ADVANCED TOPICS

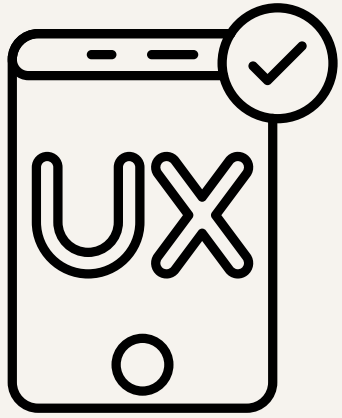
Created: Sept 2023
Last Edited: Oct 2023

UofT: CSCD71F23
-David Liu, Founder of dApp Technology Inc.

PROBLEMS WITH EOA WALLETS

Key Recovery

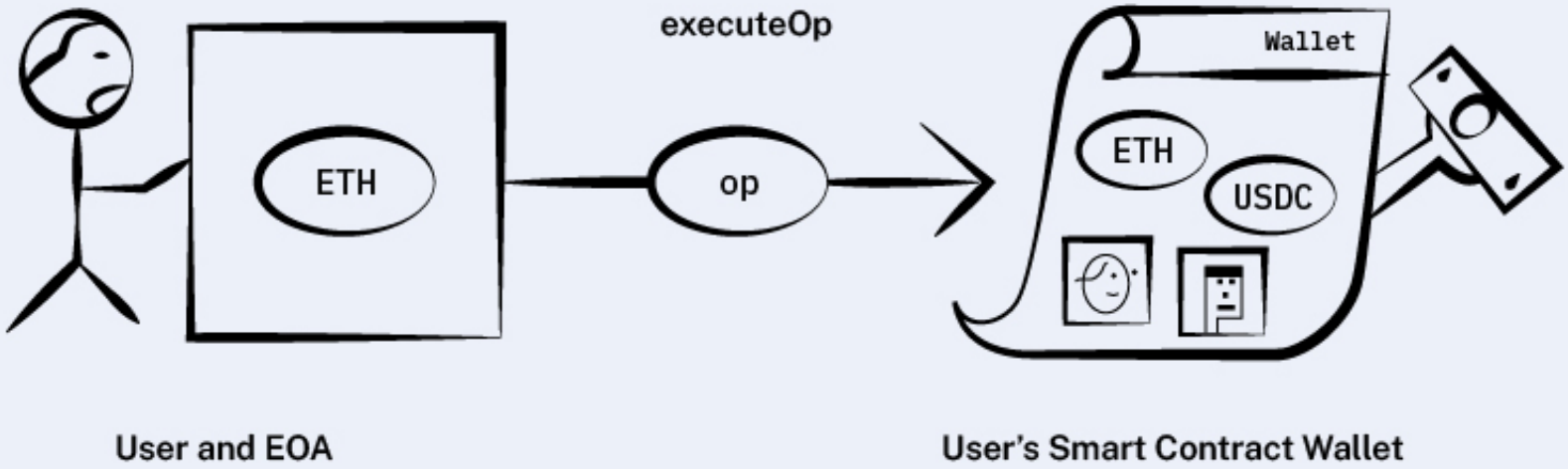
Access Control



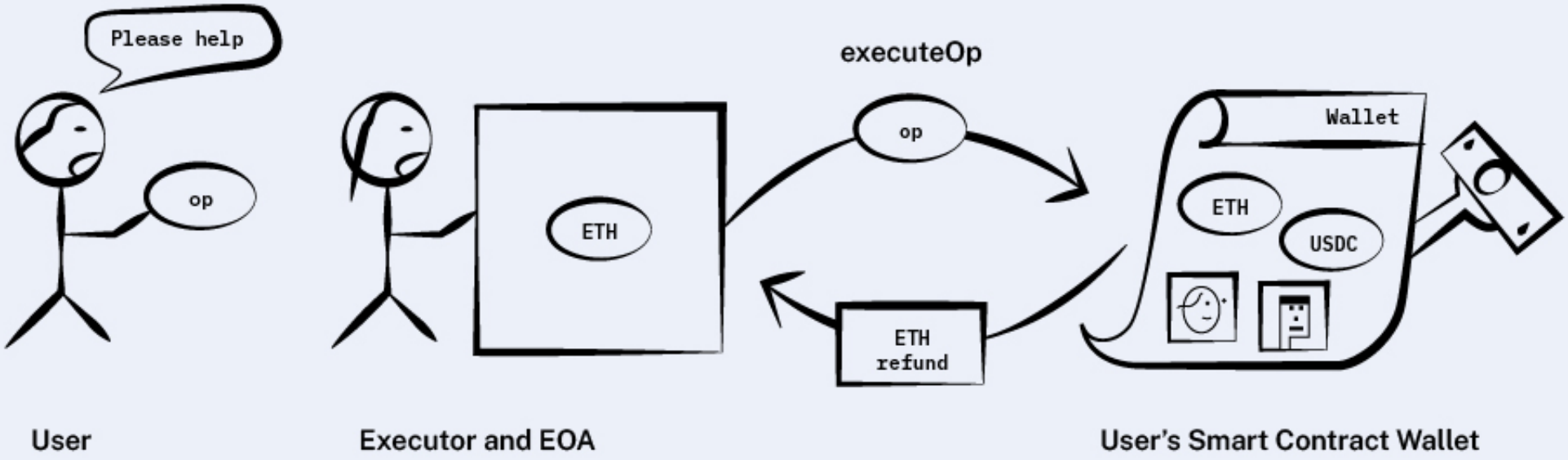
User Experience

ACCOUNT ABSTRACTION

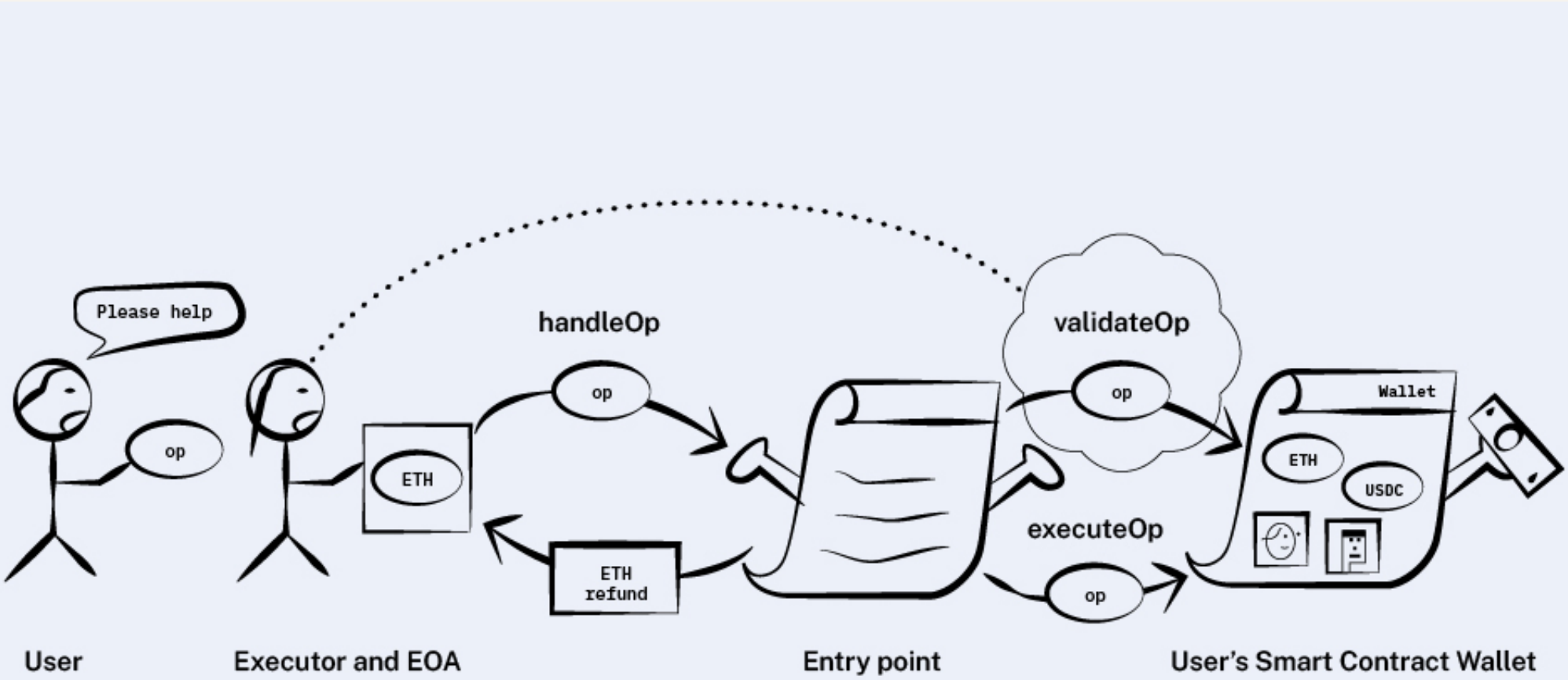
- How to make Smart Contract Wallet?



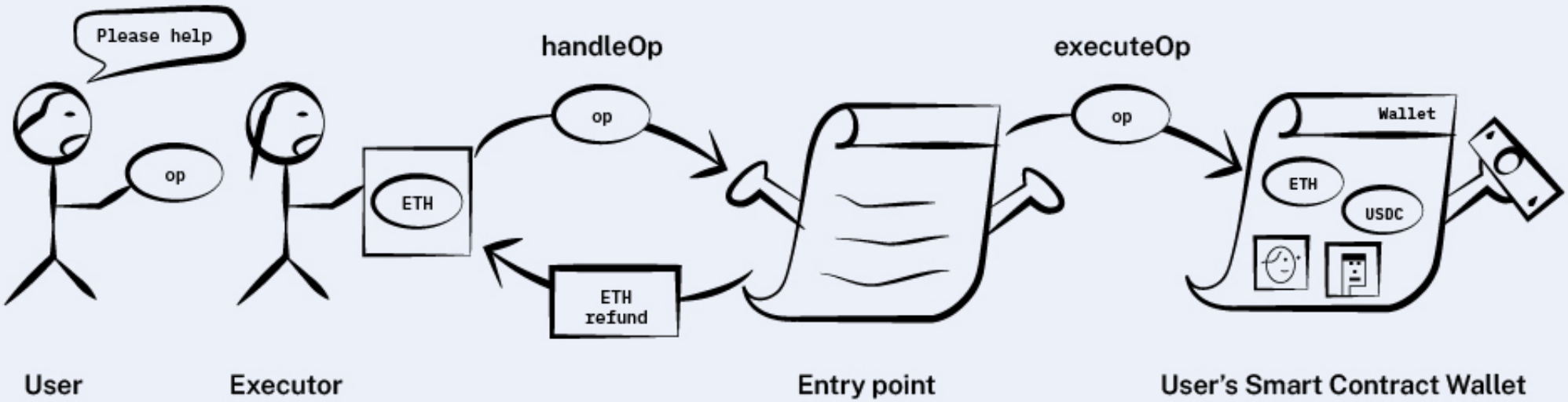
Oct 2023
https://www.alchemy.com/blog/account-abstraction



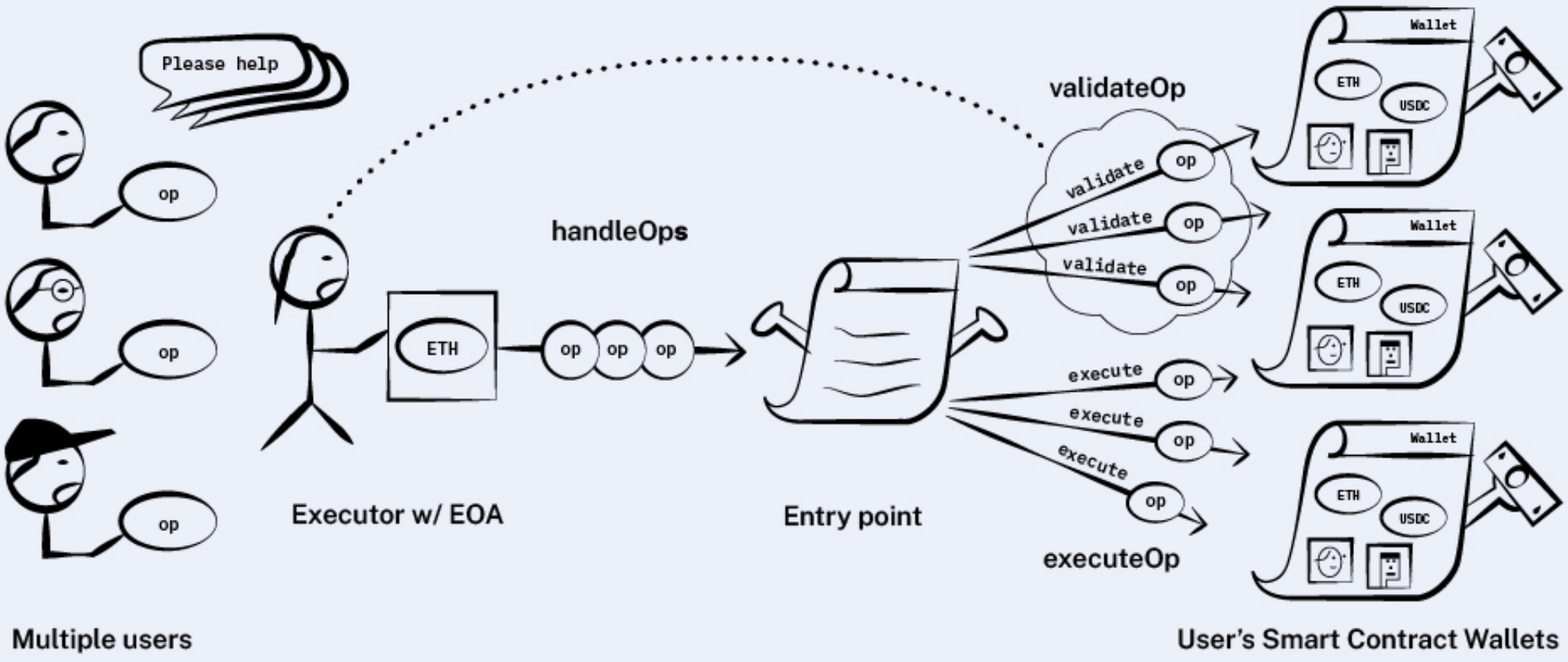
Oct 2023
https://www.alchemy.com/blog/account-abstraction



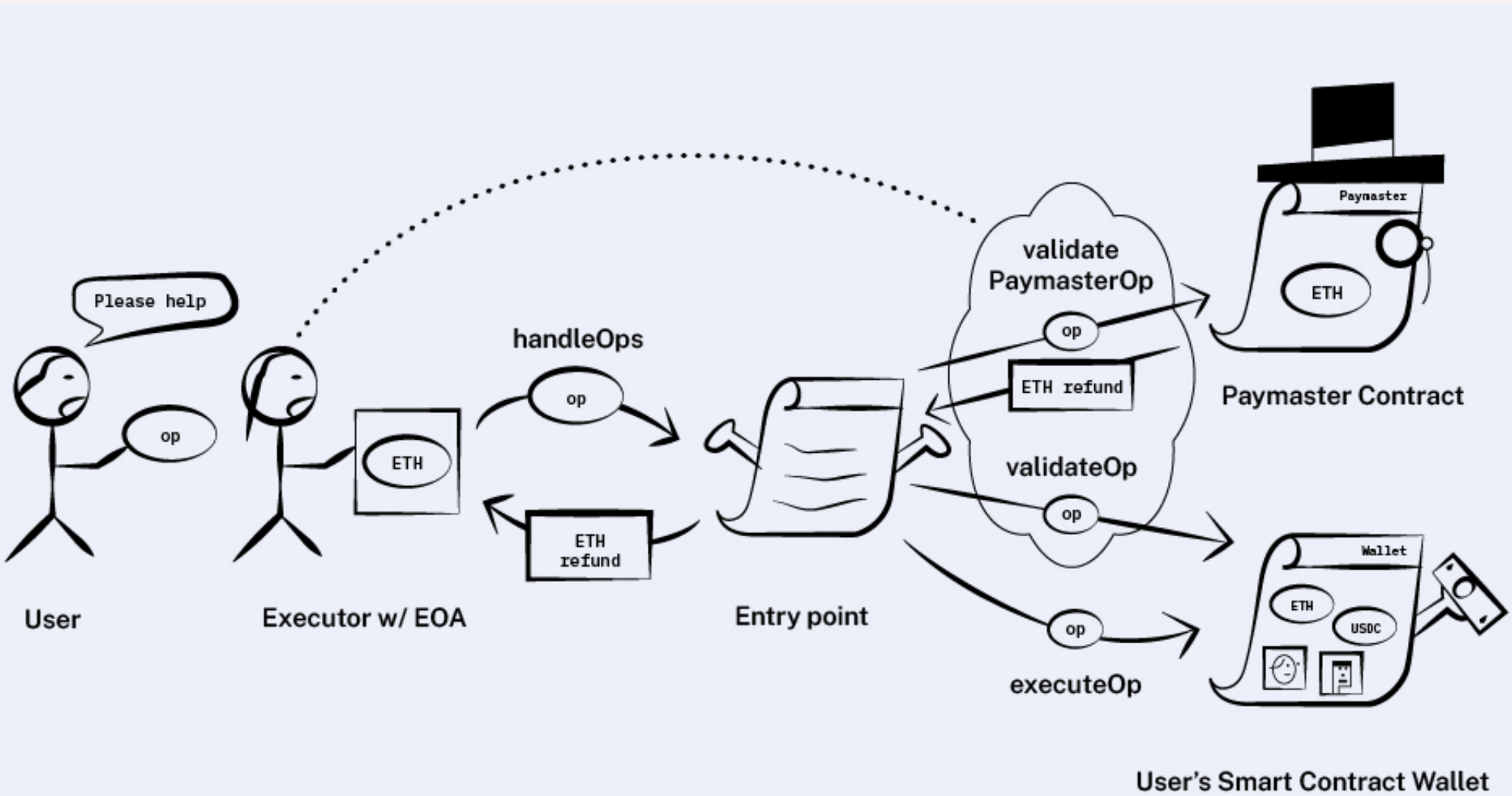
Oct 2023
https://www.alchemy.com/blog/account-abstraction



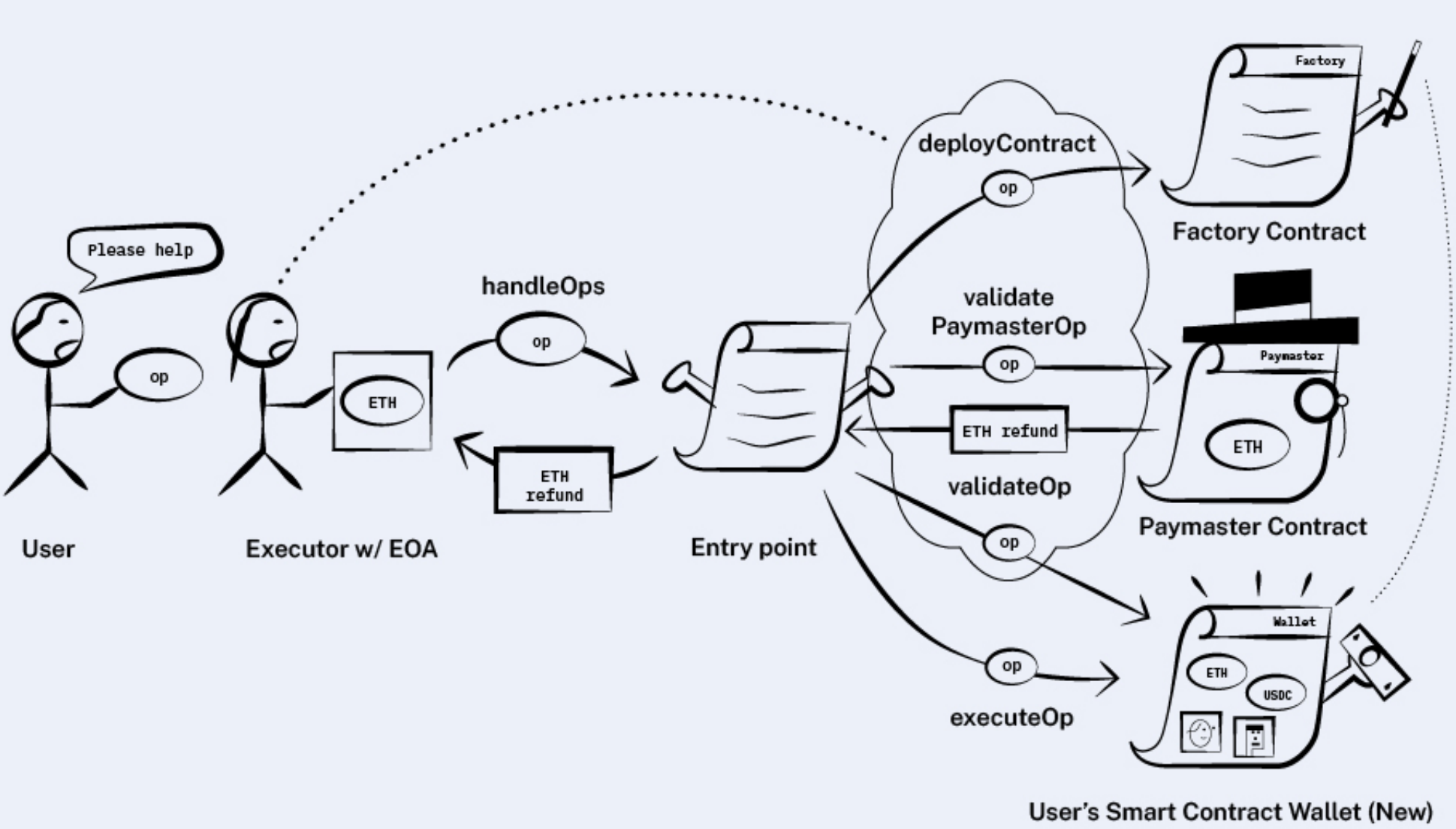
Oct 2023
https://www.alchemy.com/blog/account-abstraction



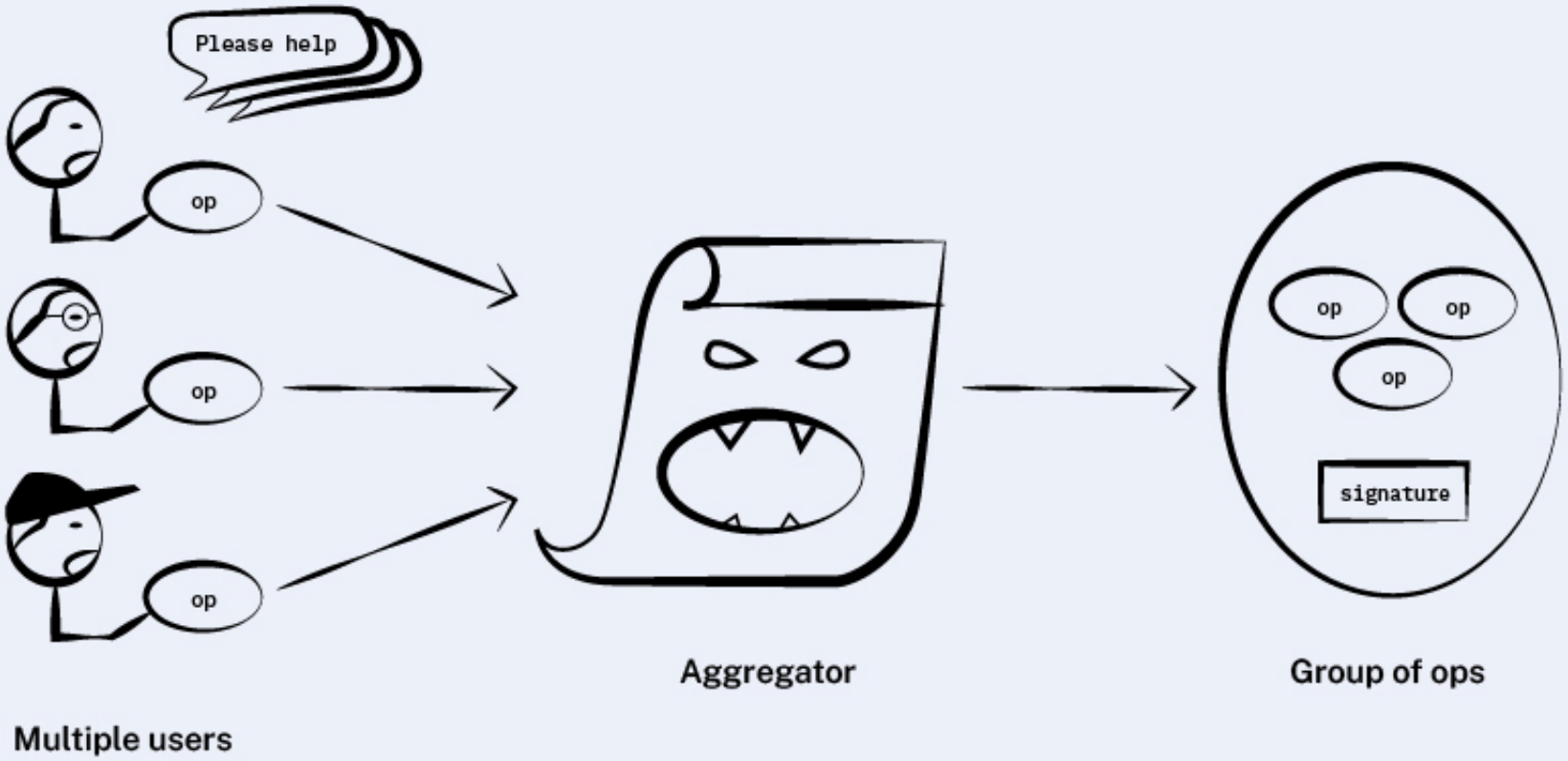
Oct 2023
https://www.alchemy.com/blog/account-abstraction



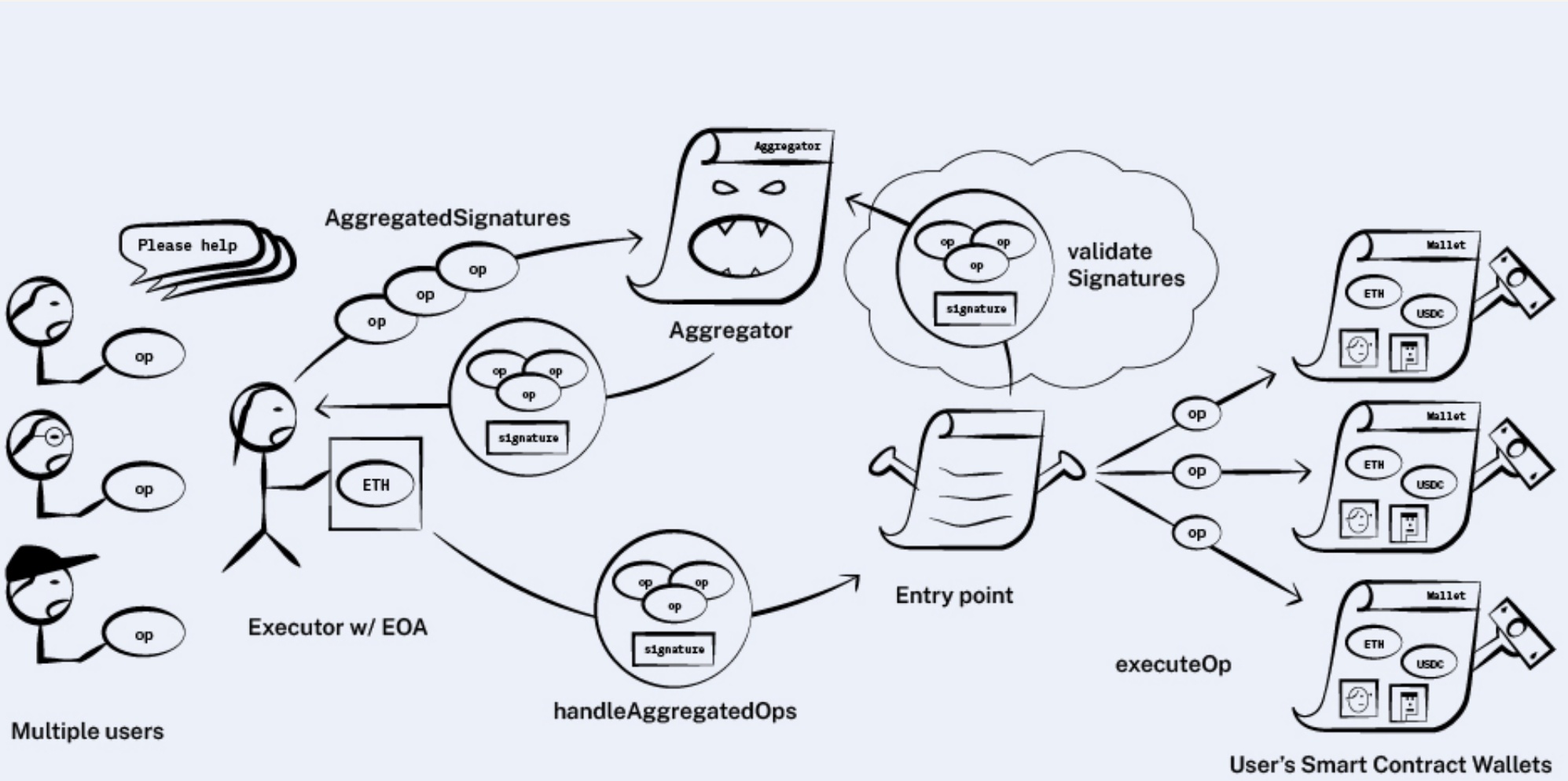
Oct 2023
https://www.alchemy.com/blog/account-abstraction



Oct 2023
https://www.alchemy.com/blog/account-abstraction



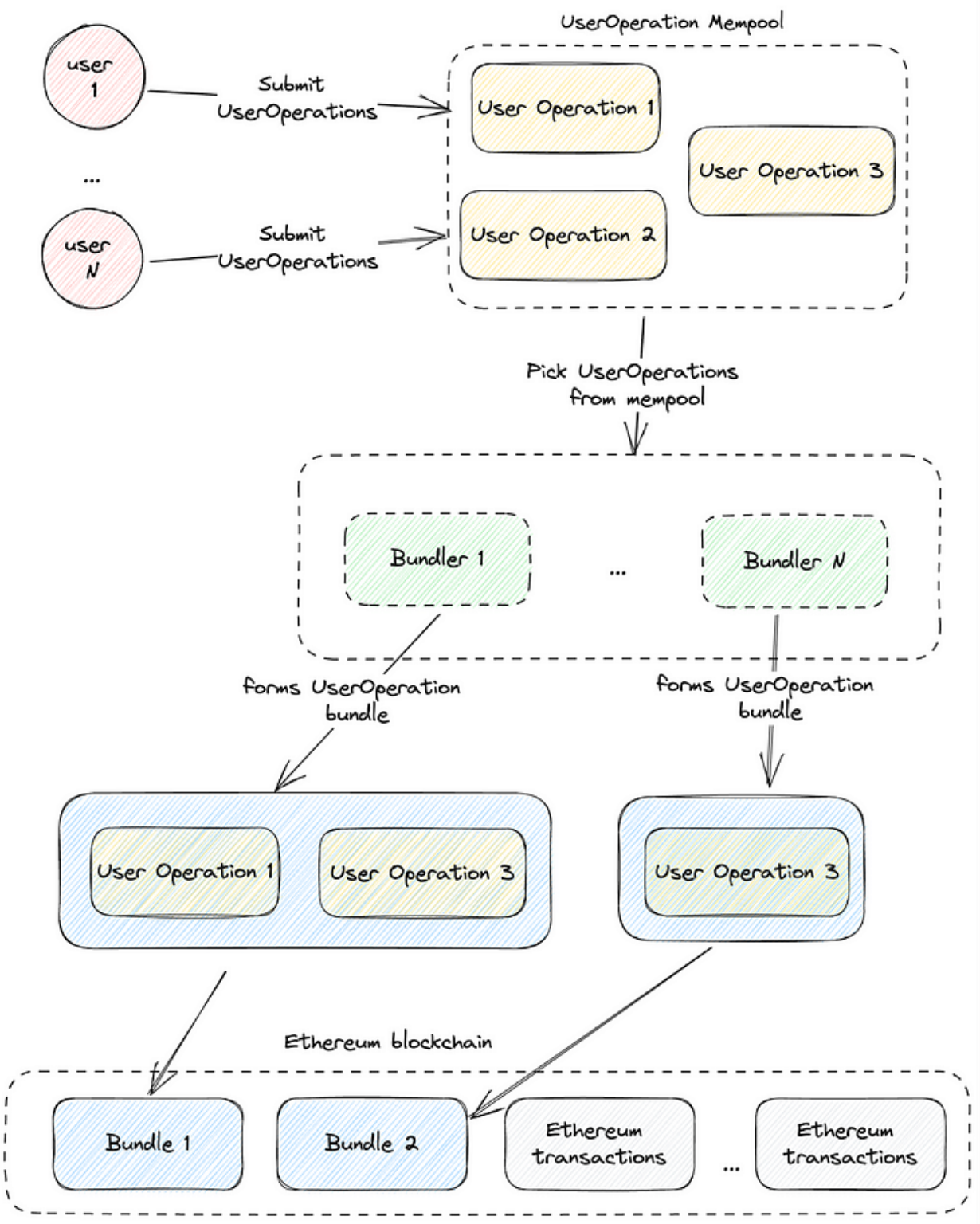
Oct 2023
https://www.alchemy.com/blog/account-abstraction



Oct 2023
https://www.alchemy.com/blog/account-abstraction

ACCOUNT ABSTRACTION

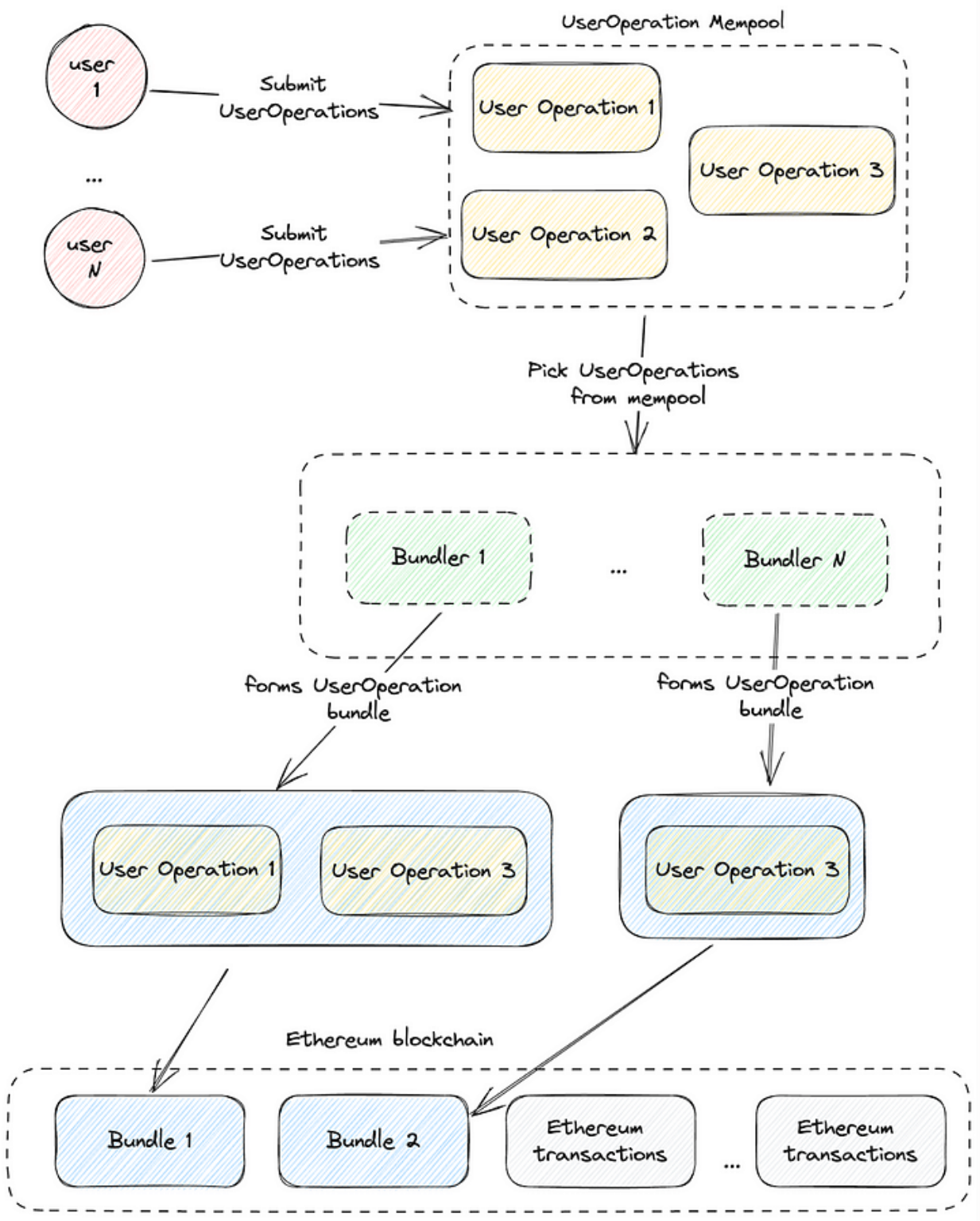
- Non-protocol change implementation in EVM as EIP-4337
- Asset ownership moved to smart contract wallet, accessed by any key pair
- Key pairs can be updated
- Wallets are now programmable



Sept 2023
https://medium.com/@olatunjimayowa0396/account-abstraction-security-considerations-risk-mitigation-best-practices-17dc657b6dc9

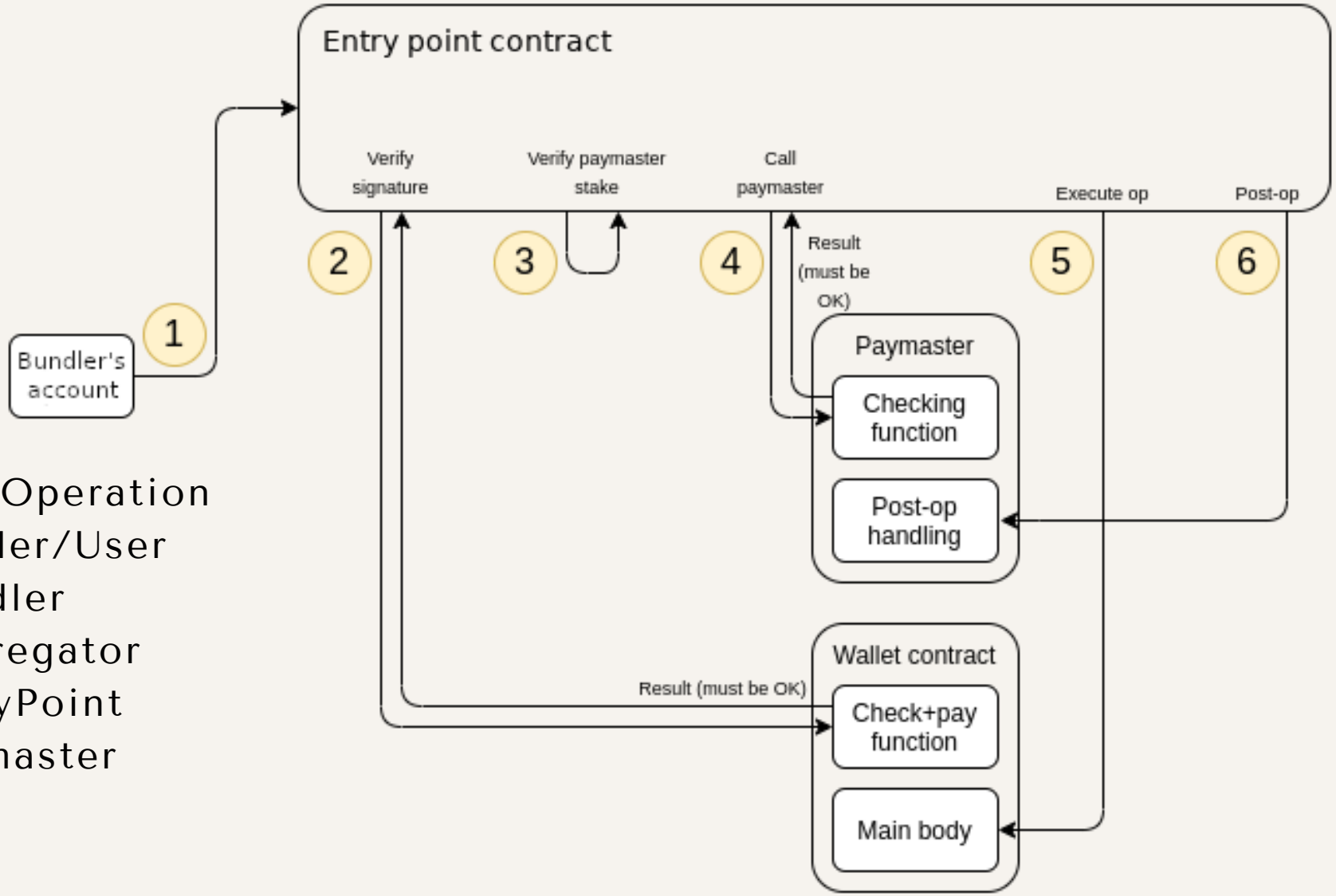
EIP-4337

- UserOperation
- Sender/User
- Bundler
- EntryPoint
- Aggregator
- Paymaster



Sept 2023
https://medium.com/@olatunjimayowa0396/account-abstraction-security-considerations-risk-mitigation-best-practices-17dc657b6dc9

EIP-4337 BUNDLE SUBMISSION



- UserOperation
- Sender/User
- Bundler
- Aggregator
- EntryPoint
- Paymaster

Sept 2023
https://eips.ethereum.org/EIPS/eip-4337

ENS

Web2 uses DNS (Domain Named Service).
Purpose is to change machine address to human readable address.
Example: www.dogs.com -> 192.256.220.91

Web3 uses ENS (Ethereum Named Service).
Purpose is to change machine address to human readable address.
Example: david.eth -> 0x9e9809988185b0ab70a992f0aaf9e057806c0f92
Example: dogs.eth -> ipfs://QmccqhJg5wm5kNjAP4k4HrYxoqaXUGNuotDUqfvYBx8jrR/qr#enter%252520text%252520here

ENS

How does it work?

There are 2 categories of smart contracts that makes up ENS. The Registry and the Resolver.

Registry: stores the owner and the resolver contract address. Also registers subdomains. Example: corgi.dog.eth

Resolver: stores the actual address of the .eth name

Lookup users will interact with the Registry and then the Resolver to get the actual address.

ENS

Additional top level domains:
.crypto
.xyz
.club

Proof of ownership represented as an NFT.

ENS NFTs are rented and need to pay a yearly fee in ETH.

ENS is decentralized and open source.

PRIVACY PROBLEM

Sept 2023
https://www.sciencedirect.com/science/article/abs/pii/S0167404820303230

ZERO KNOWLEDGE PROOF

A way to prove a statement is true, without revealing the data itself.

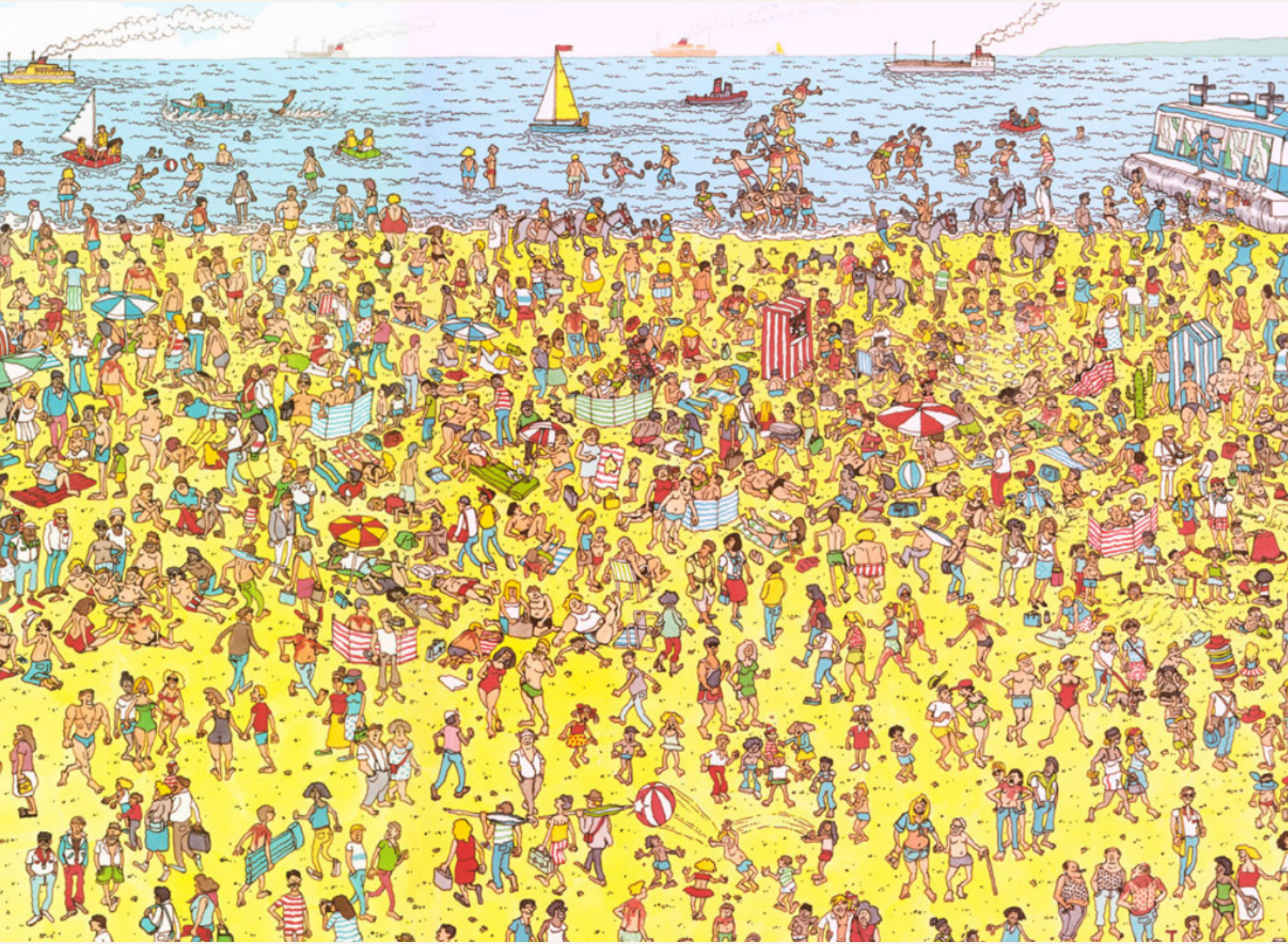
ZK Proofs satisfies 3 properties:

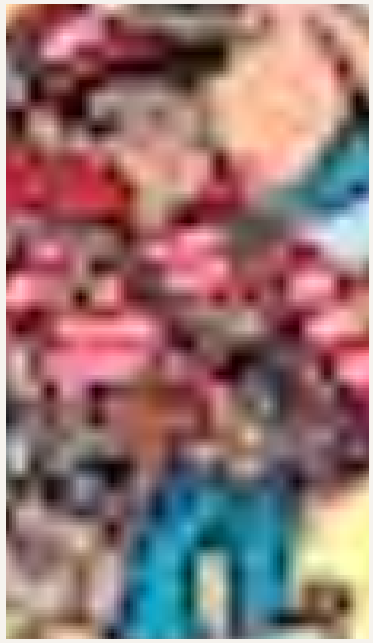
1. Completeness
2. Soundness
3. Zero Knowledge

Examples:

1. Where's Waldo
2. Colour blind ball


WHERE'S
?
WALDO®





ZK-SNARK

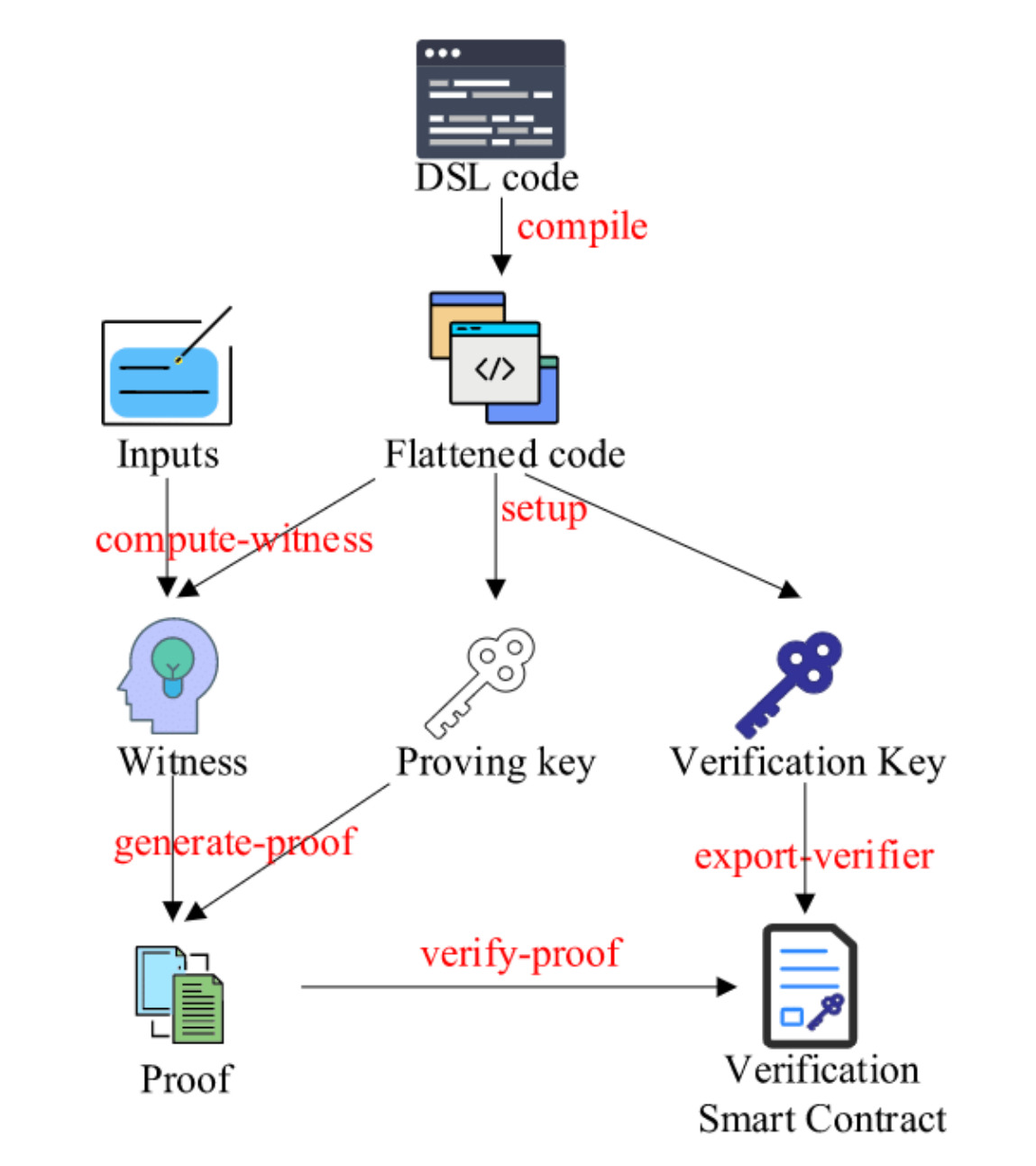
Zero-knowledge succinct non-interactive argument of knowledge

- Succinct - requires minimal computational resources and space to create and verify.
- Non Interactive - require only a single round of interaction between the prover and the verifier

Ex: Groth16

ZK-SNARK IN ETH

- Verify(
  public_inputs,
  private_inputs,
  proof)
- Trusted Setup for creation of Common Reference String, toxic waste must be deleted
- DSL: Domain Specific Language
- Witness is private + public inputs + other info necessary for the proof



Sept 2023
https://www.sciencedirect.com/science/article/abs/pii/S0167404820303230

ZK PROOF COMPARISON

Trusted setup

zk-SNARKs

Prover	Verifier	Size
2.3s	10ms	288B
Very fast	Fastest	Smallest

Bulletproofs

Prover	Verifier	Size
30s	1100ms	1,3KB
Slowest	Slowest	Middle

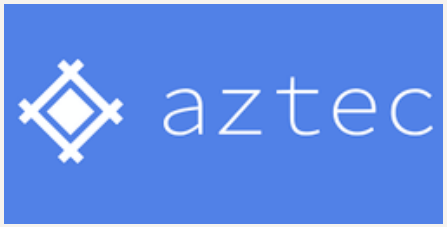
zk-STARKs

Prover	Verifier	Size
1.6s	16ms	>40KB
Fastest	Very fast	Big

Sept 2023
https://commons.wikimedia.org/wiki/File:STARK_proofs_diagram.jpg

ZK PROOF APPLICATION

- Aztec Protocol: Privacy for movement of tokens
- ZK-Sync: Layer2 Scaling Solution
- Iden3: Privacy for Decentralized Identity



zkSync

iden3

LARGE DATA STORAGE

IPFS

Interplanetary File System is a form of Decentralized File Sharing.

Web2 uses location based addressing.
Example: https://images.com/dog.png
Example: 142.127.240.100/dog.png

If the hosting server is down, users cannot retrieve their files.

IPFS

Web3 IPFS uses content based addressing.

Example:
ipfs://Qmf3xGUcdwzynagoTjZkKdWpxuo5kRVBdv38rdH9VfQ47j?filename=dog.png

Example:
https://ipfs.io/ipfs/Qmf3xGUcdwzynagoTjZkKdWpxuo5kRVBdv38rdH9VfQ47j?filename=dog.png

Qmf3xGUcdwzynagoTjZkKdWpxuo5kRVBdv38rdH9VfQ47j is the content id (CID), derived from the hash of the file data.

IPFS

How does it work?

IPFS data is organized IPFS Objects.

Each Object contains data up to 256kb and links to other IPFS Objects.

Data larger than 256kb can be split up into several objects, with each object linking to each other.

IPFS

Advantages:

1. Data Availability
2. Efficient storage (no duplicates)
3. Speed of download

Pinning Services:

1. Pinata
2. Filecoin

IPFS

Challenge: Privacy
Solution: Encrypted Content Hash

Challenge: Immutable data
Solution: Directed Acyclic Graph

Challenge: Malicious or inaccurate data served
Solution: Verification by rehashing content

Challenge: Slow download speed due to long distance
Solution: Serve files P2P with closest node

Resources Used:

https://coinsbench.com/about-evm-opcode-gas-ethereum-accounts-9f0896f09d04

https://ethereum.org/

https://hardhat.org/

https://docs.ethers.io/v5/

https://www.openzeppelin.com/

https://takenobu-hs.github.io/downloads/ethereum_evm_illustrated.pdf

https://www.skillsoft.com/