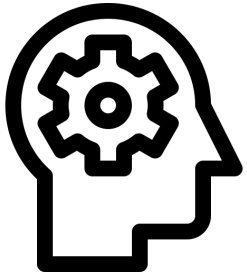
Blockchain based Resource Governance for Decentralized Web Environments

Davide Basile, Claudio Di Ciccio,
Valerio Goretti, Sabrina Kirrane

SAPIENZA
UNIVERSITÀ DI ROMA

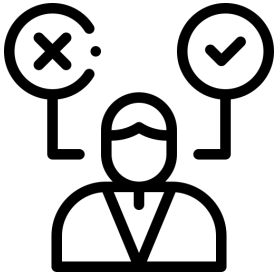
WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

What do companies use your data for ?



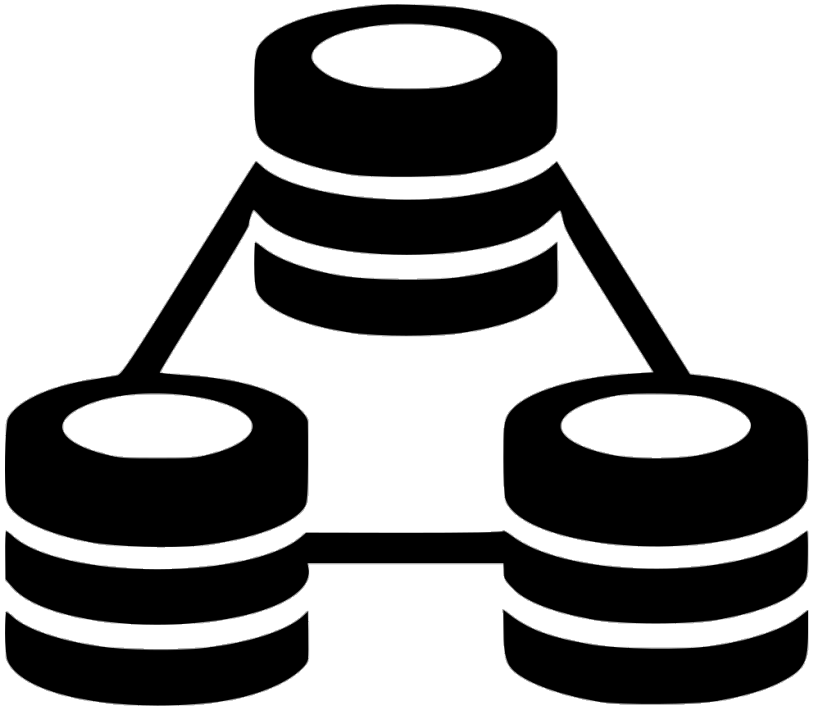
Behaviour insights

Targeted advertising



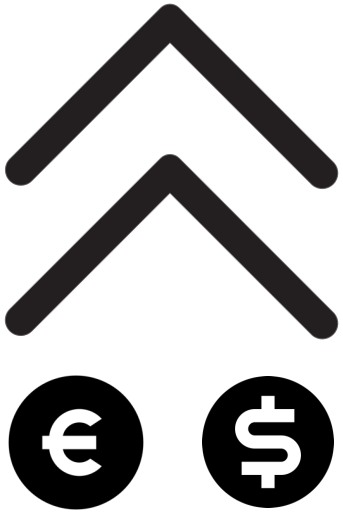
Decision making

The value of personal data

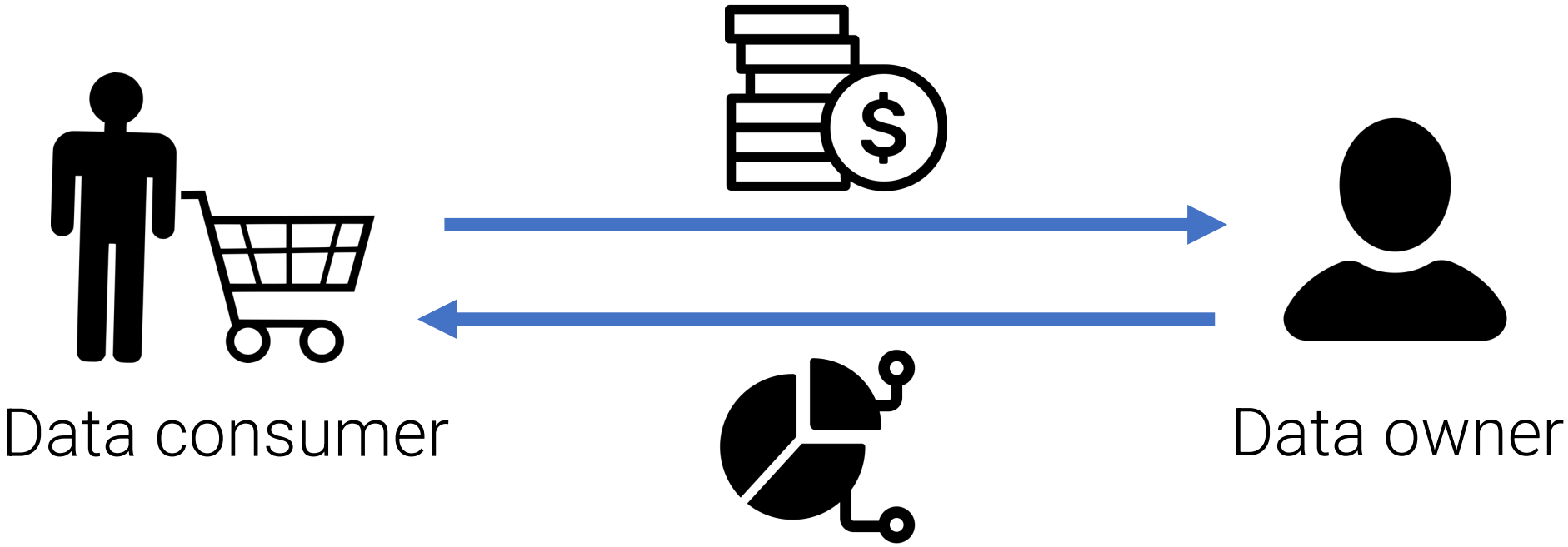


"The big data field's revenue will reach $ 273.4 billion in 2026"

MARKETSANDMARKETS

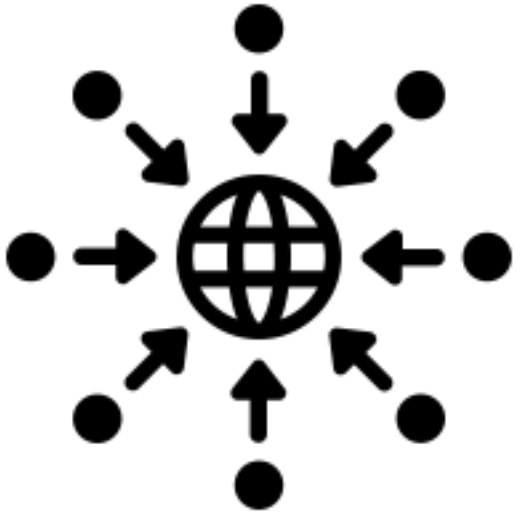


Data trading

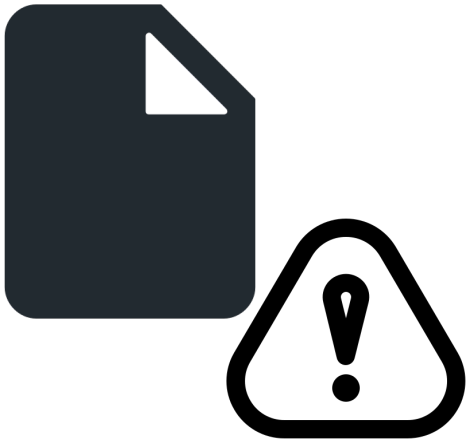


Critical issues

Centralization

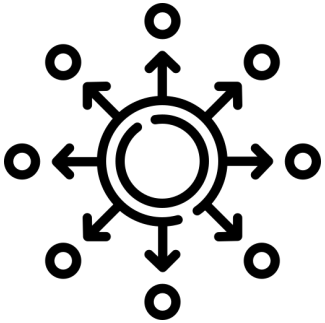


Low degree of control on shared data



Goals of DecentralTrading

Full decentralization



Usage control inspired solution

Built upon existing Web standards

Semantic Web

W3

HTTP

Functionality

Data Owner

Sets up a personal online datastore

Makes his resources available only for medical purposes

Gets a remuneration according to the number of accesses

Functionality

DecentralTrading

Data Owner

Sets up a personal online datastore

Makes his resources available only for medical purposes

Gets a remuneration according to the number of accesses

Asks the market for a web reference to access resources

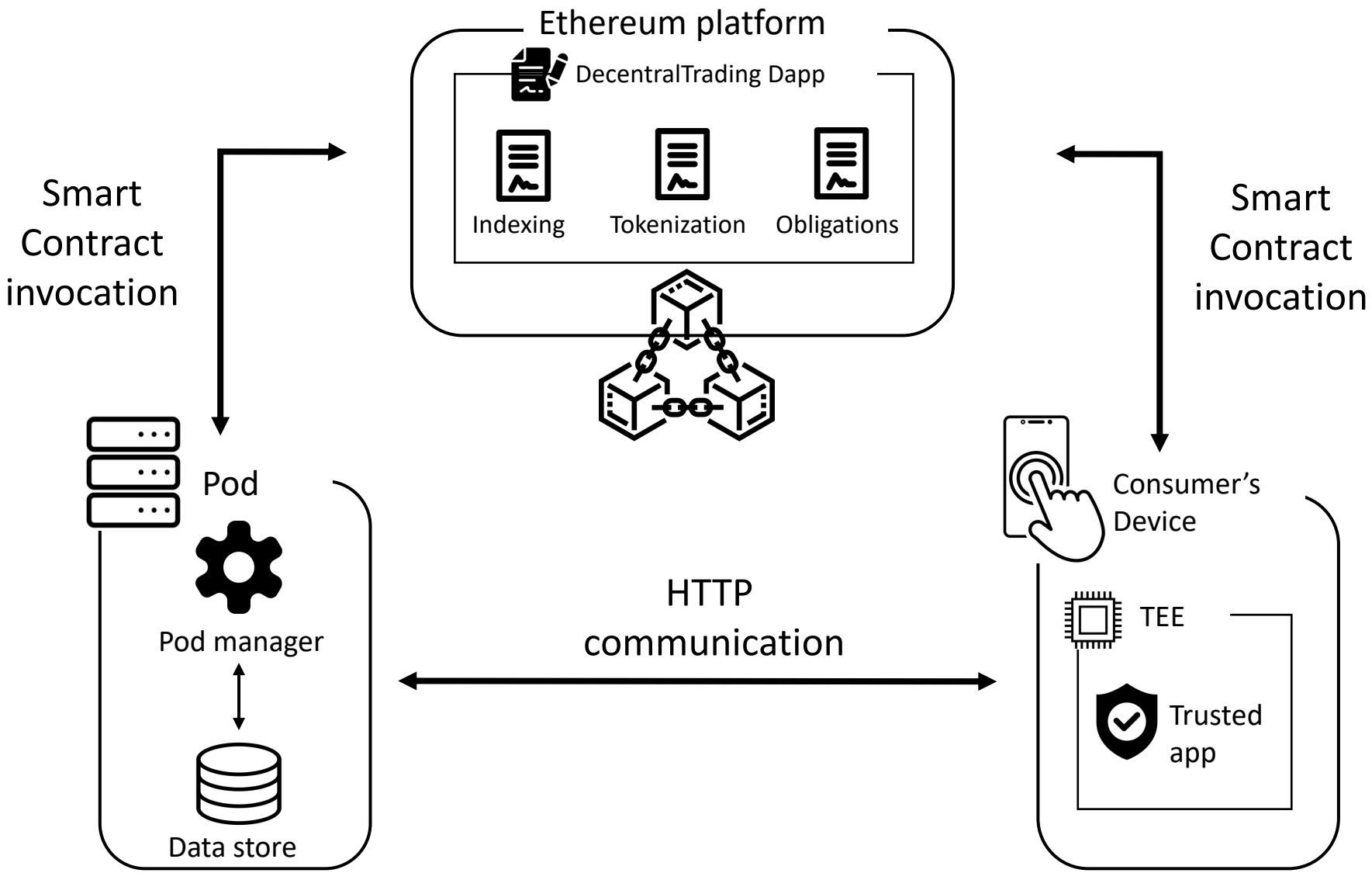
Contacts the personal datastore

Uses the retrieved resources on her trusted device

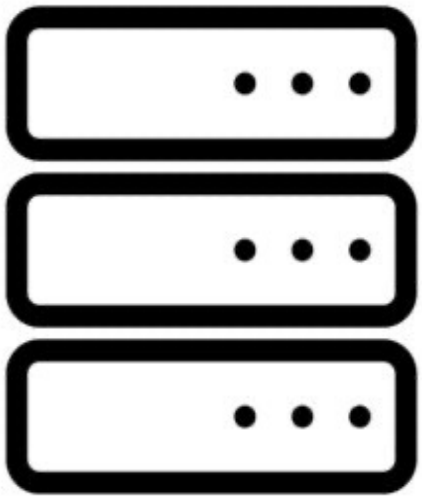
Data Consumer

Architecture

DecentralTrading



Personal Online Datastores



Data owners store shared resources in their Personal Online Datastore.

Functionalities

Data storage 

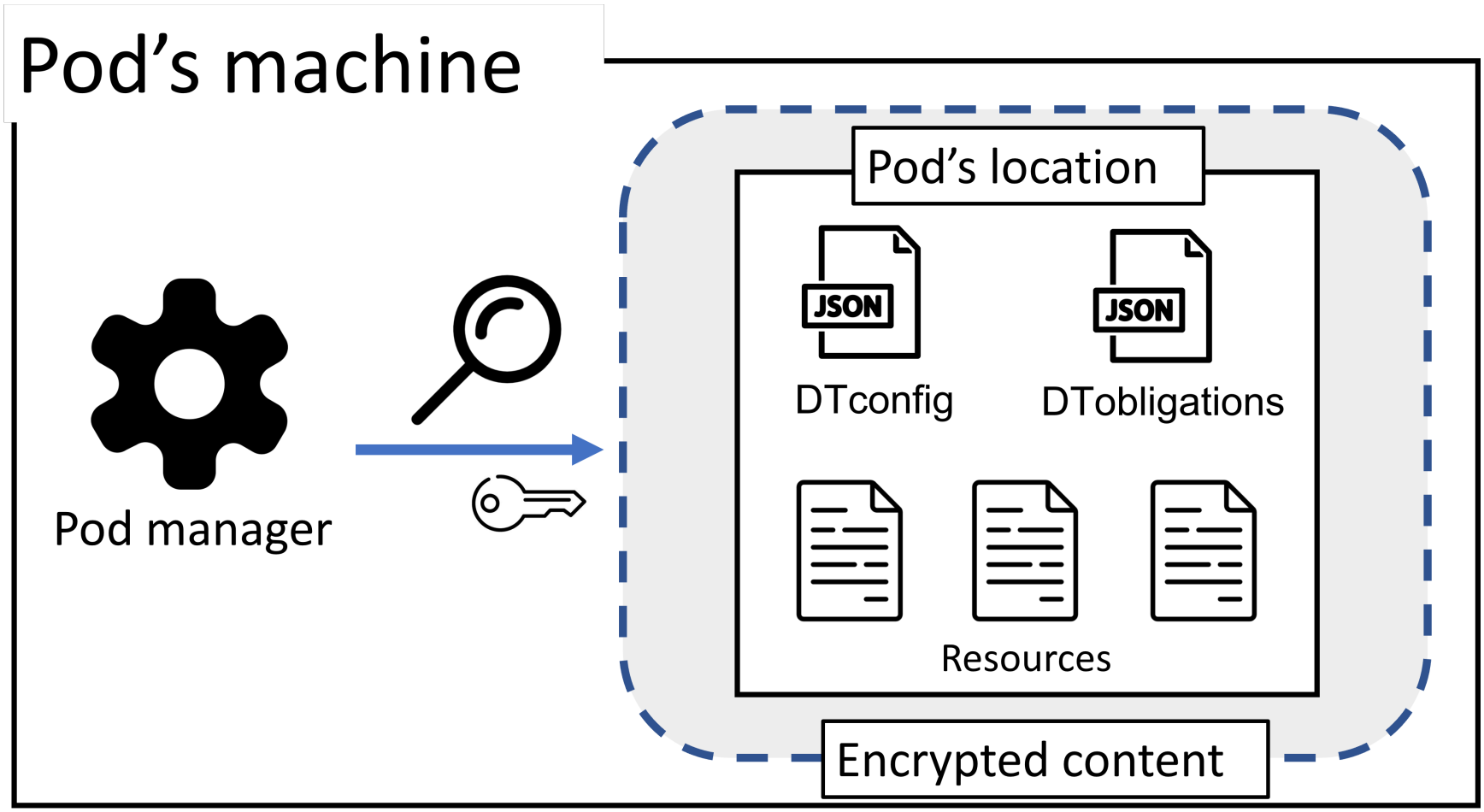
Pods initiation 

Data provision 

Resources initiation 

Obligations management 

Components of a Pod



The Ethereum infrastructure

On-chain components

Ethereum blockchain

Runs DecentralTrading's smart contracts

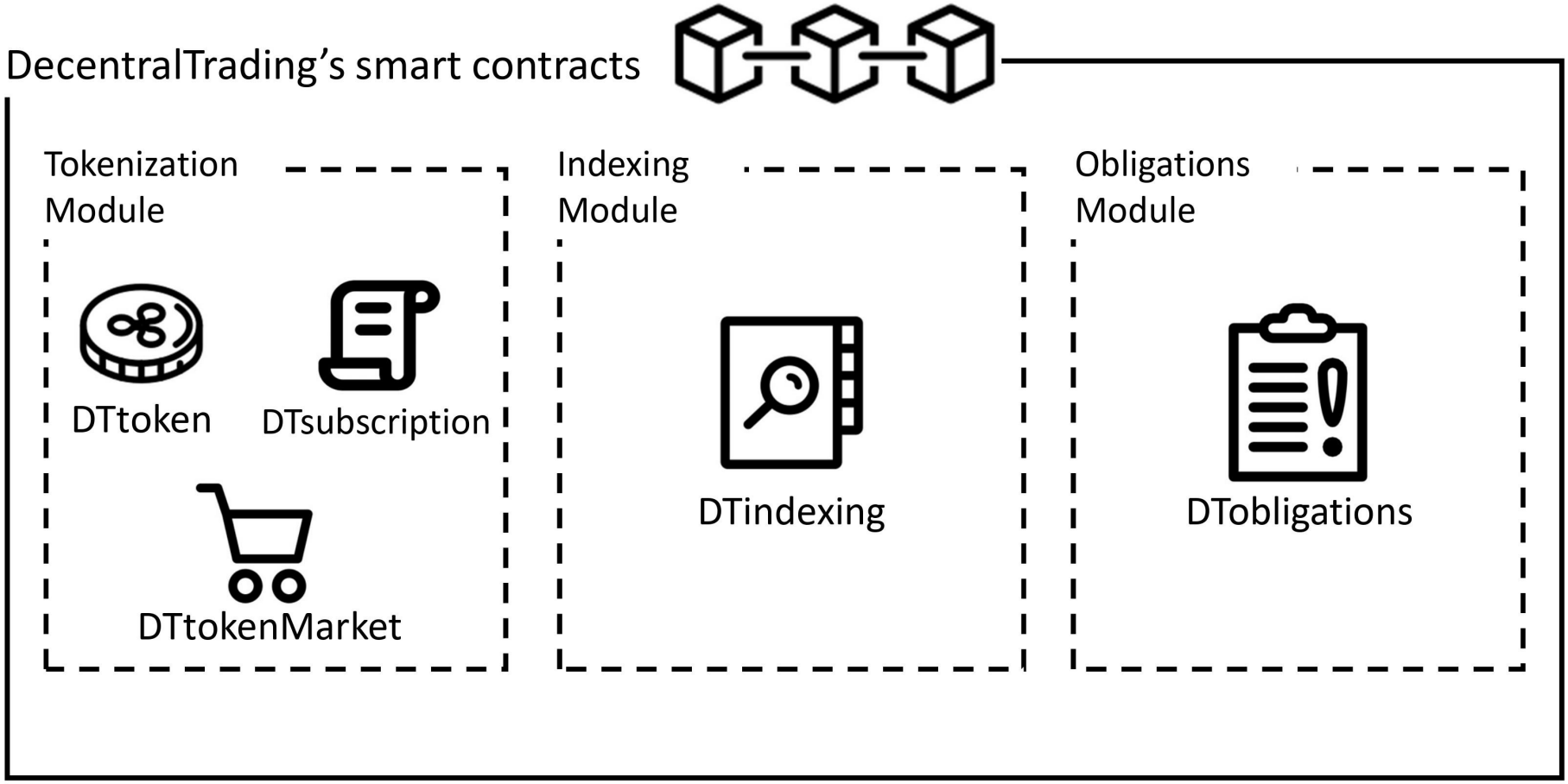
Validates and supervises exchange operations

Manages and verifies user's rights

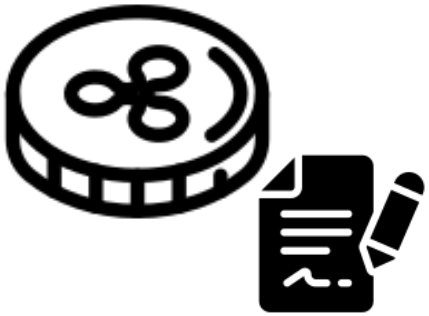
Records resources' metadata

Modules and smart contracts

On-chain components



DTtoken



Remarkable functions

balanceOf()	burn()
transfer()	approve()
mint()	transferFrom()

What is it ? → A smart contract that manages a fungible token

What is it used for ? → to buy market's subscriptions

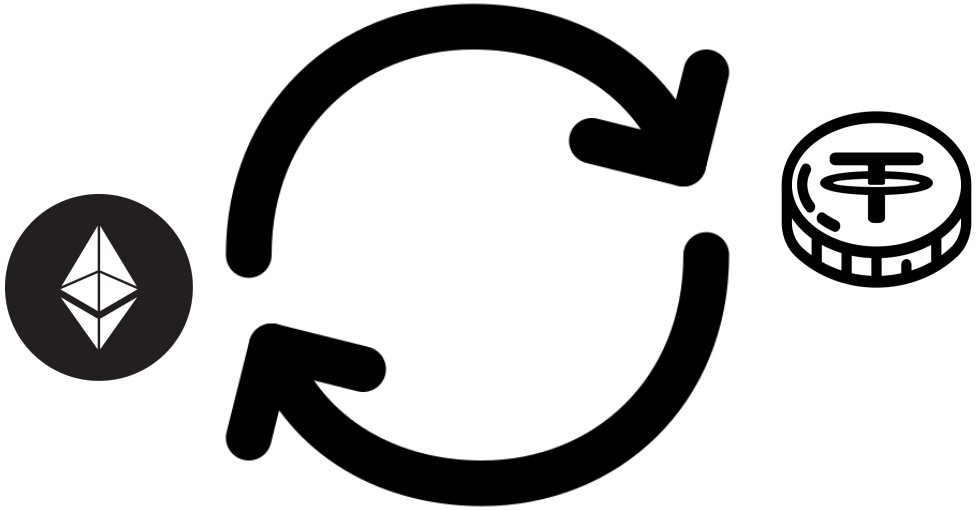
How is it implemented ? → ERC20

DTtokenMarket

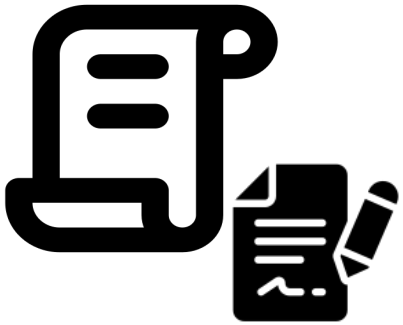
Remarkable function

buyTokens()

What is it ? → A smart contract to exchange ETH with DTtokens



DTsubscription



Remarkable function

purchaseSubscription()
verifySubscription()

What is it ? → A smart contract that controls a non-fungible token

What is it used for ? → to represent the market membership

How is it implemented ? → ERC721

DTindexing

On-chain components

Data owners' side

Data consumers' side

Push Metadata

DTindexing

Pull Metadata

Remarkable functions

registerPod()
registerResource()

Remarkable functions

getPodResources()
getSocialPods()

DTobligation

The smart contract stores and represents rules concerning the usage of the resources

Remarkable functions

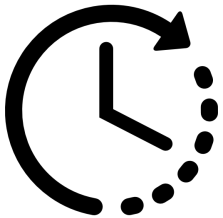
setDomainObligation()
removeDomainObligation()

Access Counter obligation

Country obligation

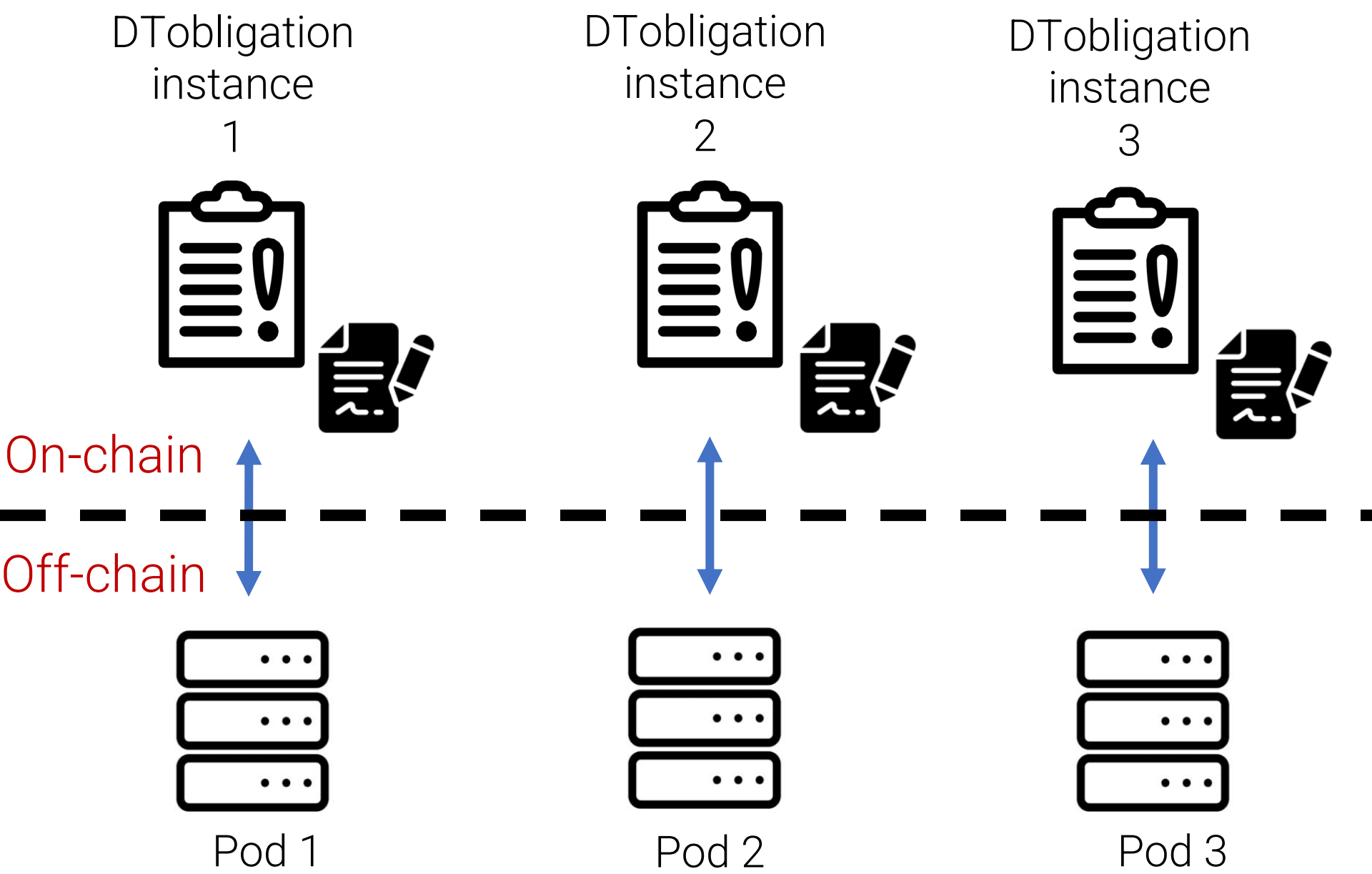
Domain obligation

Temporal obligation

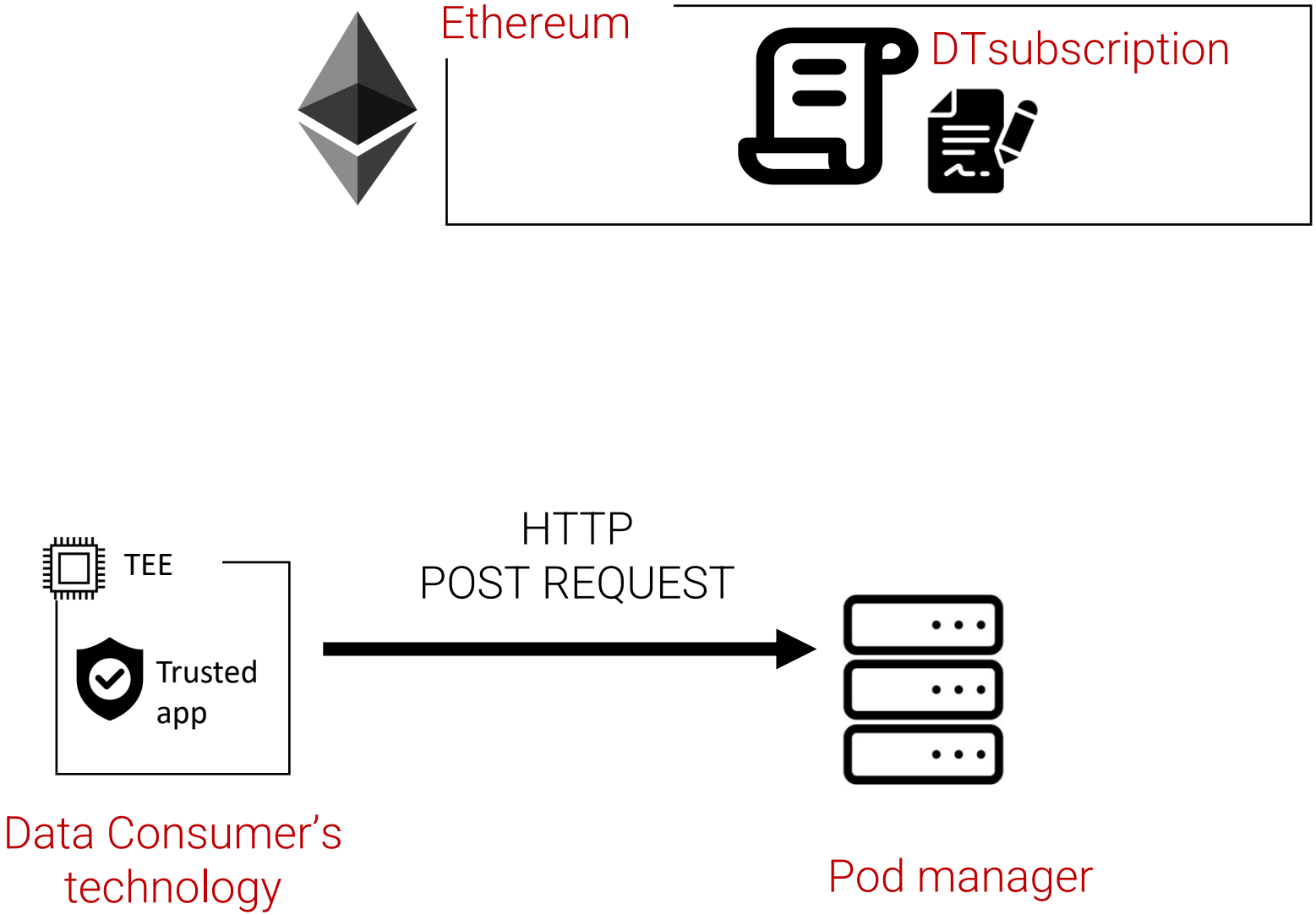


DTobligation instances

On-chain components

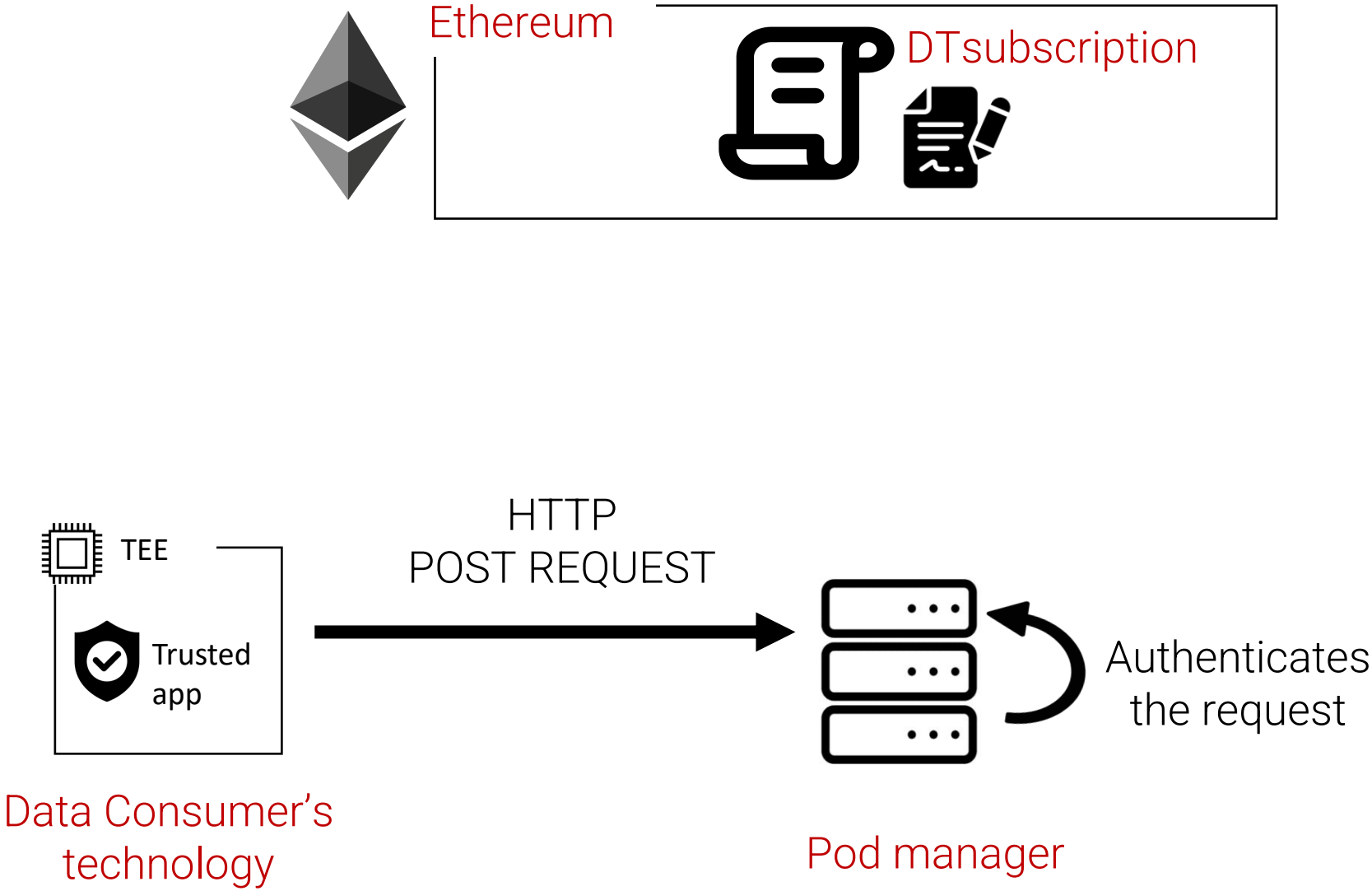


Data provision

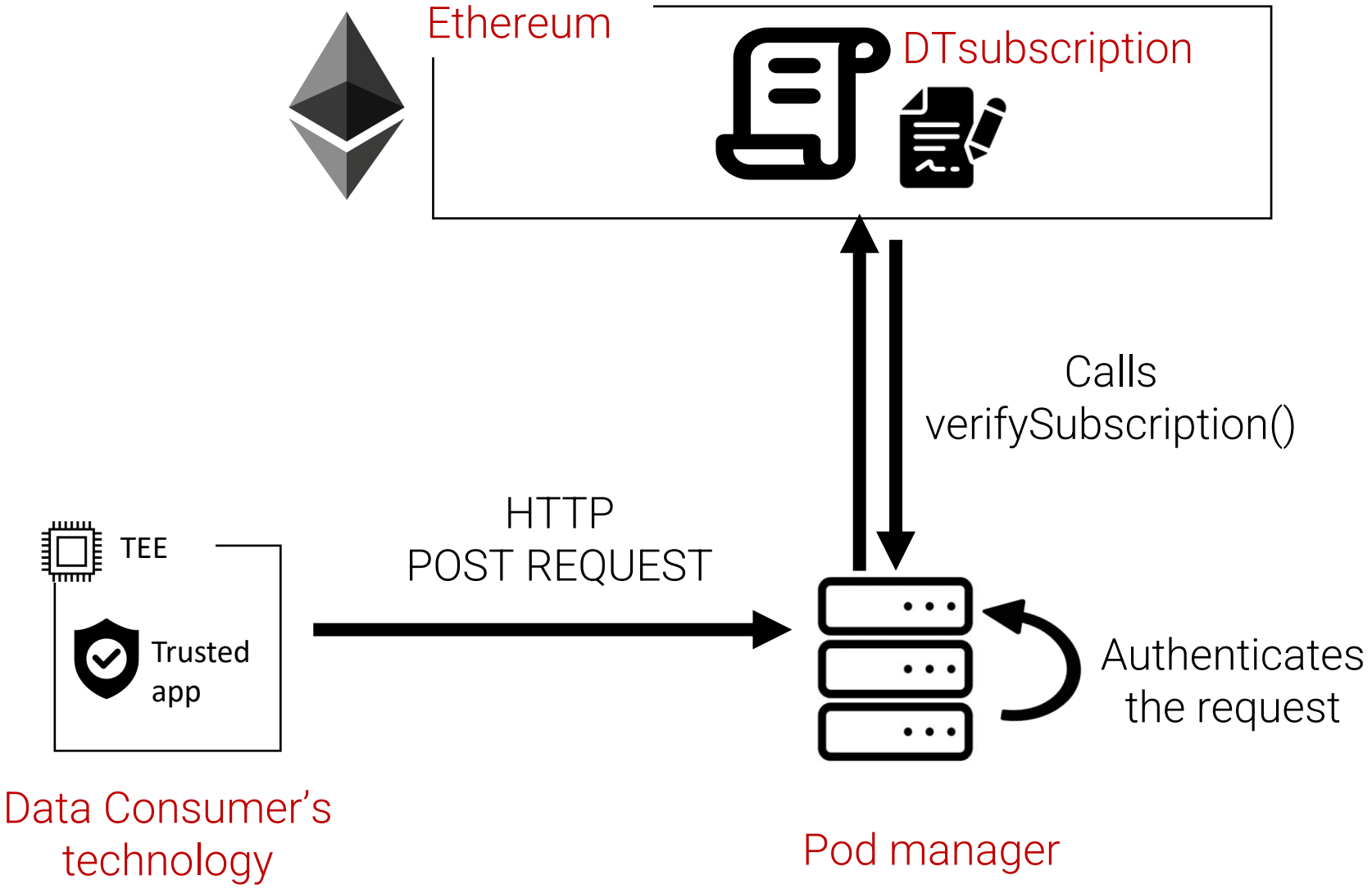


Data provision

Pods

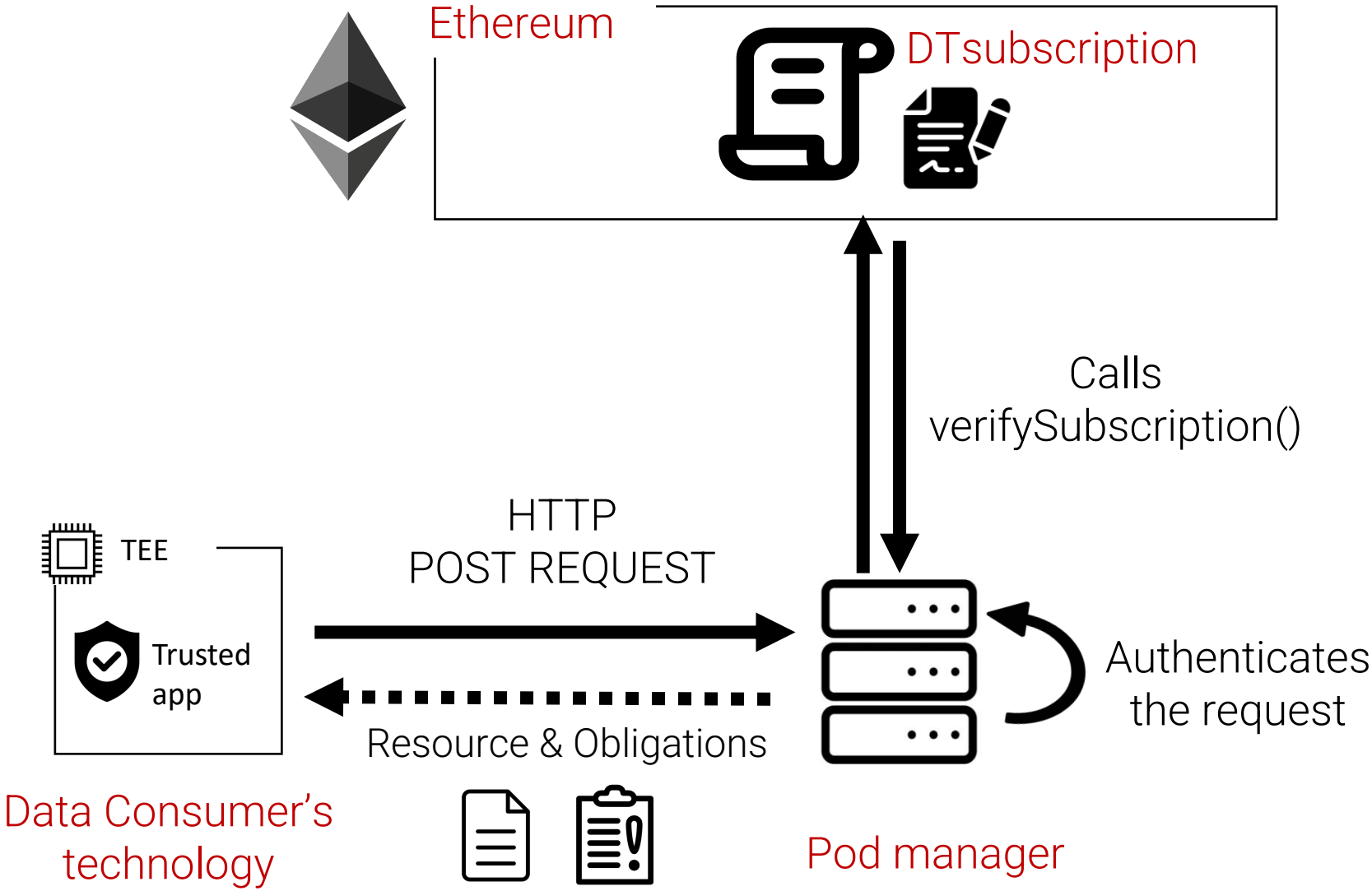


Data provision



Data provision

Pods



HTTP parameters

auth_token

Signature of a message obtained using an Ethereum private key

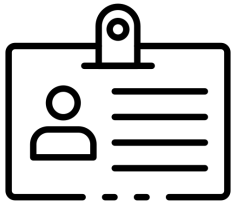
HTTP parameters

Pods

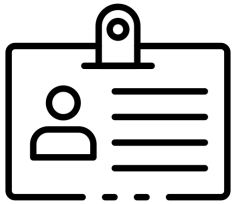
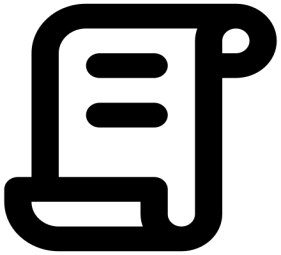
auth_token

Signature of a message obtained using an Ethereum private key

claimed_identity



Ethereum public address

HTTP parameters		Pods
auth_token		Signature of a message obtained using an Ethereum private key
claimed_identity		Ethereum public address
subscription_id		DTsubscription identifier

auth_token parameter

Encrypted with the user's private key

folder/..../folder/Resource.extension :*:* 1664558775

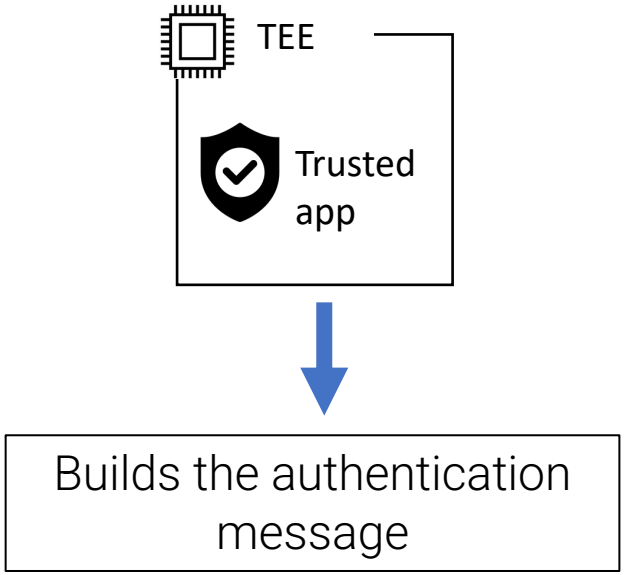
Location of the resource in the pod | Separator | Rounded Unix epoch

Remarkable functions

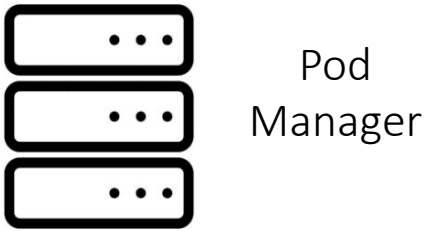
web3.eth.account.**sign_message**(unsigned_msg,private_key)

web3.eth.account.**recover_message**(unsigned_msg,signature)

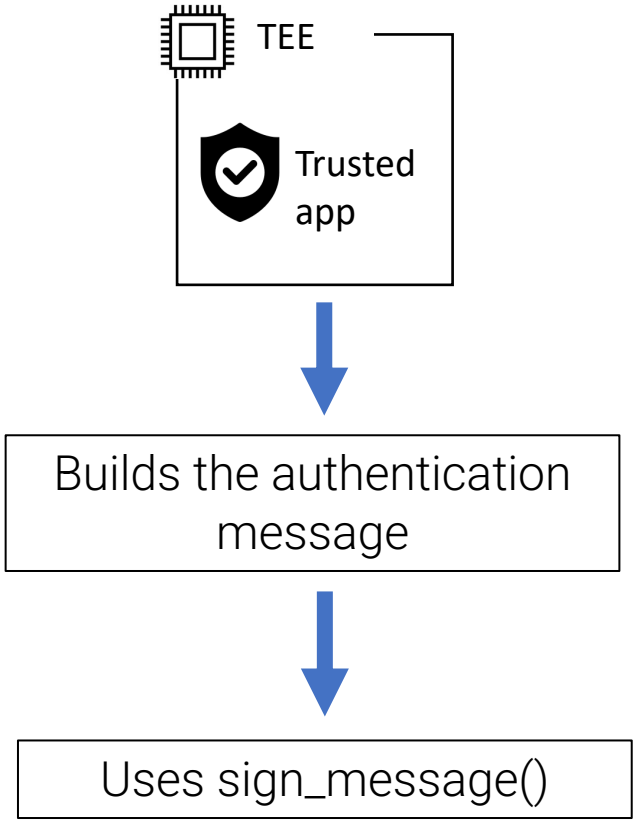
Authentication



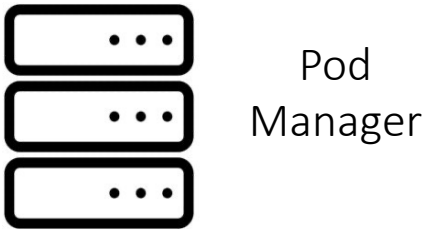
Pods



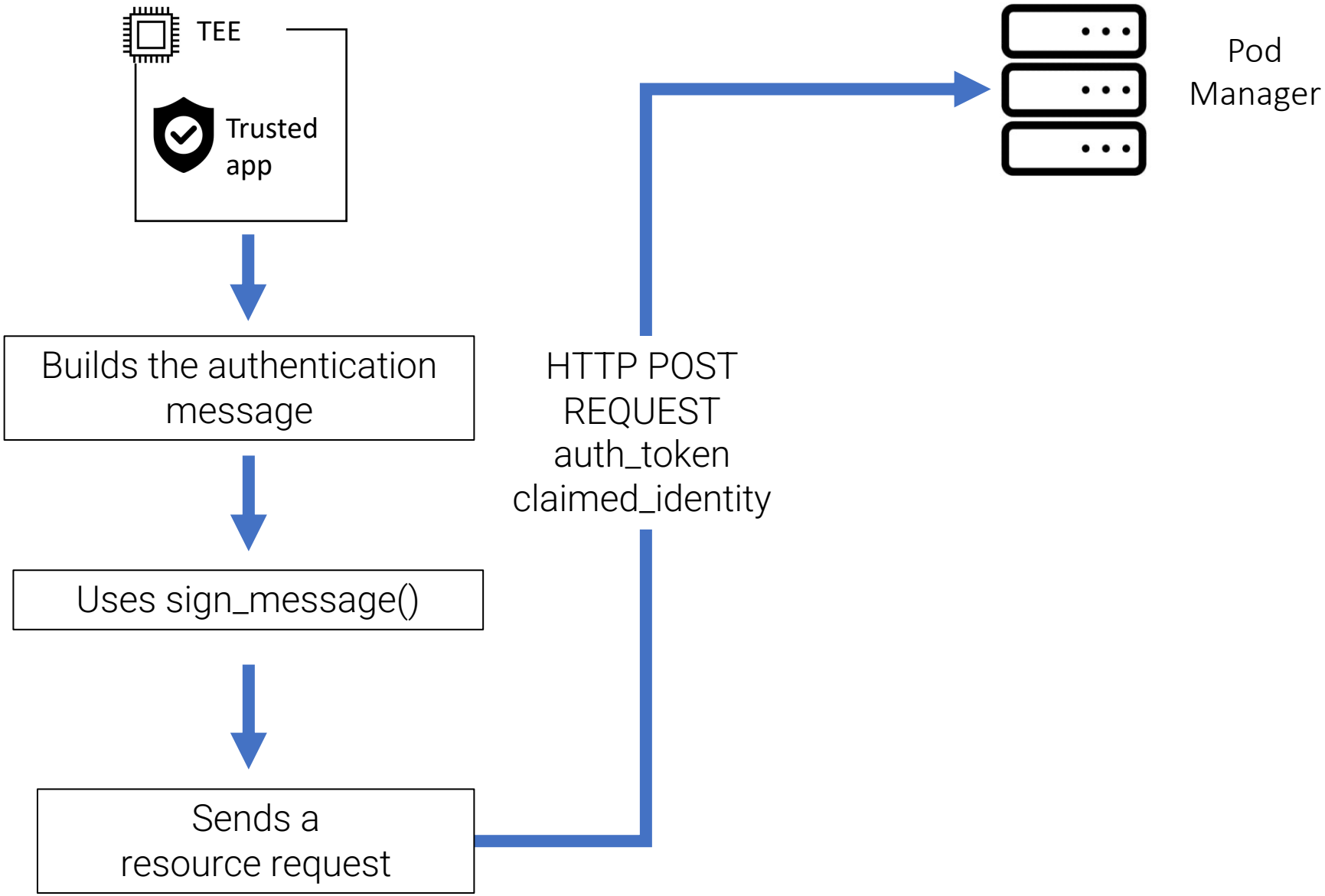
Authentication



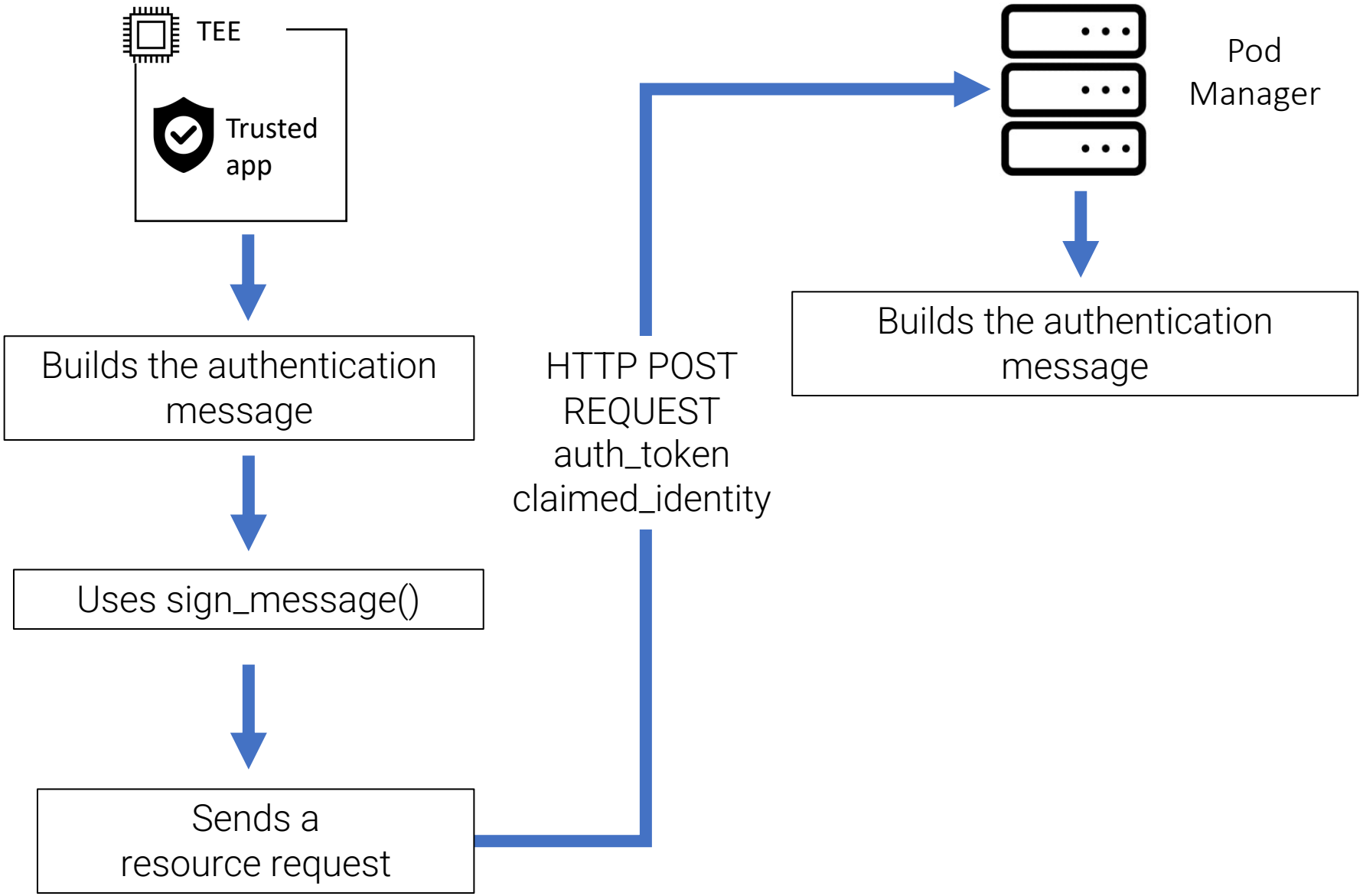
Pods



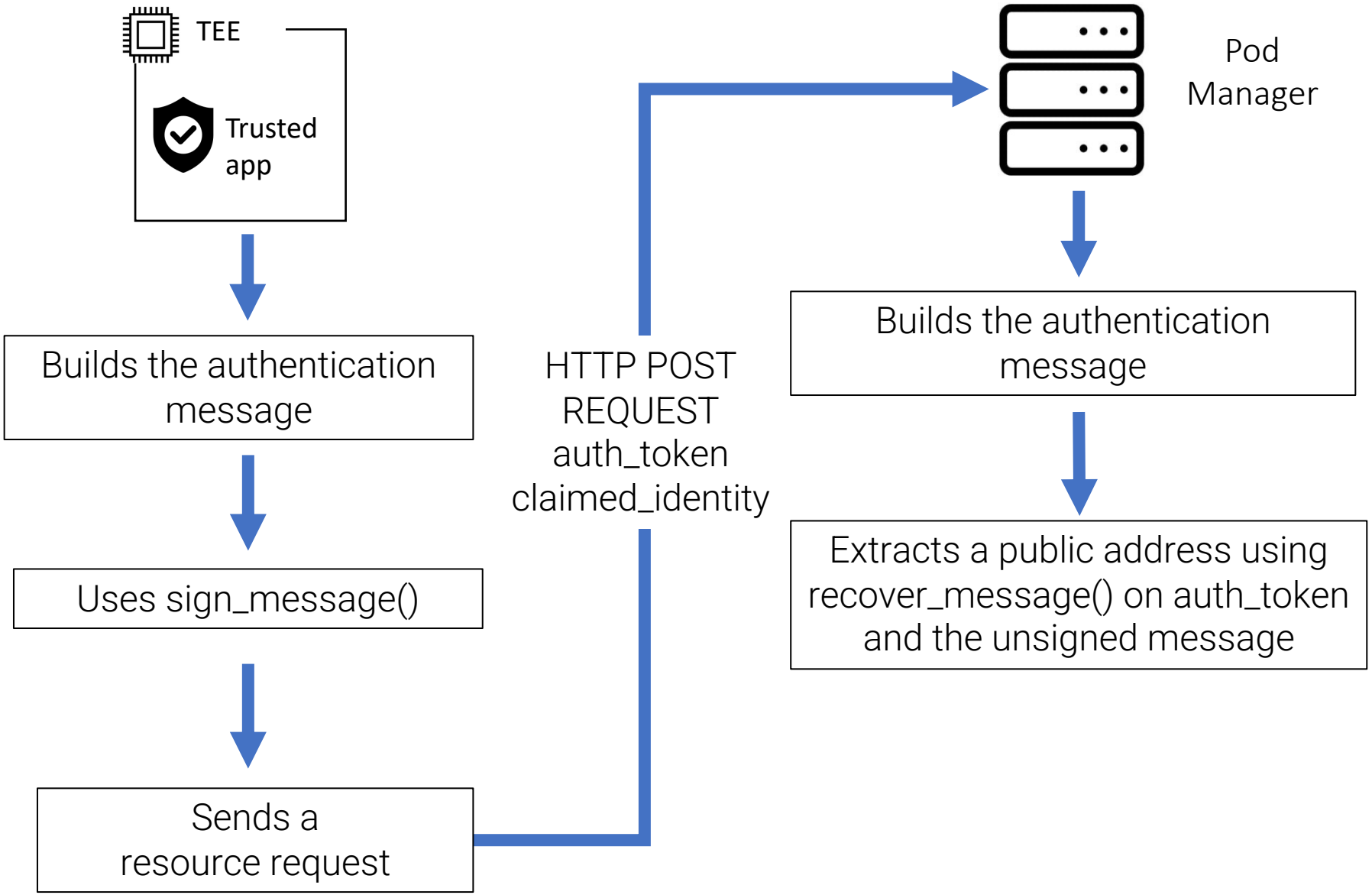
Authentication



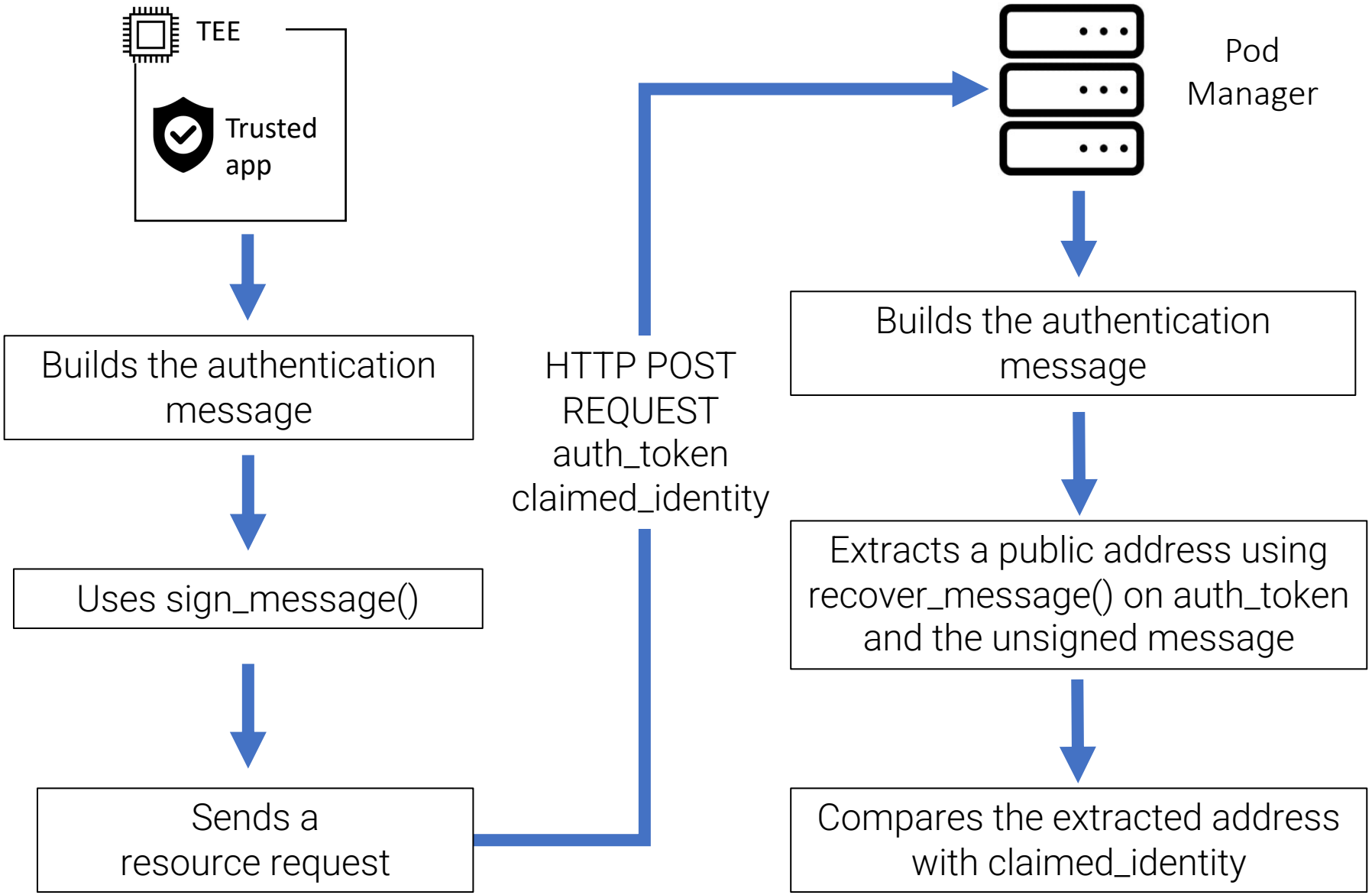
Authentication



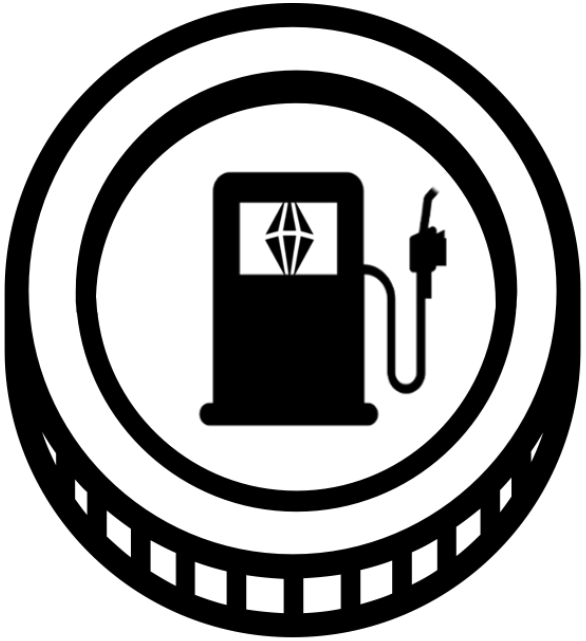
Authentication



Authentication

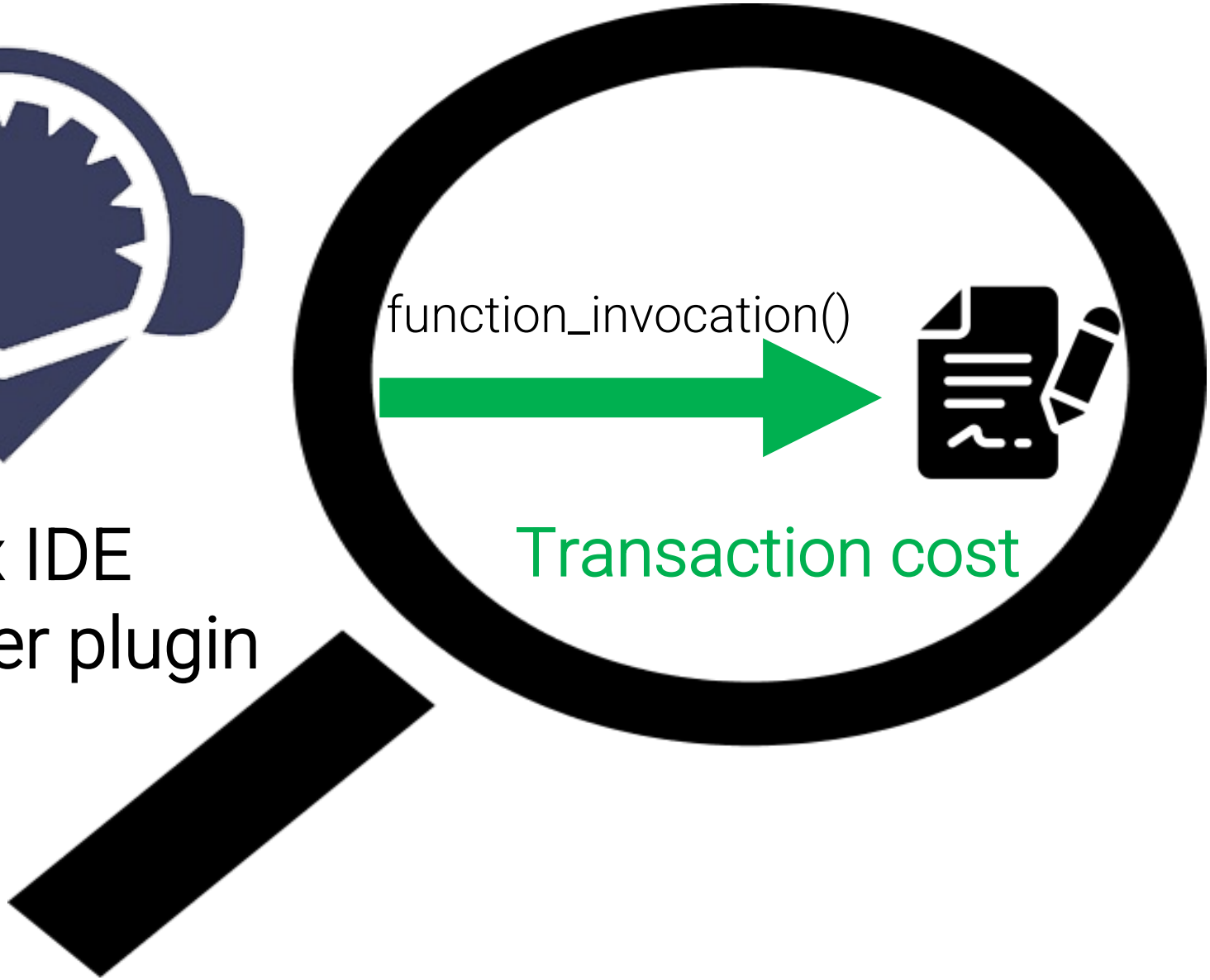


Subject of the evaluation



Gas

Remix IDE
Gas Profiler plugin



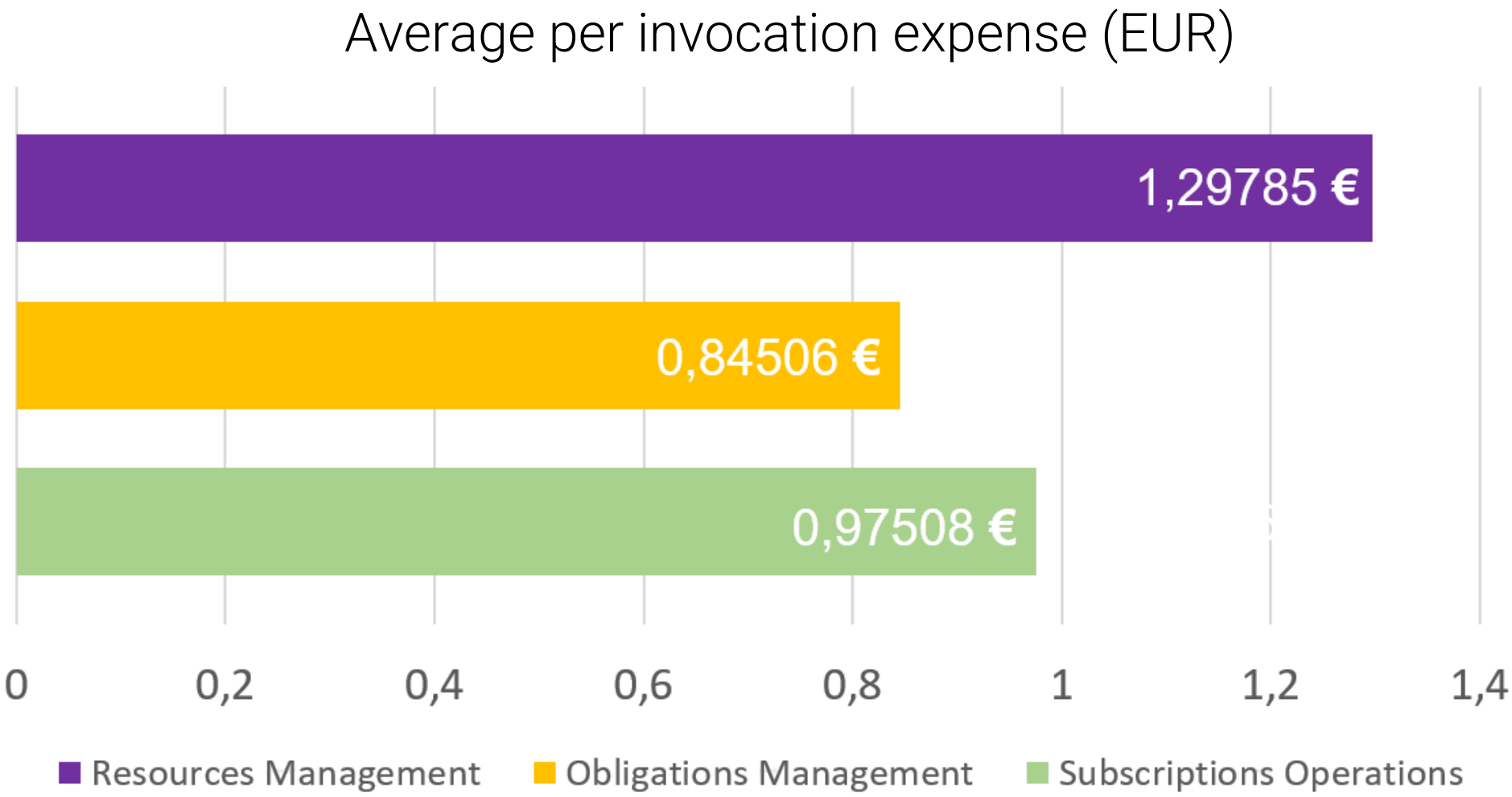
Methodology

Evaluation

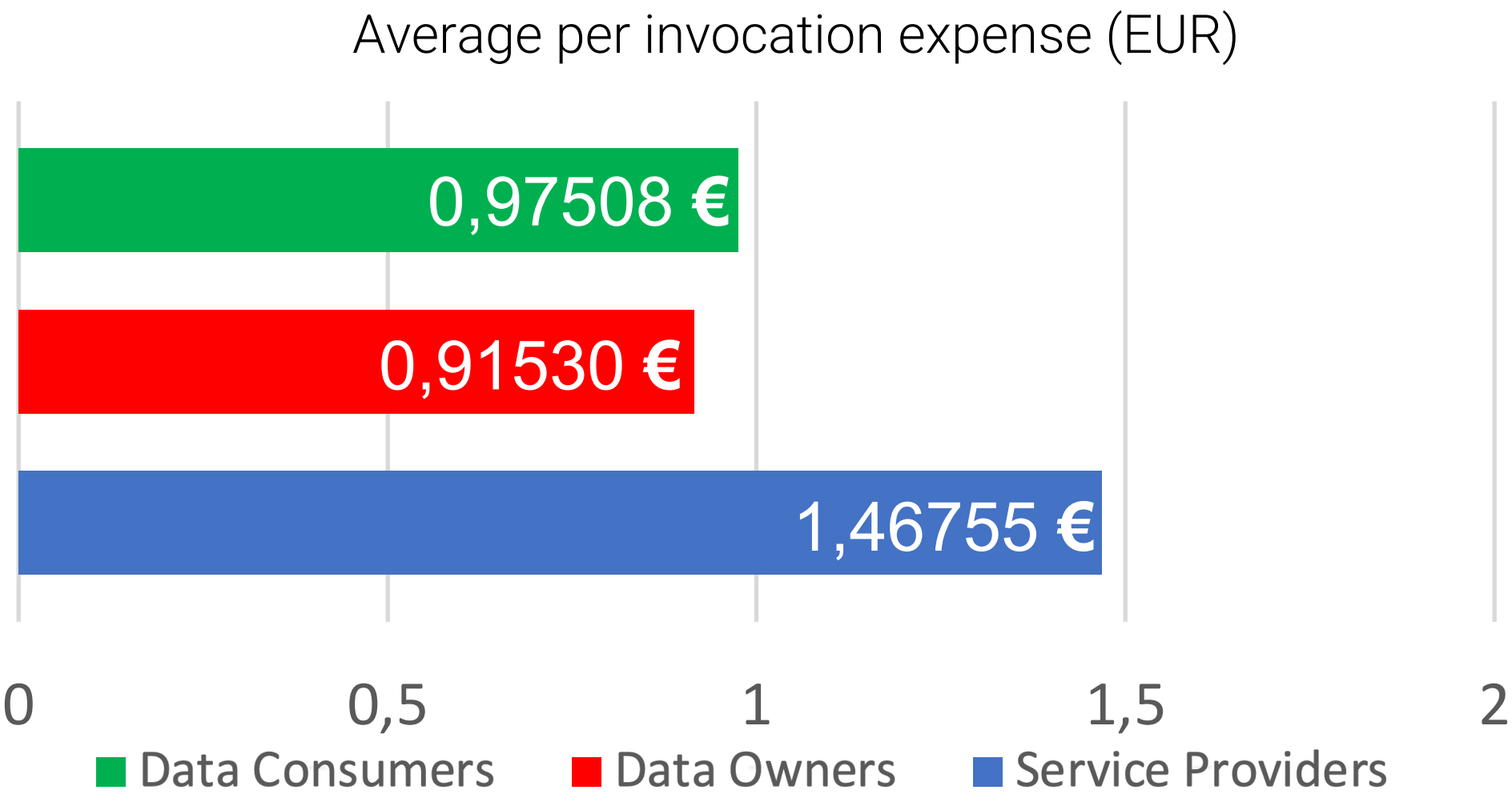
Function	Cost (Gas)	Target User
deployment	1623406	Service Providers
mint()	37640	Service Providers
burn()	36730	Service Providers
transfer()	36811	Service Providers, Data Owners, Data Consumers
transferFrom()	45752	Service Providers, Data Owners, Data Consumers
increaseAllowance()	46000	Service Providers, Data Owners, Data Consumers
decreaseAllowance()	15828	Service Providers, Data Owners, Data Consumers
allowance()	-	Service Providers, Data Owners, Data Consumers
balanceOf()	-	Service Providers, Data Owners, Data Consumers

Results table for the DTtoken smart contract

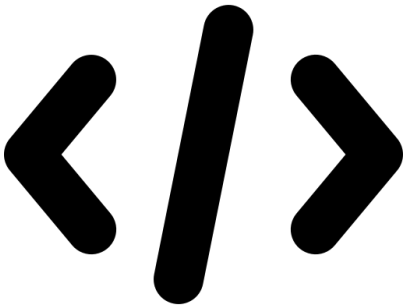
Results for data owners



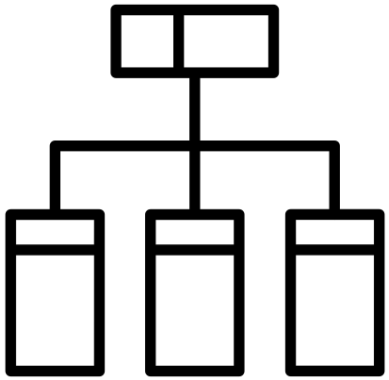
General results



How to reduce costs for users ?

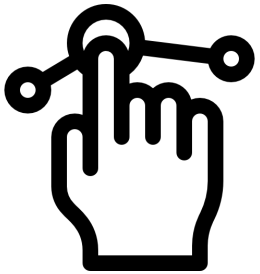


On-chain code optimization



Architecture alternatives

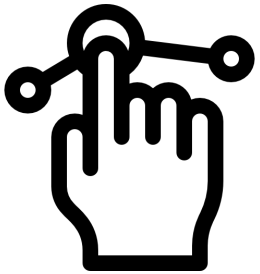
Future work



Conclusion

System usability

Future work



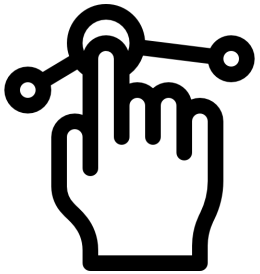
System usability

Integration with Ethereum 2.0

Conclusion

Future work

Conclusion



System usability

ethereum 2.0

Integration with Ethereum 2.0

HYPERLEDGER

Algorand

Blockchains comparasion

Publications

- Blockchain based Resource Governance for Decentralized Web Environments, Davide Basile, Claudio Di Ciccio, Valerio Goretti, Sabrina Kirrane https://arxiv.org/abs/2301.06919

- An Ethereum-based system for resource ownership in data markets, Davide Basile, MSc Thesis.

- Safe and controllable information consumption for data market applications: A solution based on Trusted Execution Environments and the Ethereum blockchain, Valerio Goretti, MSc Thesis.