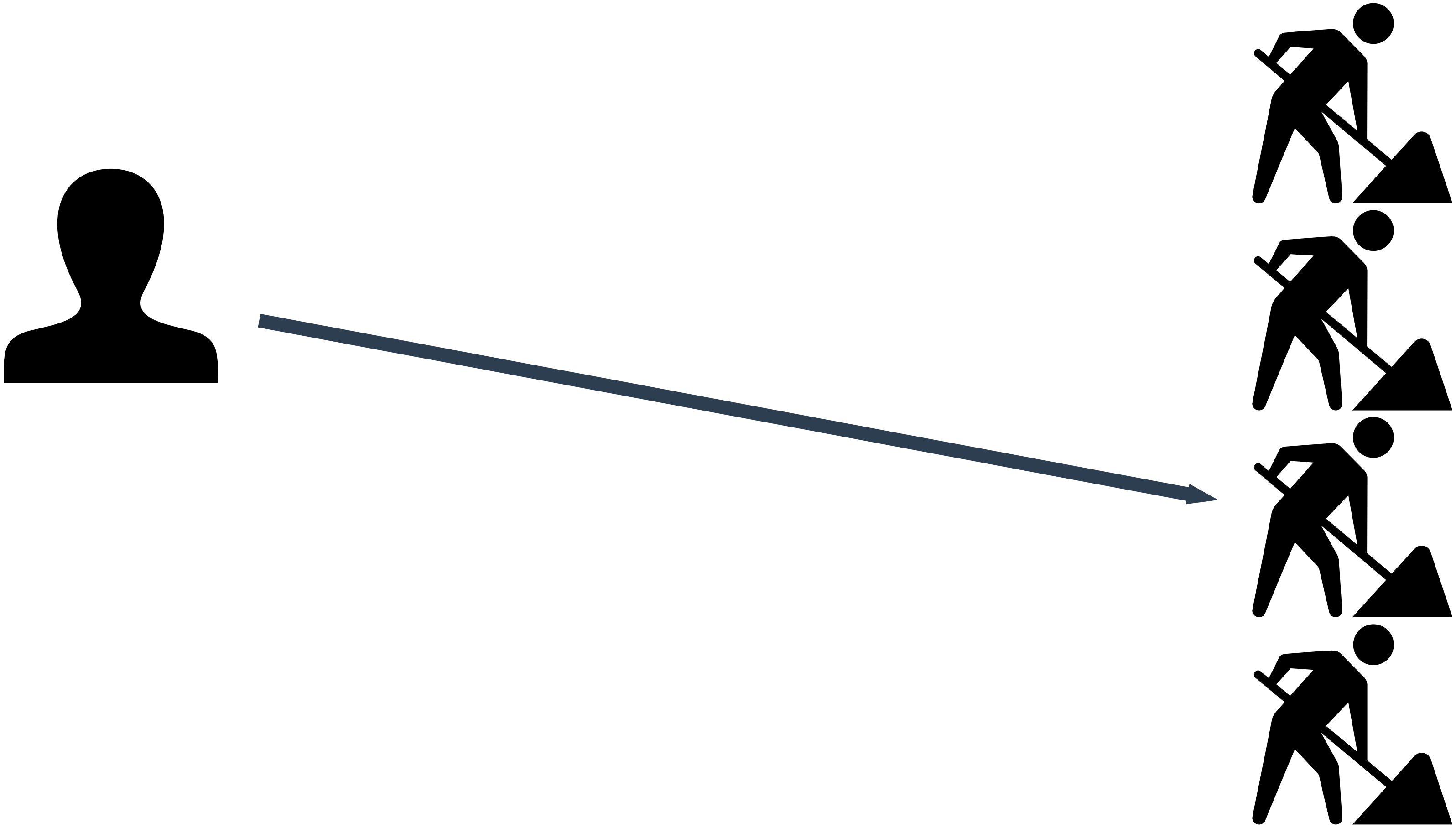
# Bids privacy



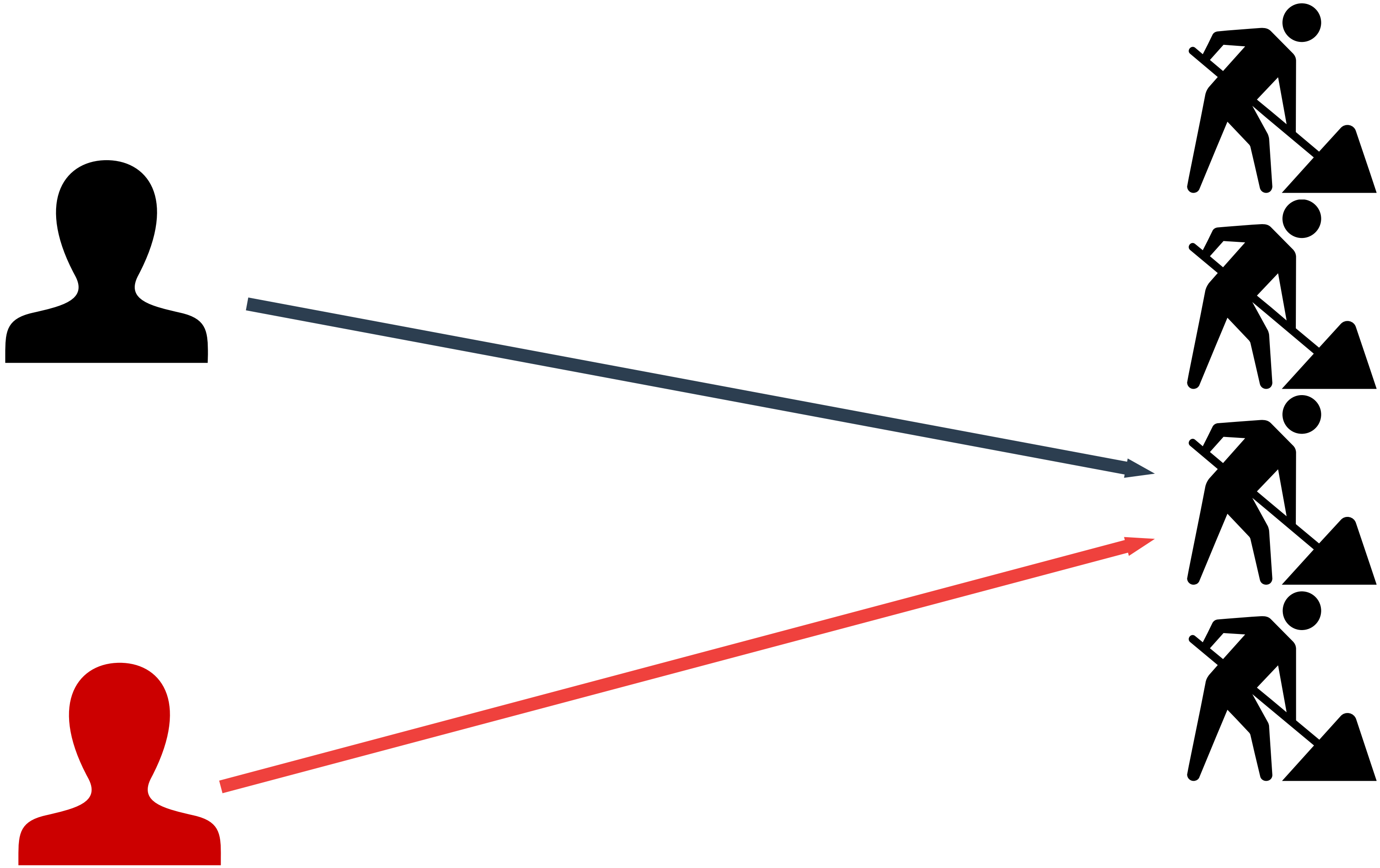
# Bids privacy



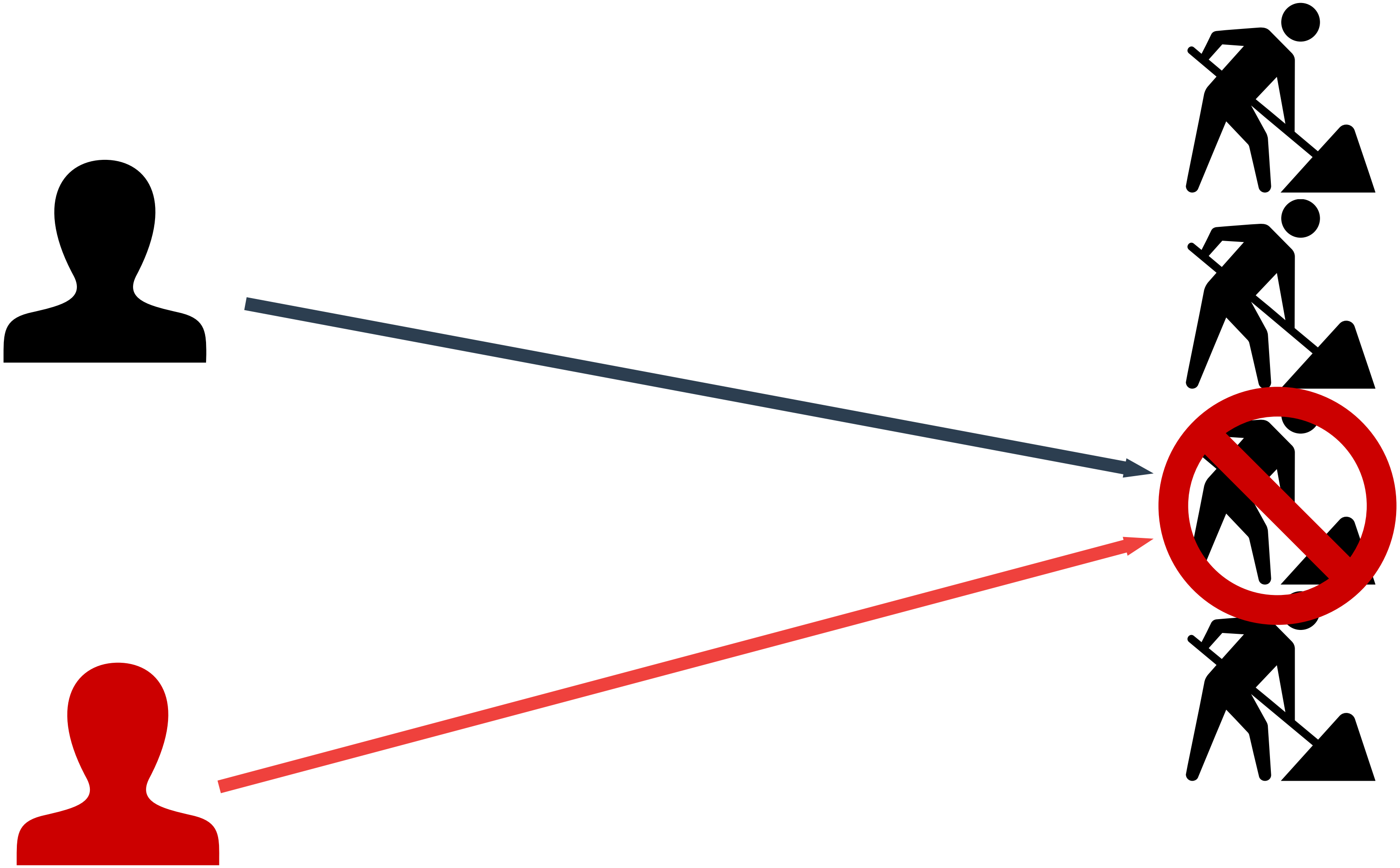
# Bidders privacy



# Bidders privacy



# Bidders privacy

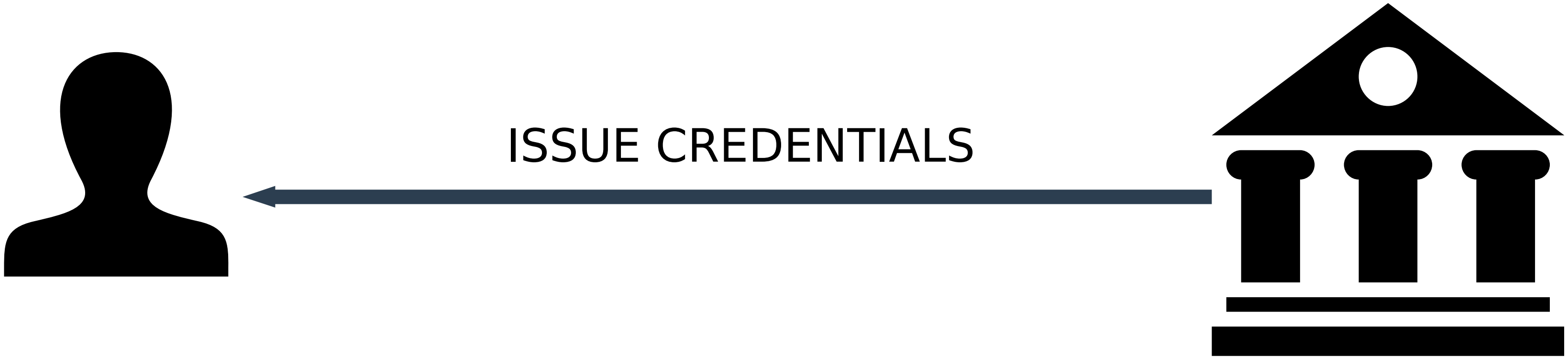


# Asterisk

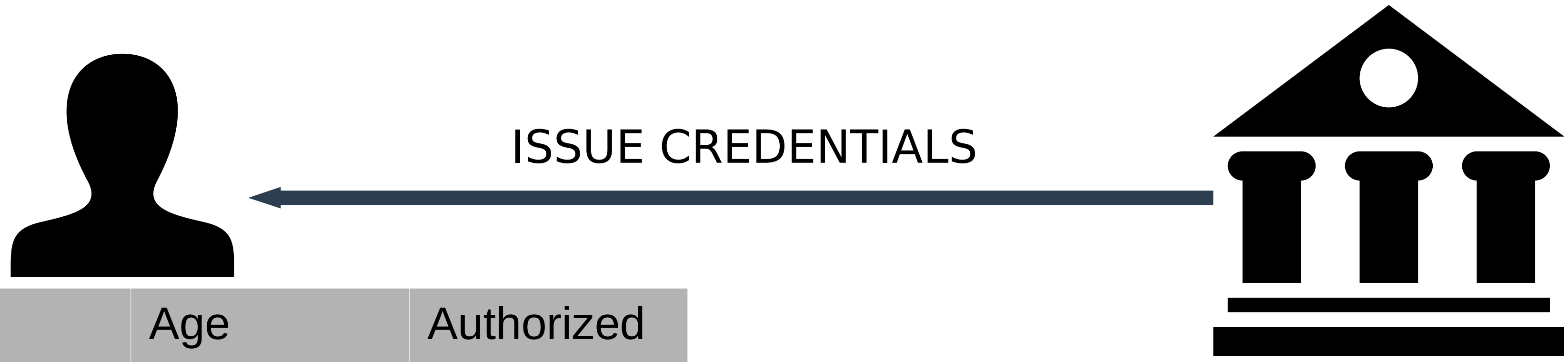
- Auction-based shared economy resolution system running on top of blockchain
- Hides submitted bids/minimum price and protects bidders identity
- Does not rely on a single trusted 3rd party
- Allows workers to automatically claim money upon submission of a proof of useful work
- Designed for Filecoin, but can be used with other systems

# Anonymous Credentials

# Anonymous Credentials

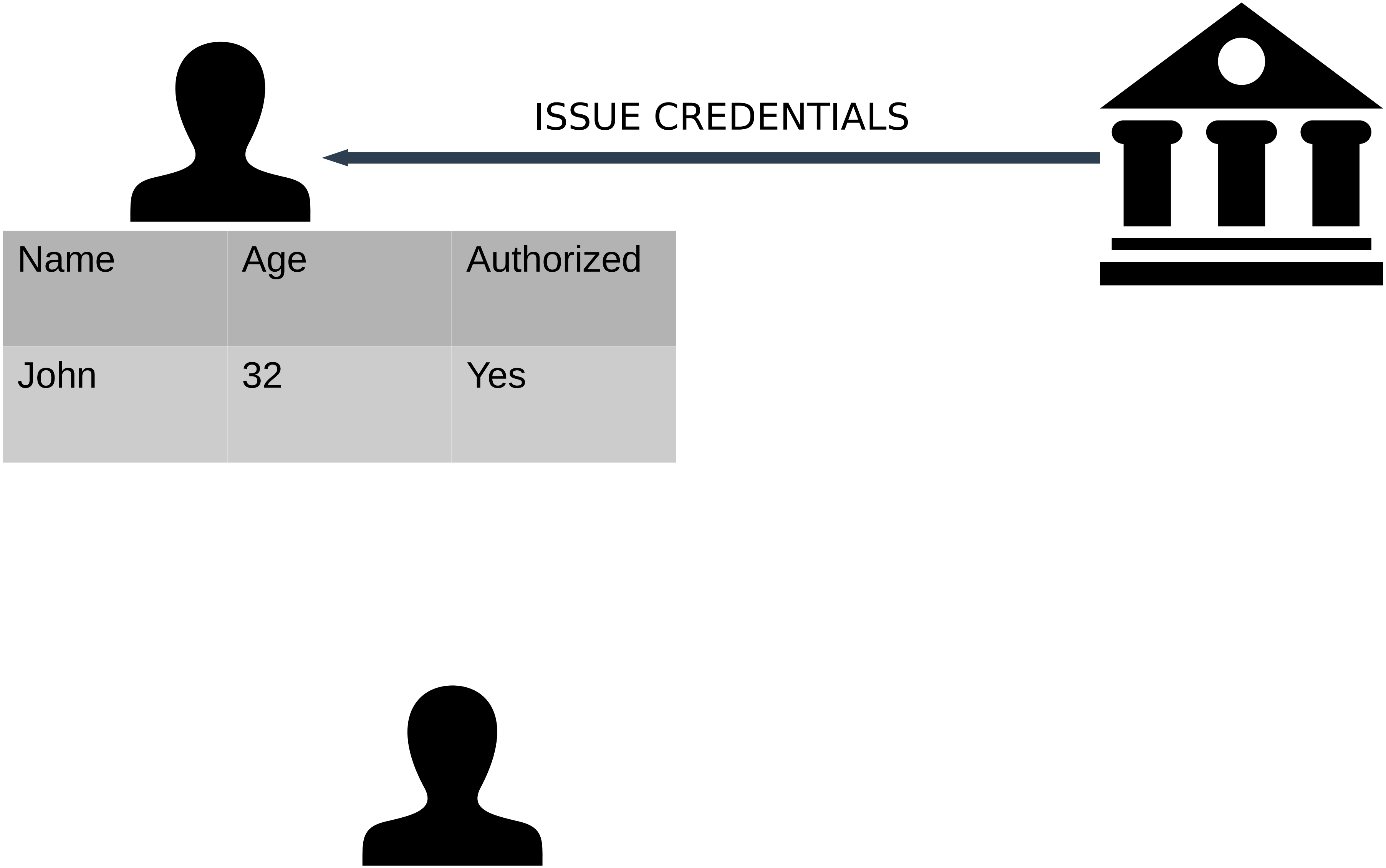


# Anonymous Credentials



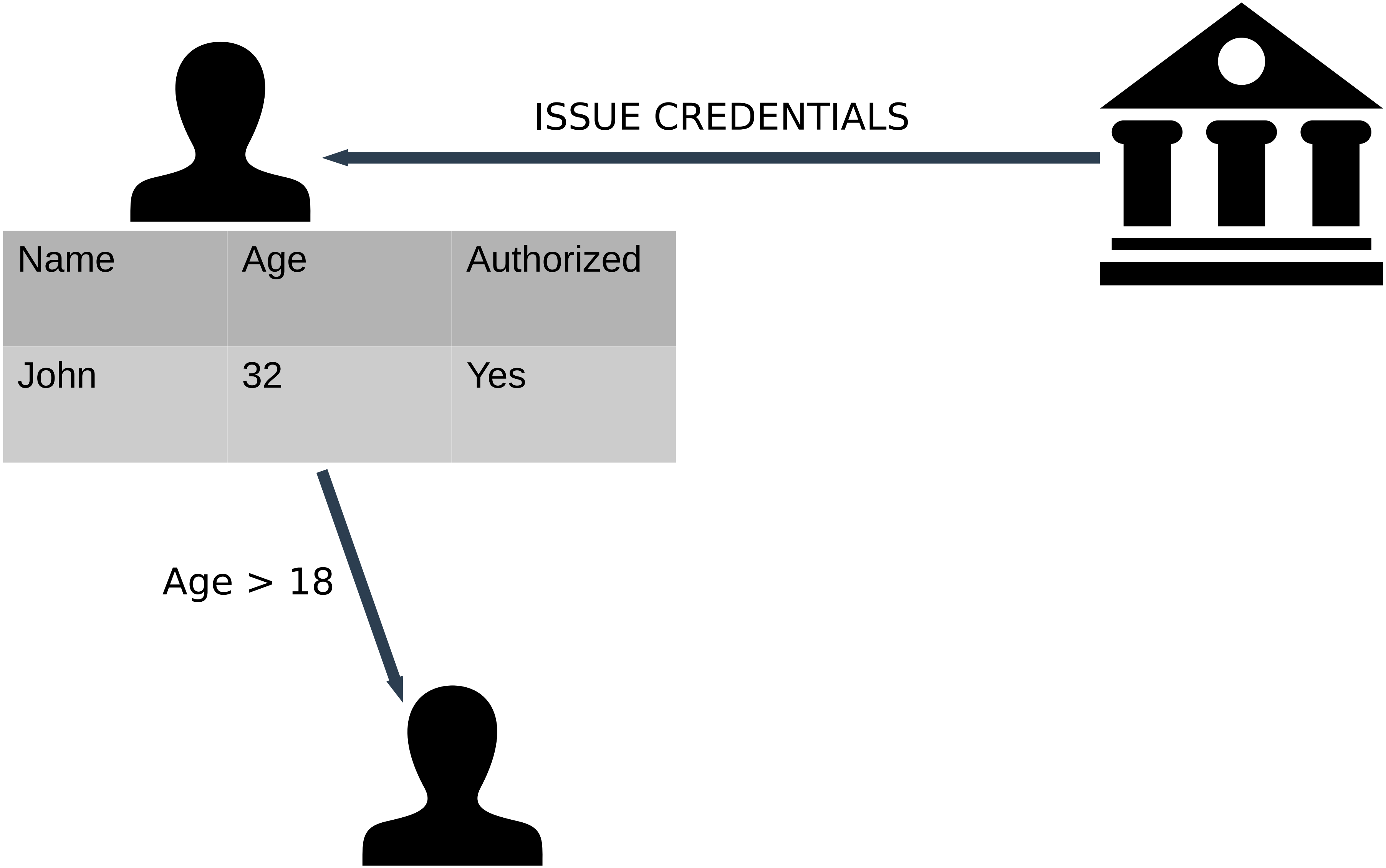
| Name | Age | Authorized |
|---|---|---|
| John | 32 | Yes |

# Anonymous Credentials



| Name | Age | Authorized |
|---|---|---|
| John | 32 | Yes |

# Anonymous Credentials

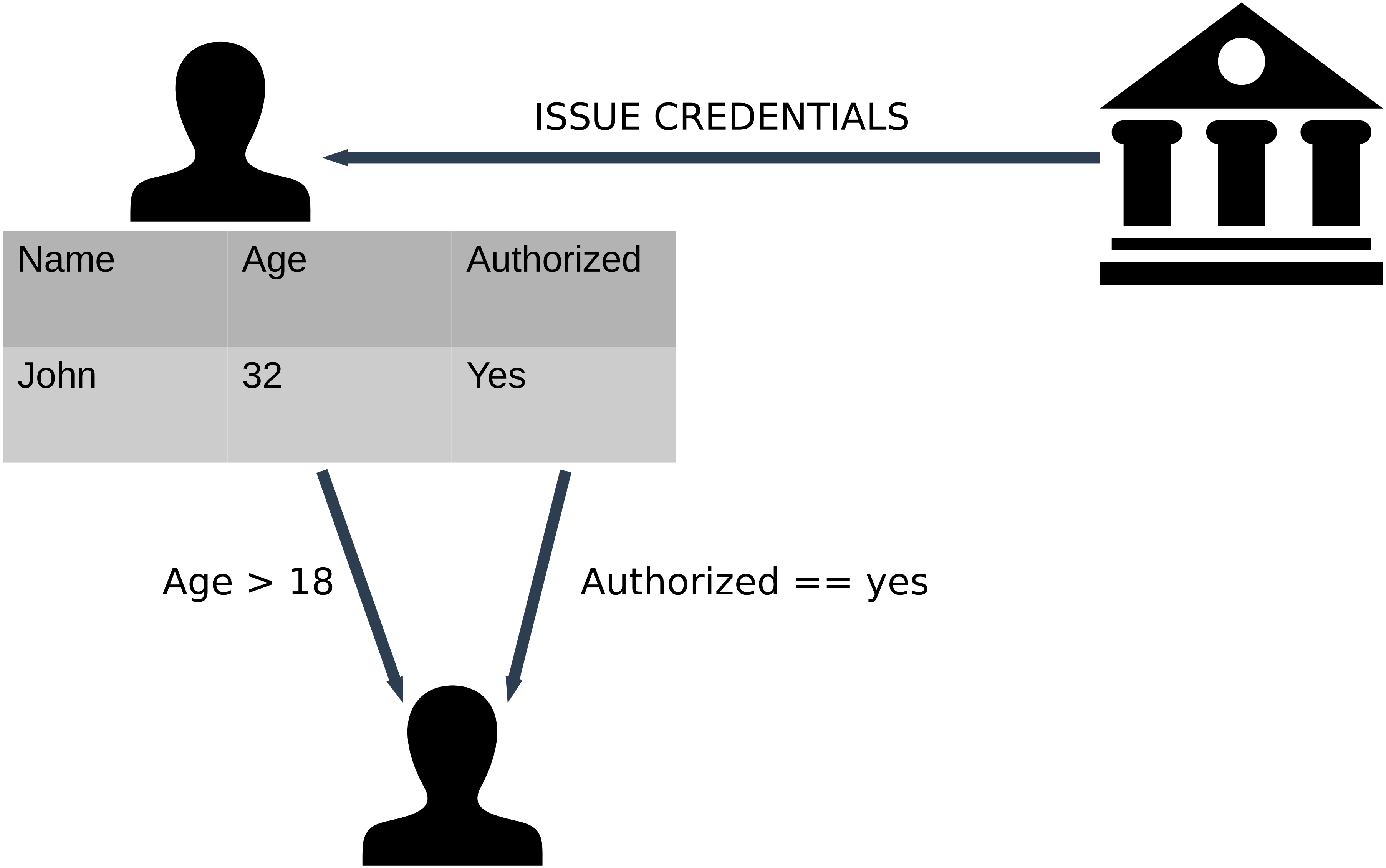


ISSUE CREDENTIALS

| Name | Age | Authorized |
|---|---|---|
| John | 32 | Yes |

Age > 18

# Anonymous Credentials



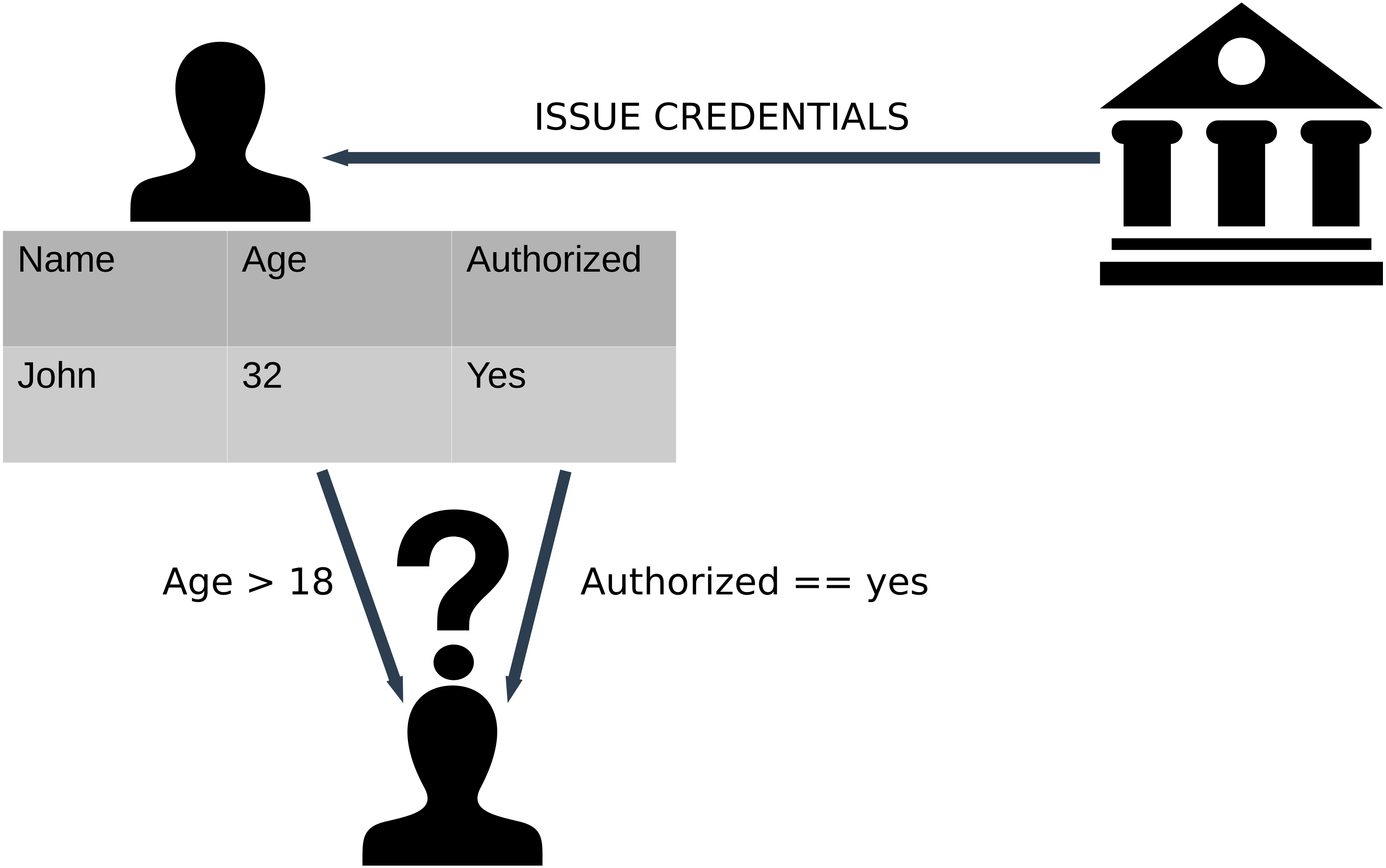
ISSUE CREDENTIALS

| Name | Age | Authorized |
|---|---|---|
| John | 32 | Yes |

Age > 18

Authorized == yes

# Anonymous Credentials



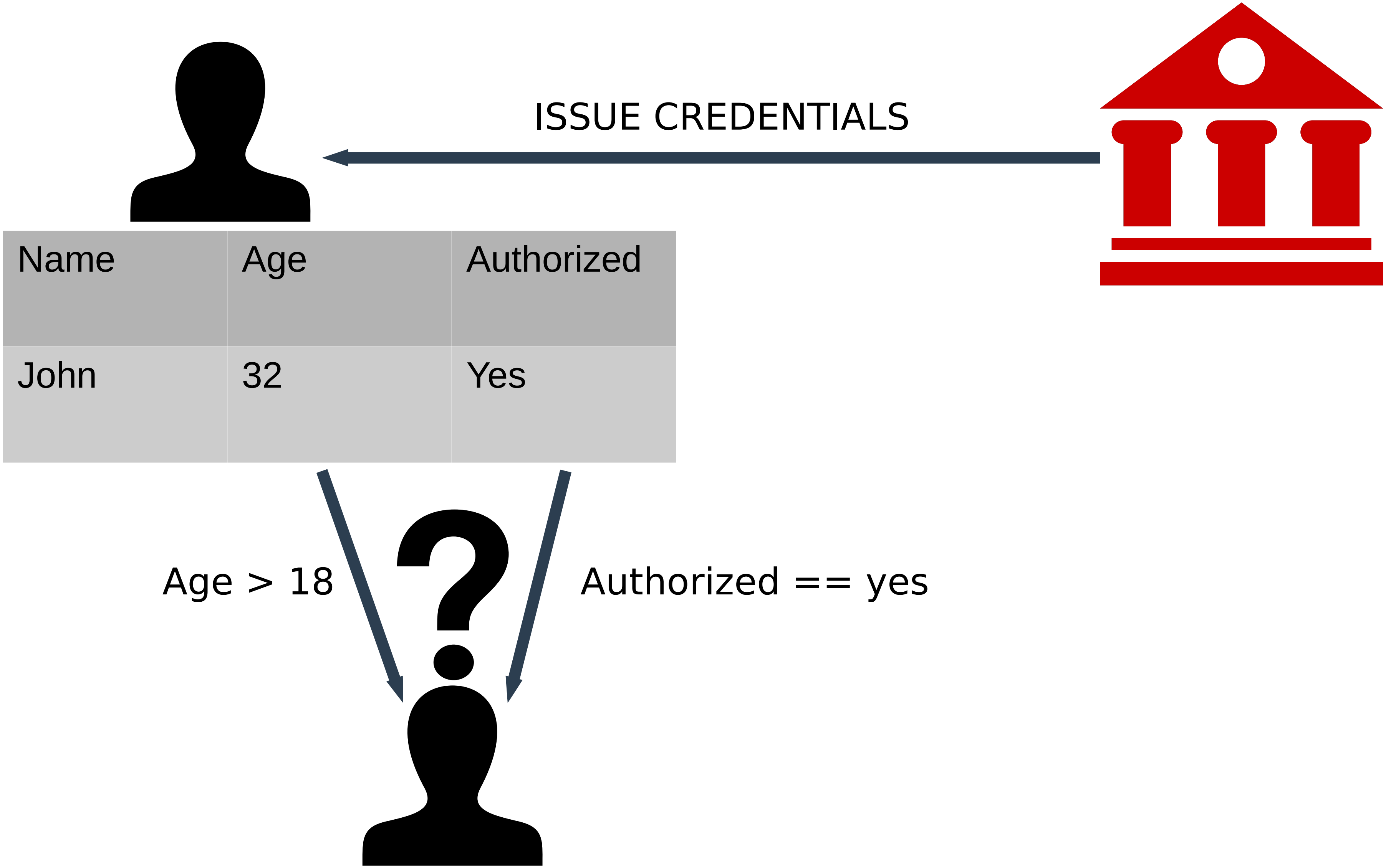
ISSUE CREDENTIALS

| Name | Age | Authorized |
|---|---|---|
| John | 32 | Yes |

Age > 18

Authorized == yes

# Anonymous Credentials



ISSUE CREDENTIALS

| Name | Age | Authorized |
|---|---|---|
| John | 32 | Yes |

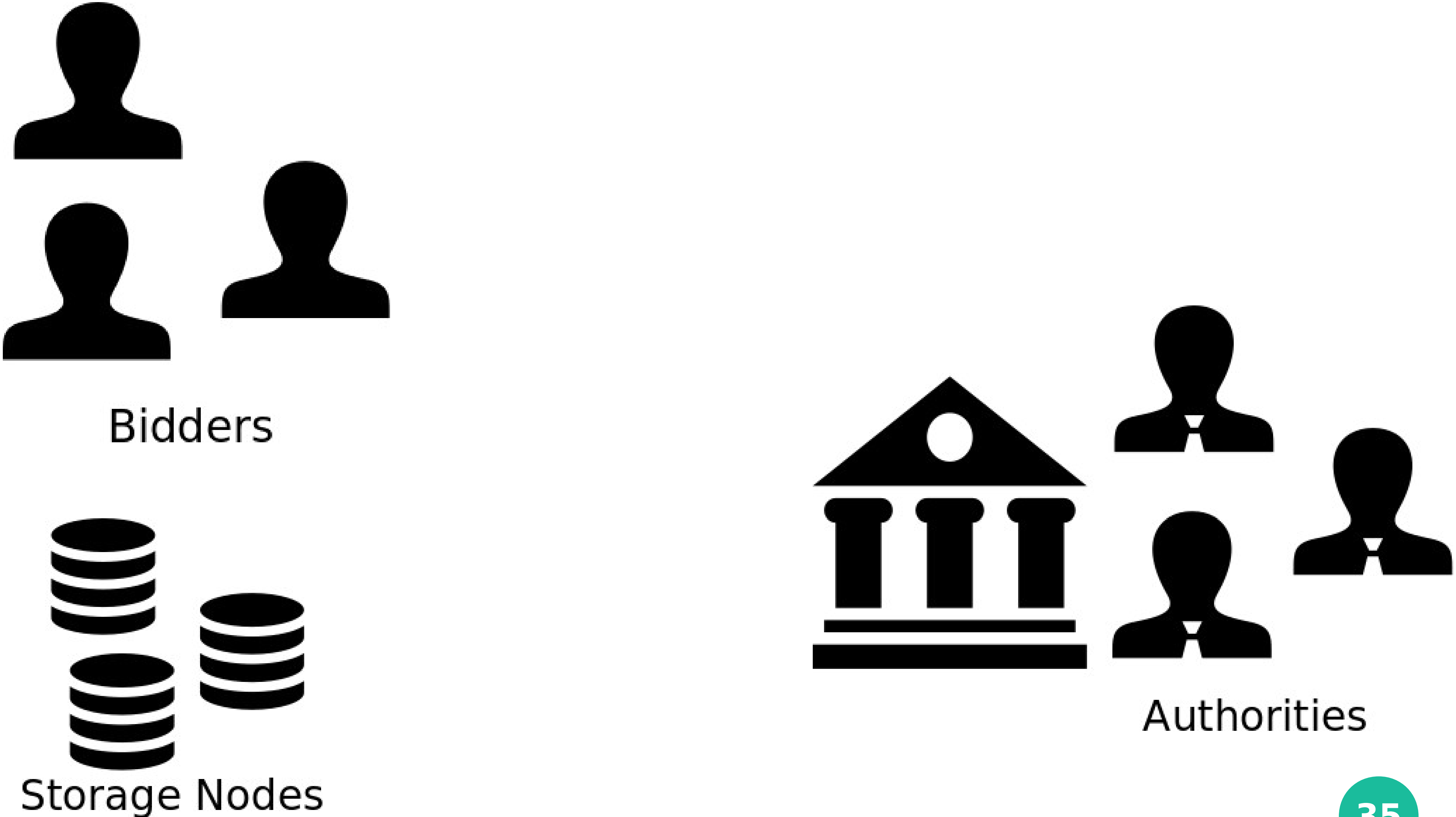
Age > 18

Authorized == yes

# Coconut

- Credentials issued by multiple authorities
- Authenticity and availability even when a subset of authorities are malicious or offline
- Colluding authorities cannot break unlinkability and de-anonymize users

# Preparation phase

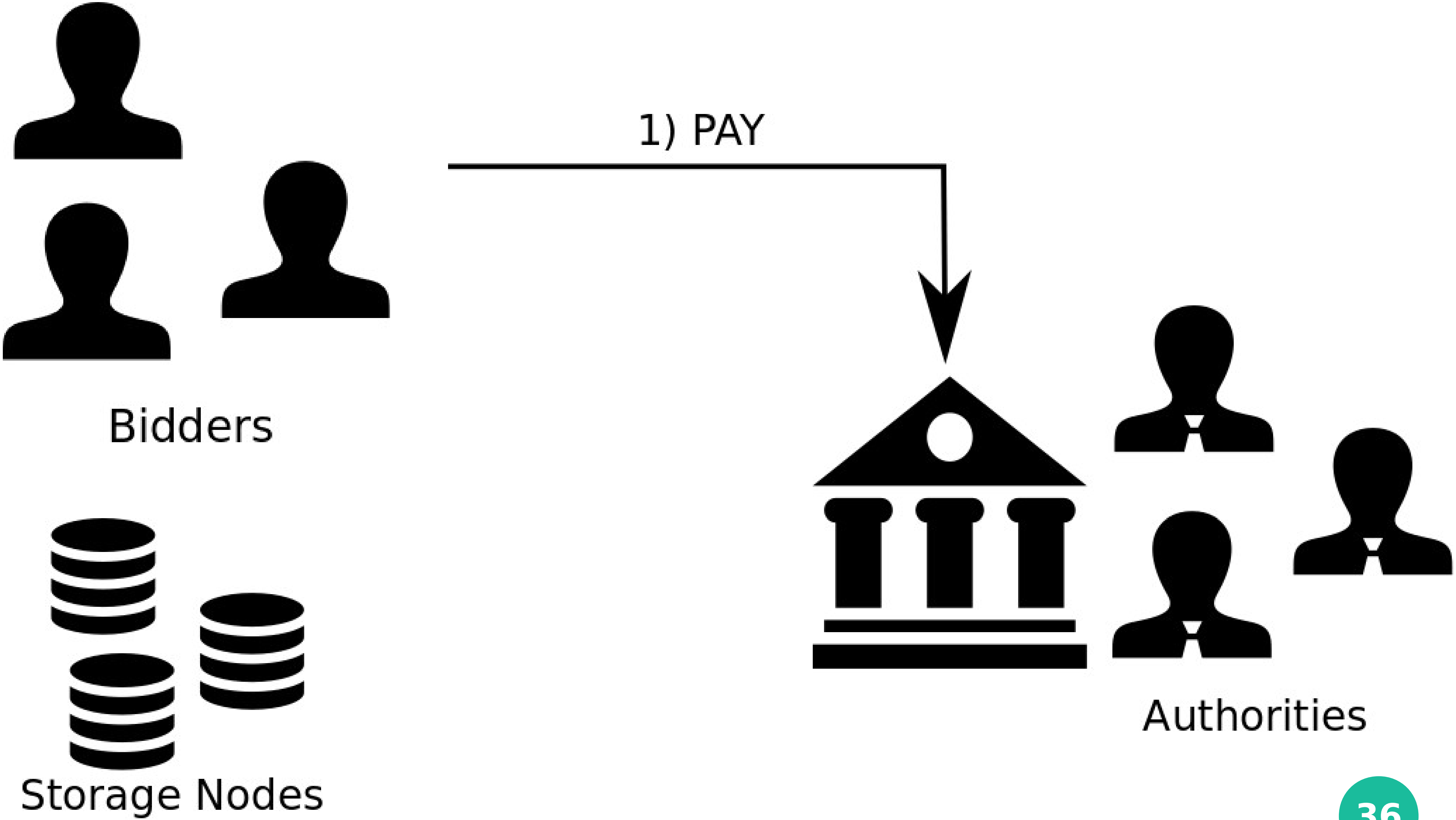


Bidders

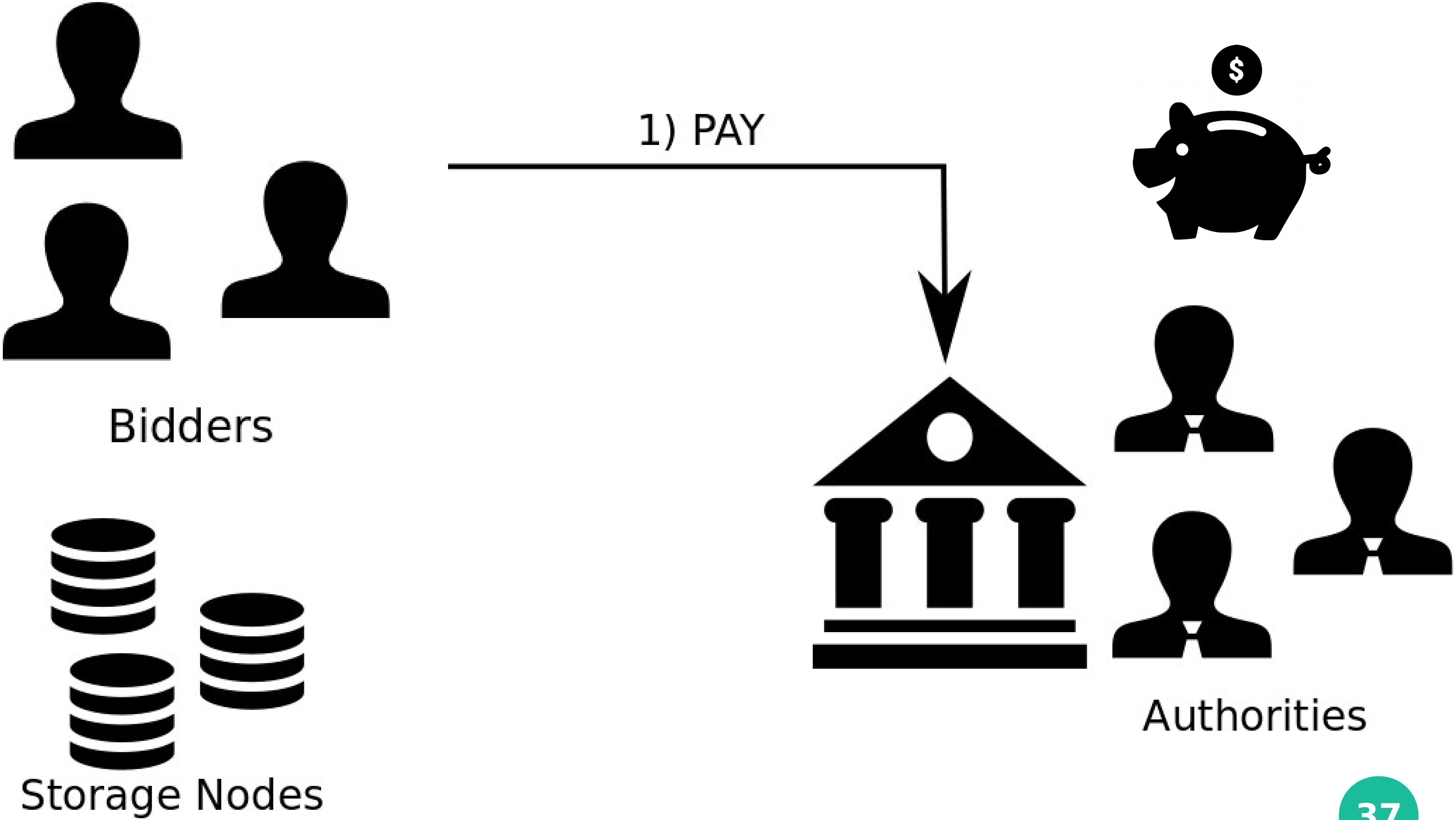
Storage Nodes

Authorities

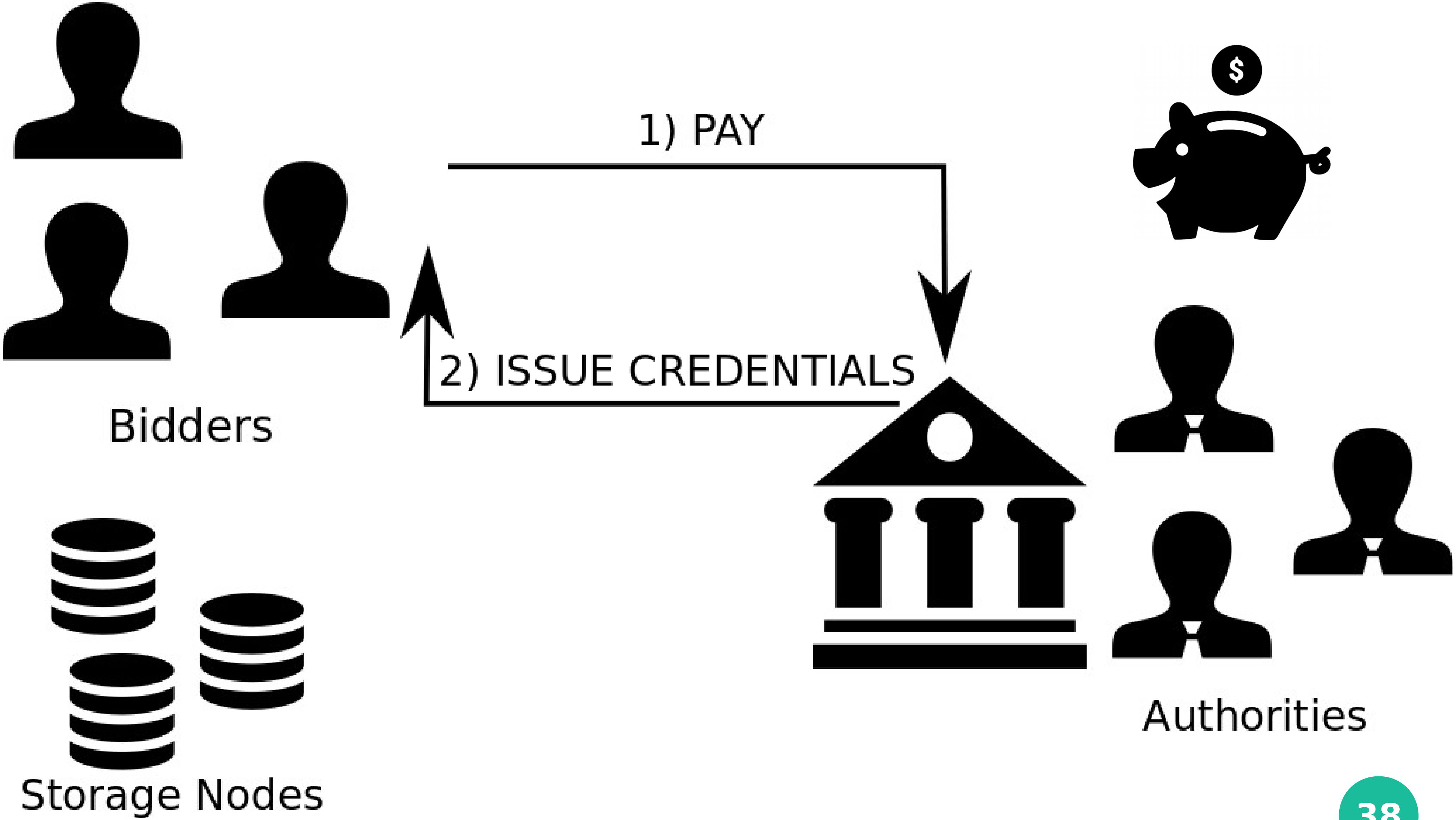
# Preparation phase



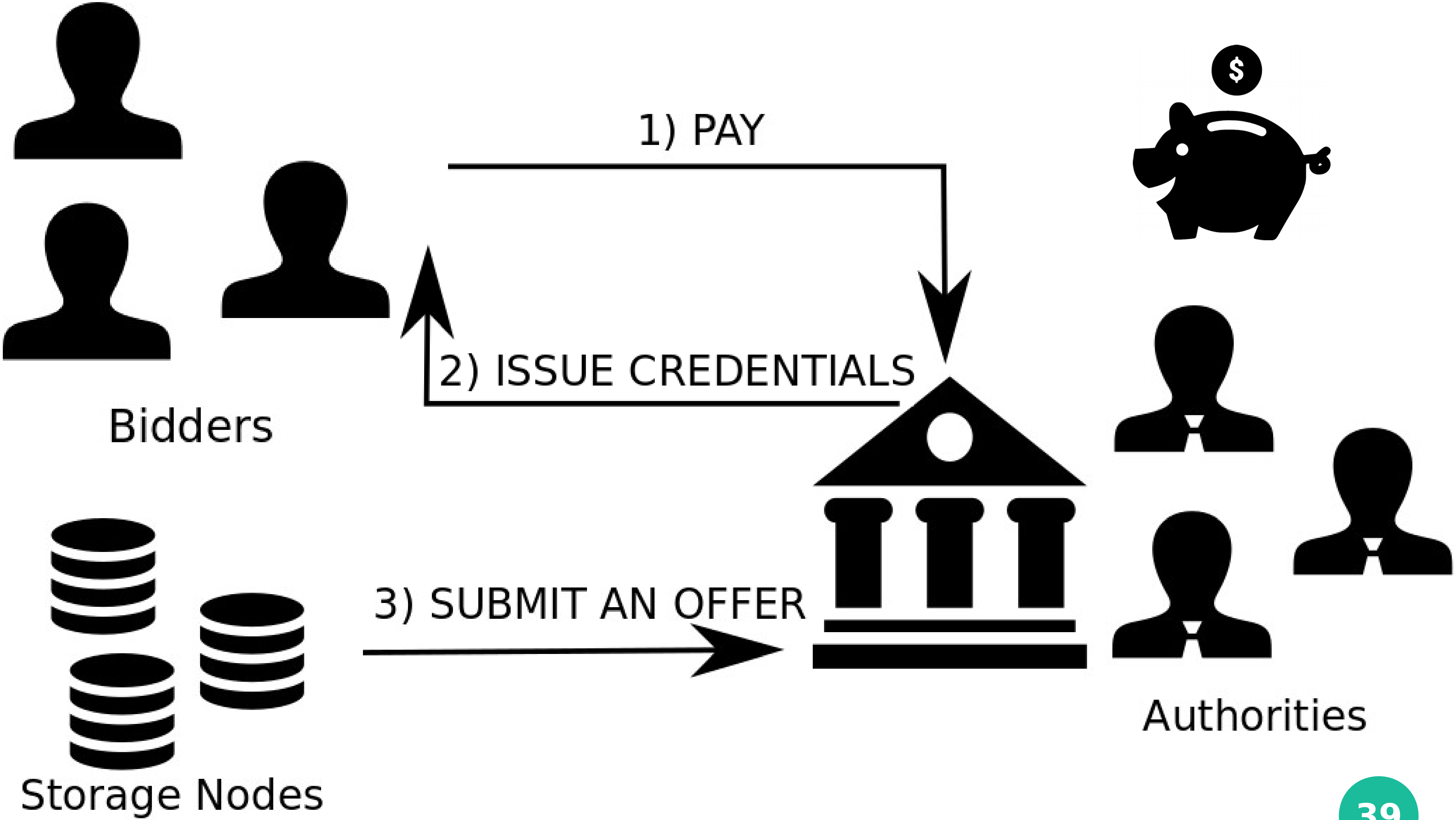
# Preparation phase



# Preparation phase



# Preparation phase



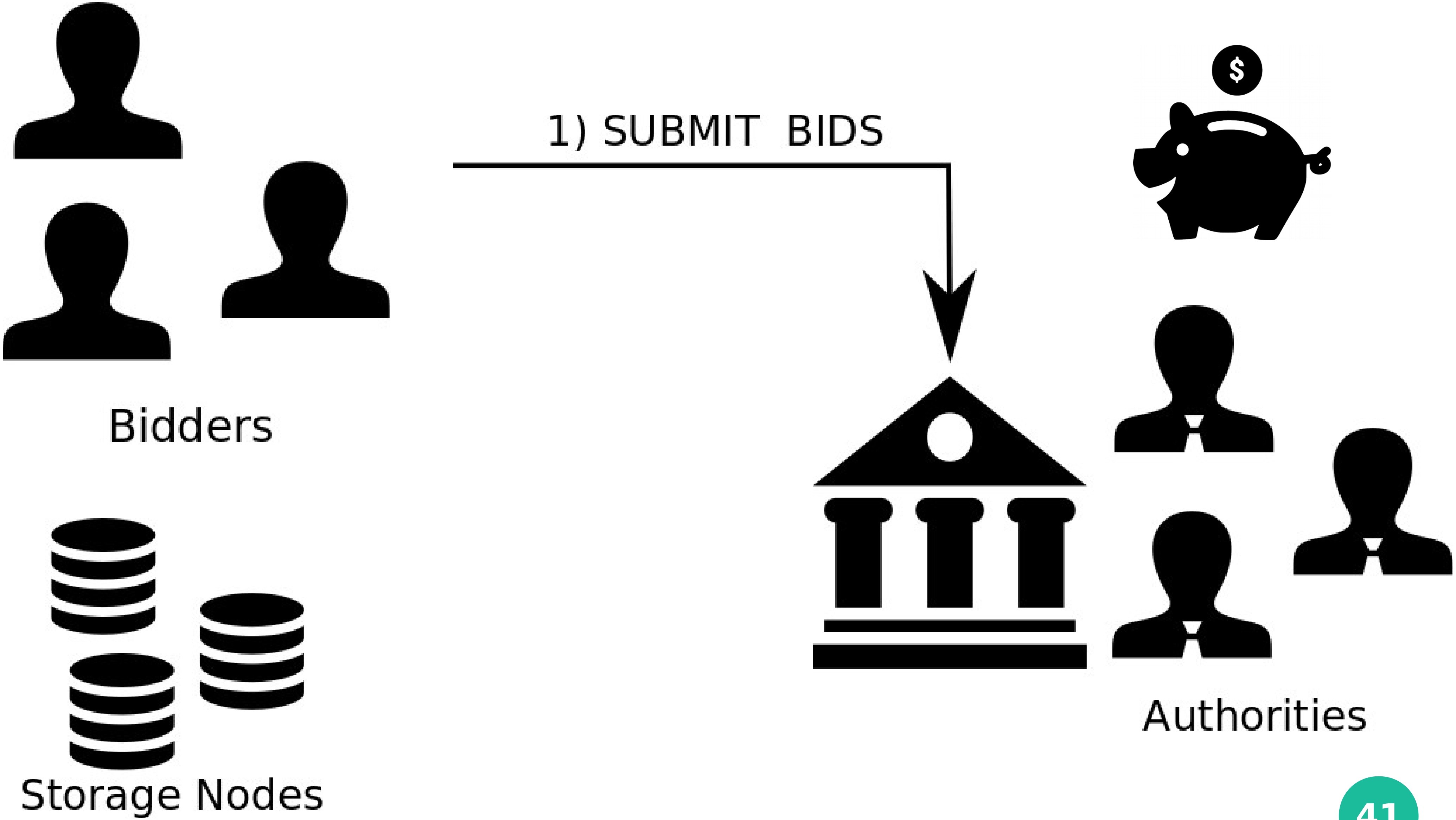
# Auction phase

Bidders

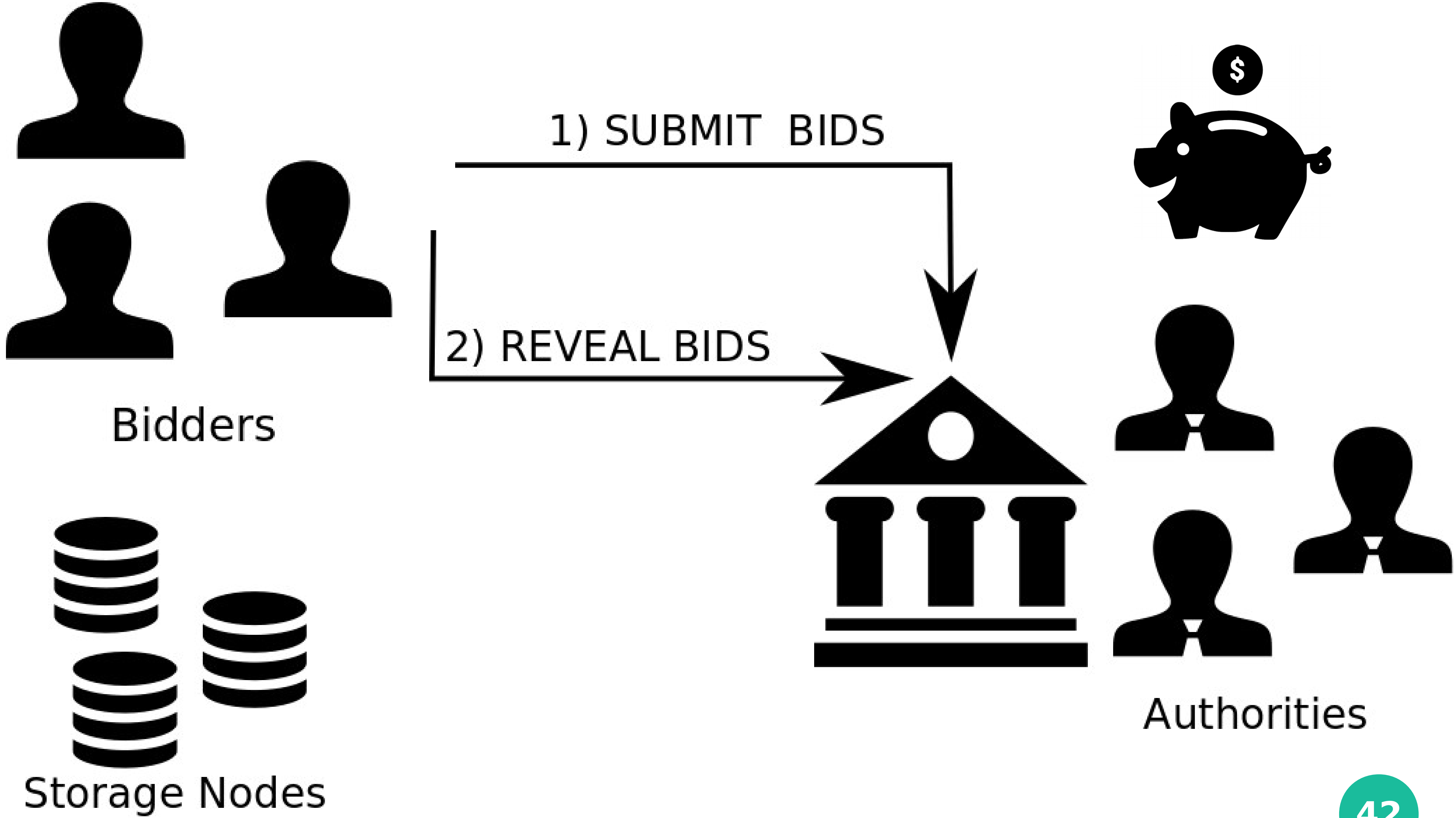
Storage Nodes

Authorities

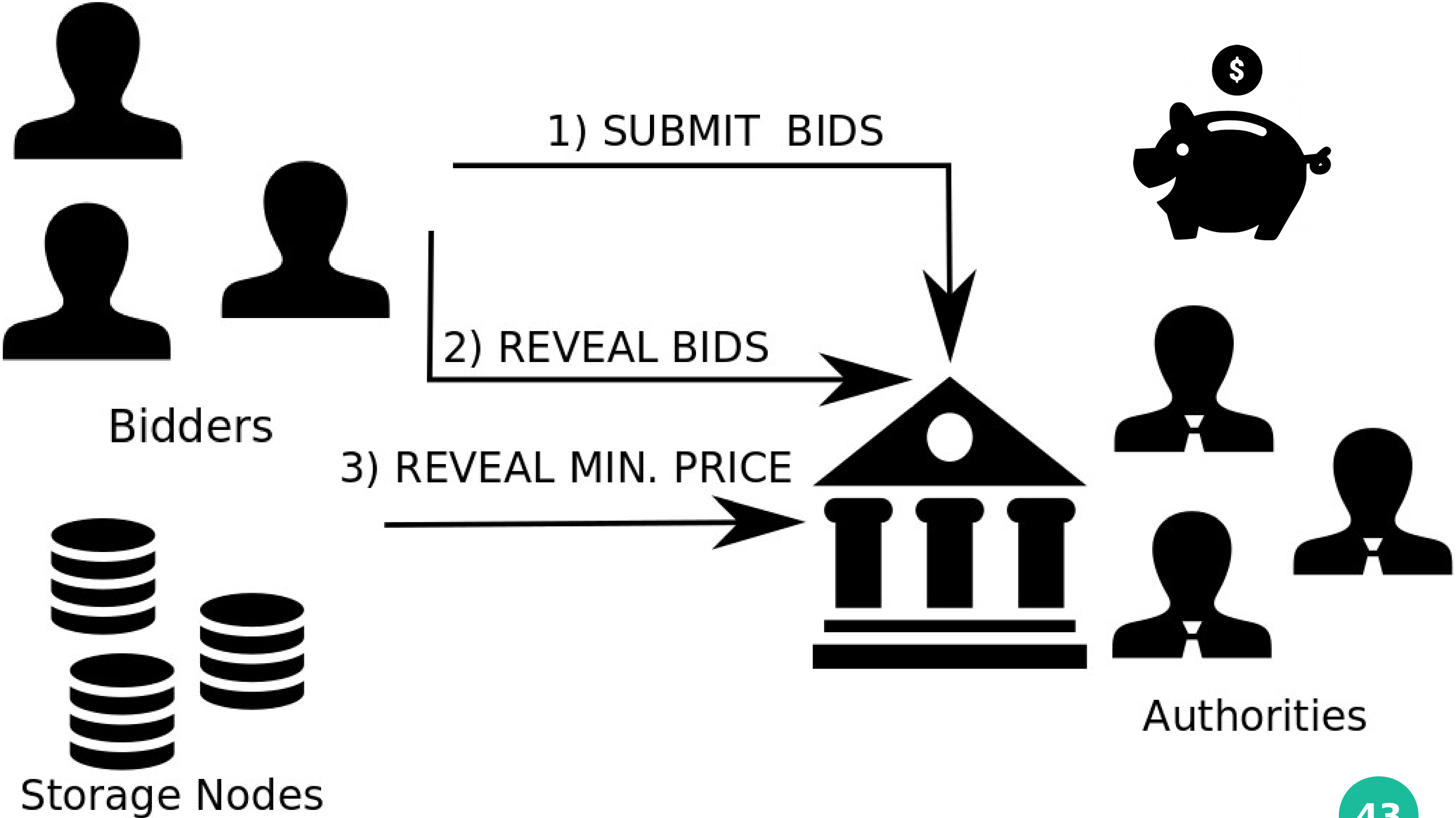
# Auction phase



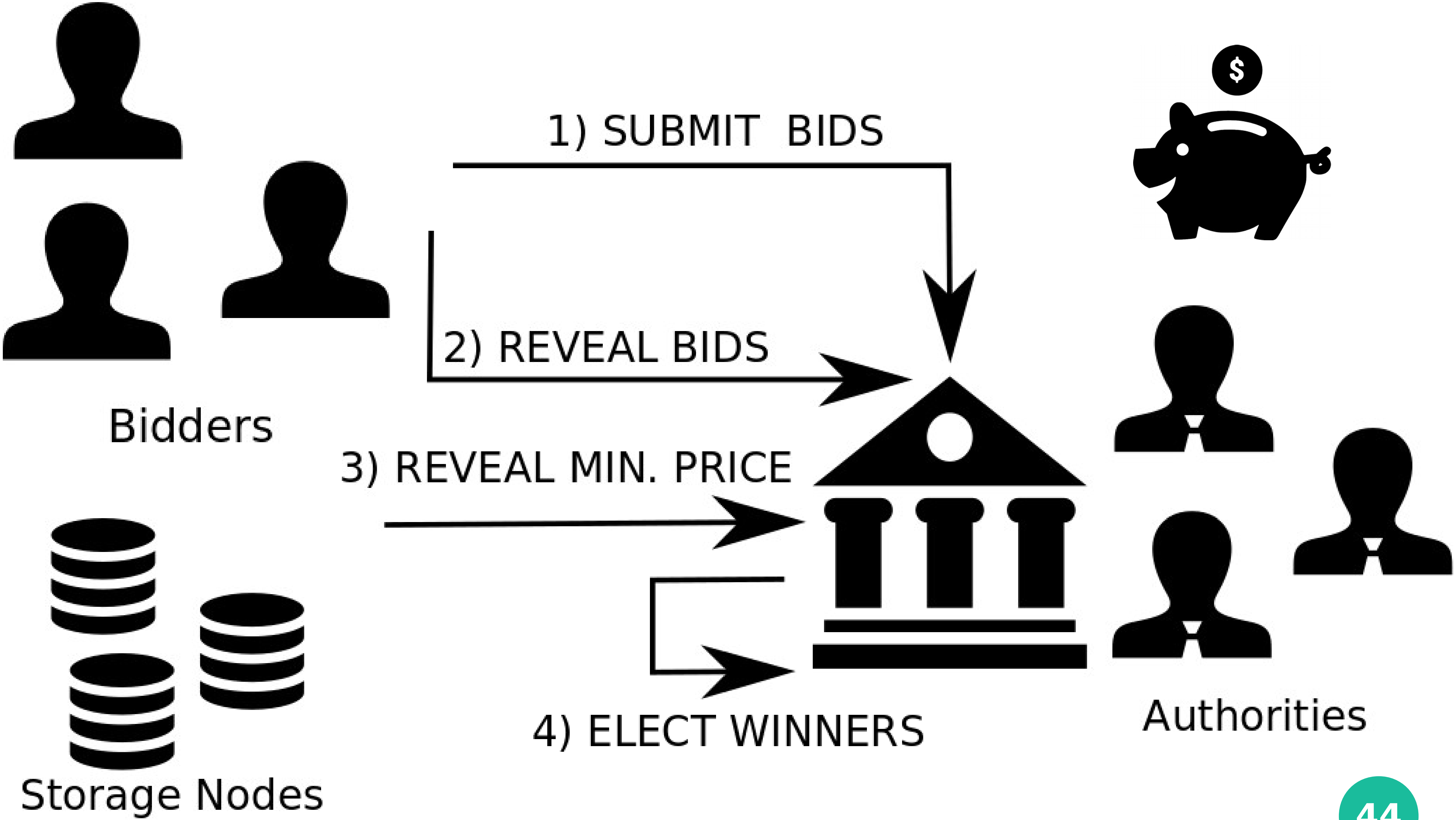
# Auction phase



# Auction phase



# Auction phase



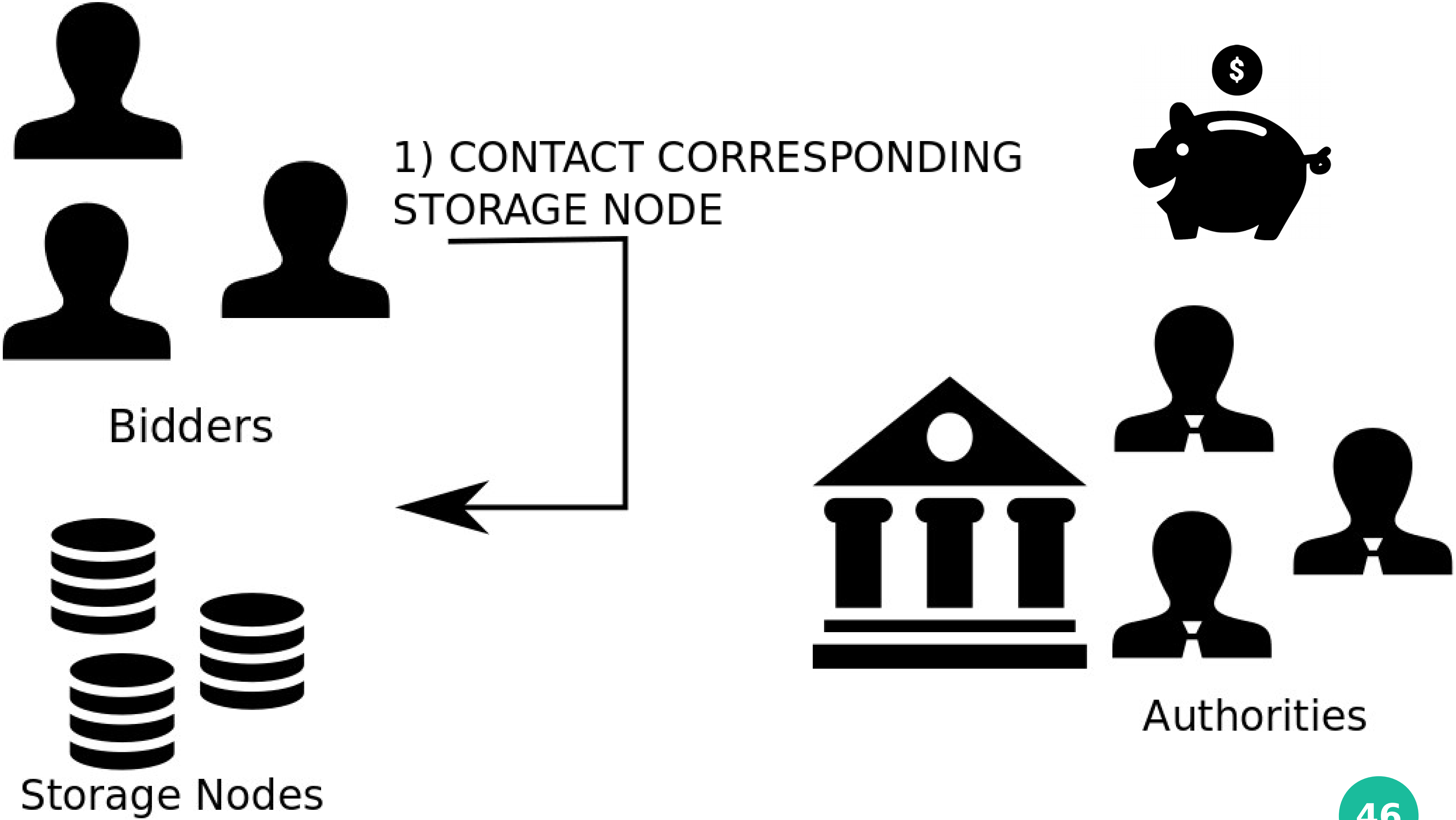
# Execution phase

Bidders

Storage Nodes

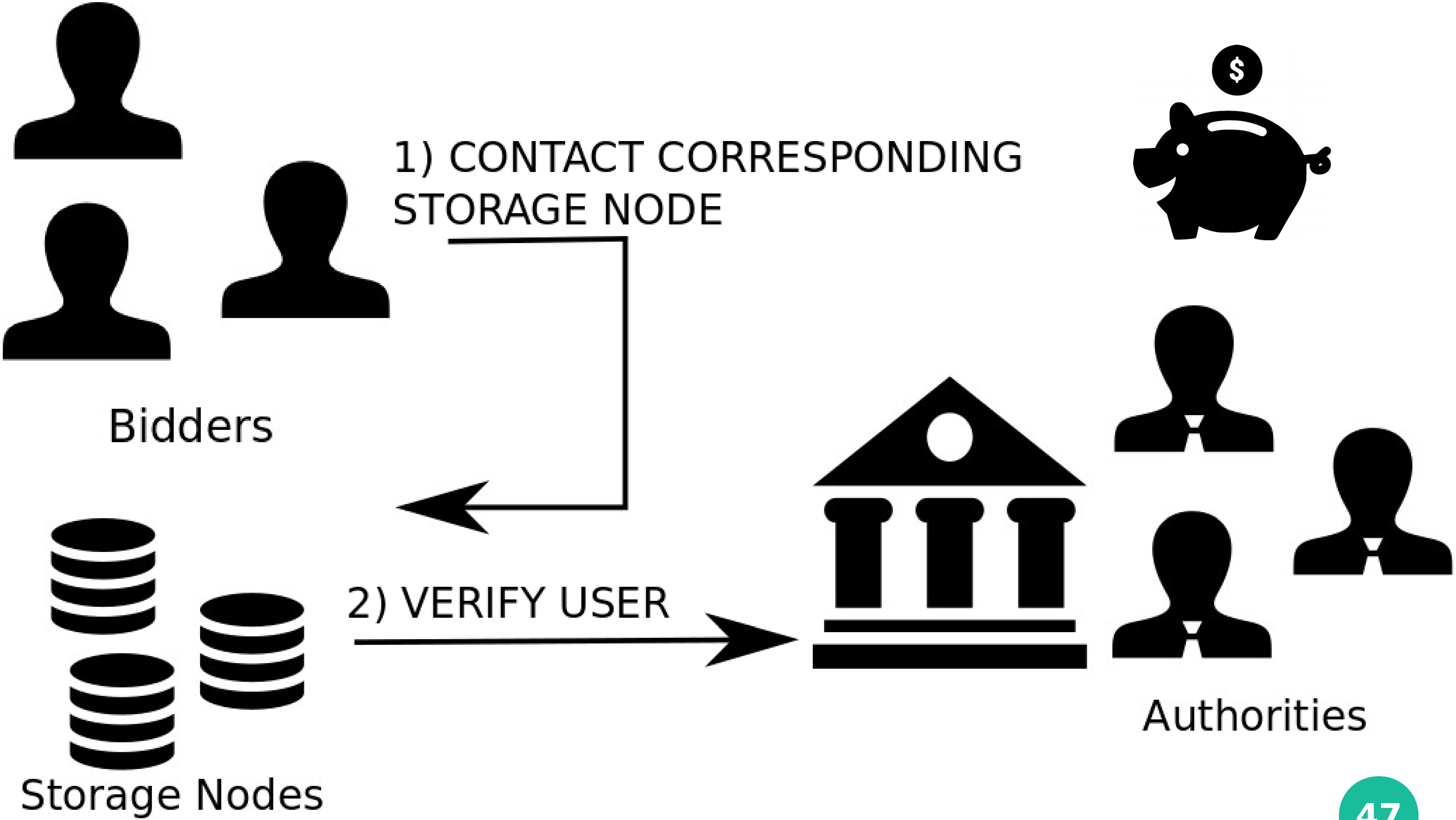
Authorities

# Execution phase



1) CONTACT CORRESPONDING STORAGE NODE

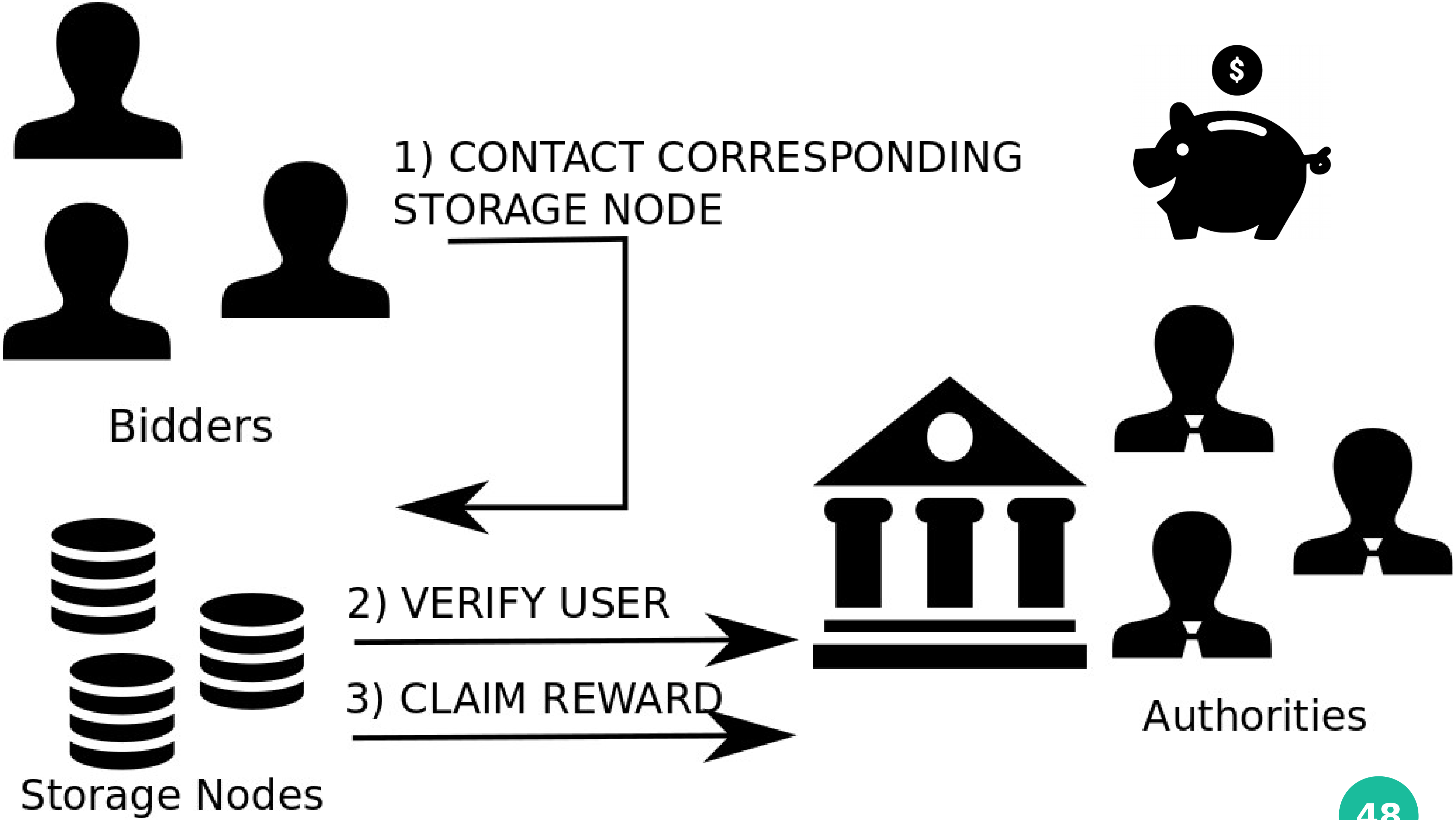
# Execution phase



1) CONTACT CORRESPONDING STORAGE NODE

2) VERIFY USER

# Execution phase



1) CONTACT CORRESPONDING STORAGE NODE

Bidders

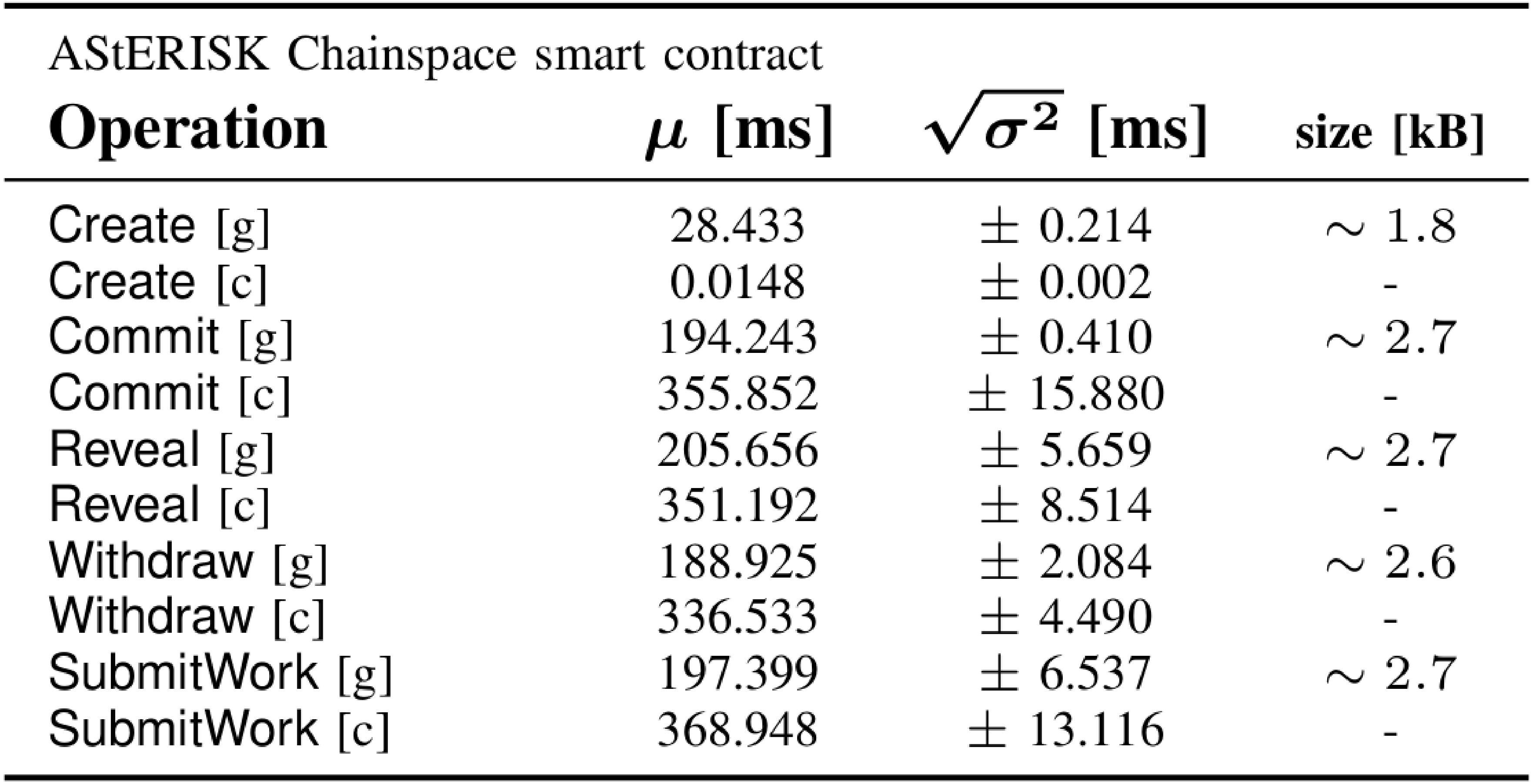
2) VERIFY USER

3) CLAIM REWARD

Storage Nodes

Authorities

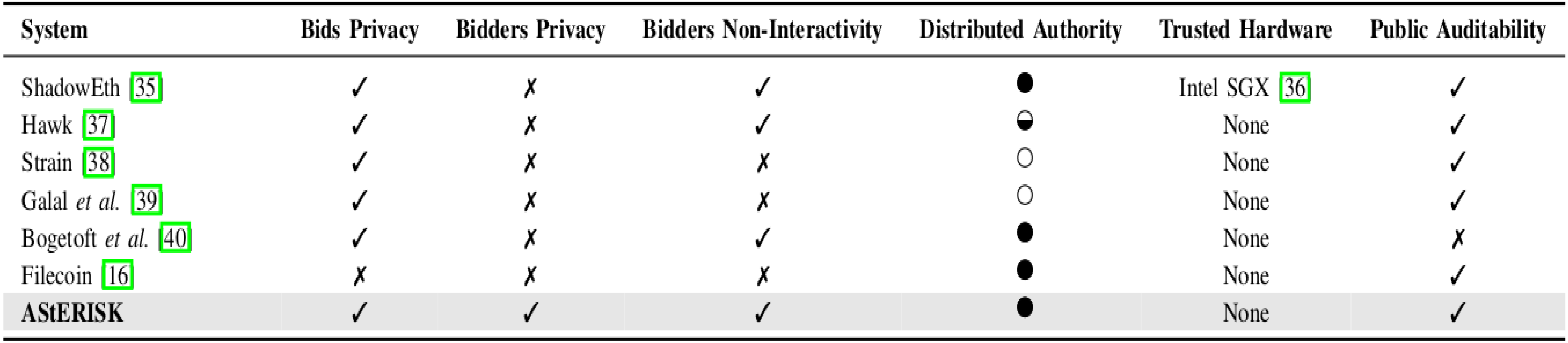
# Performance



AStERISK Chainspace smart contract

| **Operation** | $\mu$ **[ms]** | $\sqrt{\sigma^2}$ **[ms]** | **size [kB]** |
|---|---|---|---|
| Create [g] | 28.433 | ± 0.214 | ~ 1.8 |
| Create [c] | 0.0148 | ± 0.002 | - |
| Commit [g] | 194.243 | ± 0.410 | ~ 2.7 |
| Commit [c] | 355.852 | ± 15.880 | - |
| Reveal [g] | 205.656 | ± 5.659 | ~ 2.7 |
| Reveal [c] | 351.192 | ± 8.514 | - |
| Withdraw [g] | 188.925 | ± 2.084 | ~ 2.6 |
| Withdraw [c] | 336.533 | ± 4.490 | - |
| SubmitWork [g] | 197.399 | ± 6.537 | ~ 2.7 |
| SubmitWork [c] | 368.948 | ± 13.116 | - |

# Related Work



| System | Bids Privacy | Bidders Privacy | Bidders Non-Interactivity | Distributed Authority | Trusted Hardware | Public Auditability |
|---|---|---|---|---|---|---|
| ShadowEth [35] | ✓ | ✗ | ✓ | ● | Intel SGX [36] | ✓ |
| Hawk [37] | ✓ | ✗ | ✓ | ◒ | None | ✓ |
| Strain [38] | ✓ | ✗ | ✗ | ○ | None | ✓ |
| Galal *et al.* [39] | ✓ | ✗ | ✗ | ○ | None | ✓ |
| Bogetoft *et al.* [40] | ✓ | ✗ | ✓ | ● | None | ✗ |
| Filecoin [16] | ✗ | ✗ | ✗ | ● | None | ✓ |
| **AStERISK** | ✓ | ✓ | ✓ | ● | None | ✓ |

# Limitations

- **Does not scale well with a large number of users**
- **The winner of the auction may refuse to transfer data to the worker preventing the worker from claiming the reward**

# Future work

- Prototype with off-chain computations and on-chain verification
- Support for different auction types

Questions?