

Pedro Gomes

Founder & Director
WalletConnect Foundation

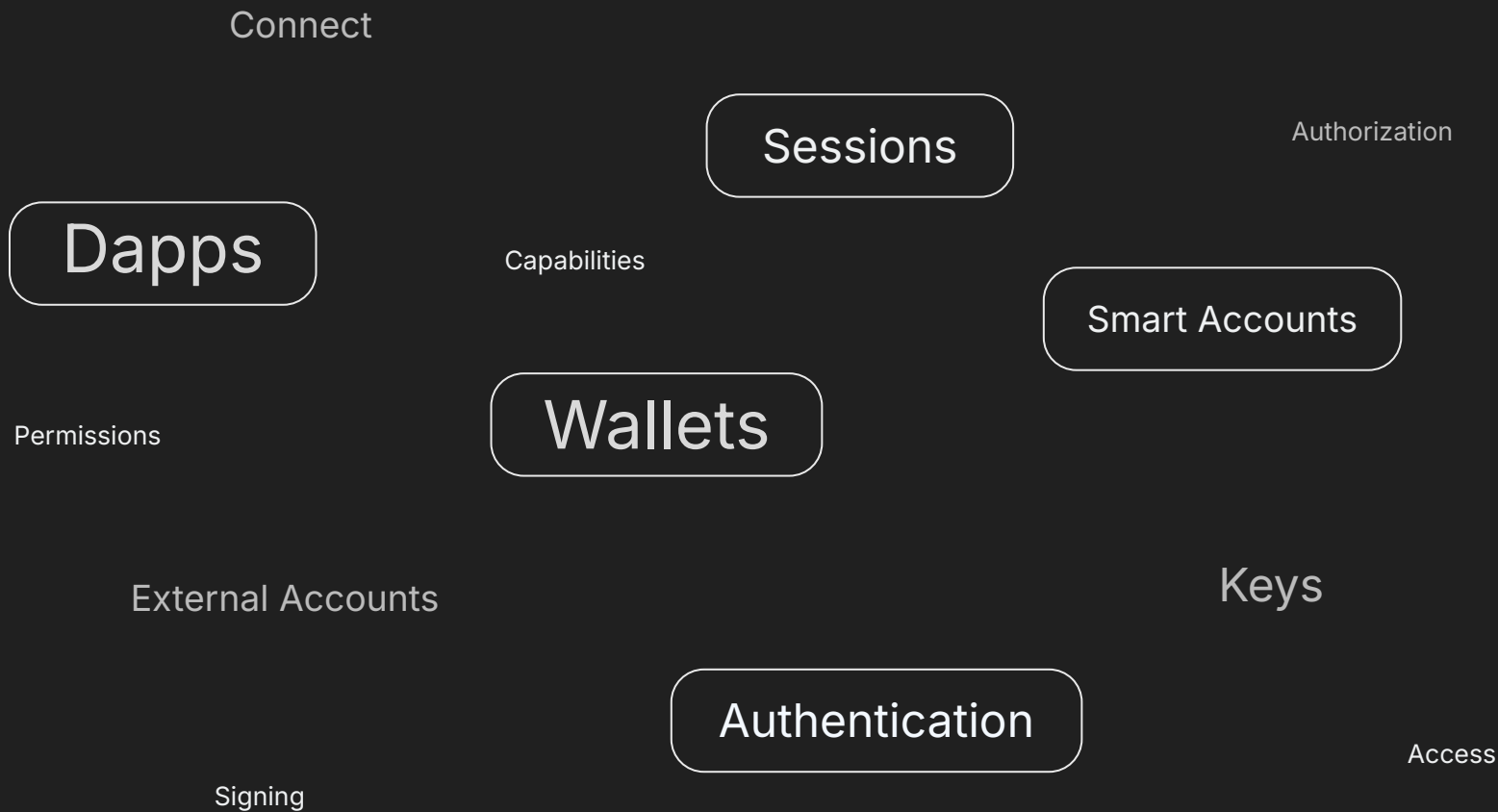


Smart
Accounts

need Smart
Sessions

Breaking down the lingo







authentication

/ɔːˌθɛntɪˈkeɪʃn/

noun

the process or action of proving or showing something to be true, genuine, or valid.
"the prints will be stamped with his seal and accompanied by a letter of authentication"

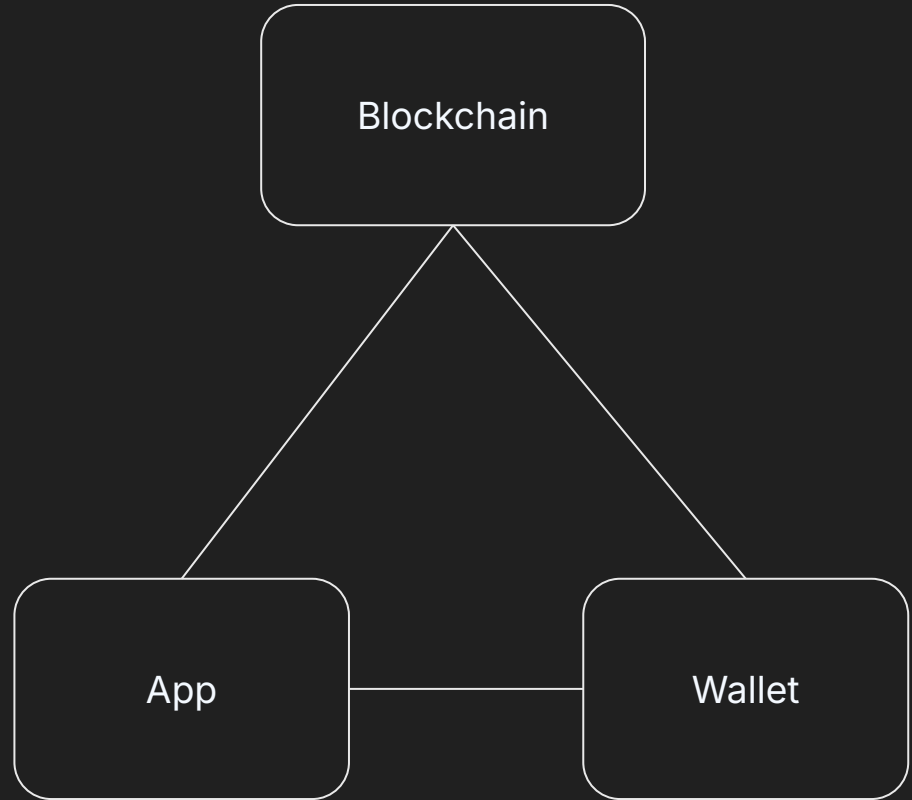
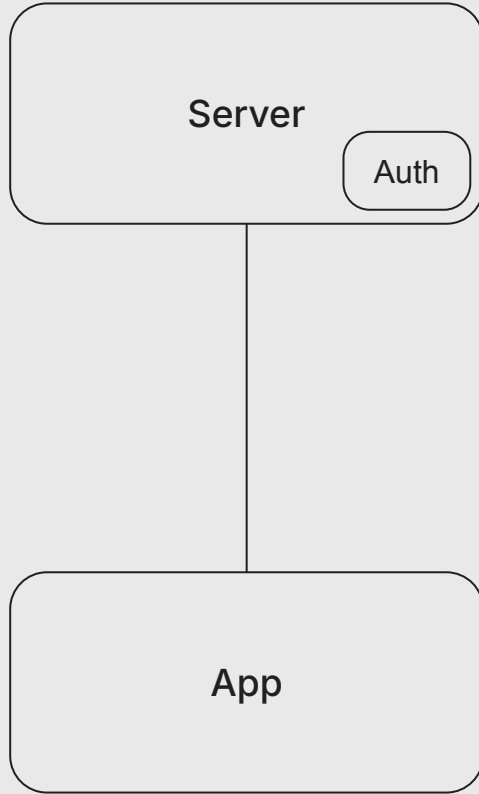
- **COMPUTING**

the process or action of verifying the identity of a user or process.
"user authentication for each device ensures that the individual using the device is recognized by the company"

LET ME IN!

Less (clicks) is more!

Why is **web3** different?



Wallet = Credentials + Signing + Account

| | Mobile & Browser | Hardware Devices | Cloud or MPC |
|-------------|----------------------|------------------------|------------------------|
| Credentials | Password or Pin Code | Pin Code or Biometrics | Email / Phone / Social |
| Signing | Local Software | Local Hardware | Remote Server or Node |
| Account | External Account | External Account | External Account |

ERC-4361

Sign-In with Ethereum



`https://example.com` wants you to sign in with your Ethereum account:
`0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2`

I accept the ExampleOrg Terms of Service: `https://example.com/tos`

URI: `https://example.com/login`

Version: 1

Chain ID: 1

Nonce: 32891756

Issued At: 2021-09-30T16:25:24Z

Resources:

- `ipfs://bafybeiemxf5abjwjbikoz4mc3a3dla6ual3jsqpdr4cjr3oz3evfyavhwq/`
- `https://example.com/my-web2-claim.json`



`https://example.com` wants you to sign in with your Ethereum account:
`0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2`

I accept the ExampleOrg Terms of Service: `https://example.com/tos`

URI: `https://example.com/login`

Version: 1

Chain ID: 1

Nonce: 32891756

Issued At: 2021-09-30T16:25:24Z

Resources:

- `ipfs://bafybeiemxf5abjwjbikoz4mc3a3dla6ual3jsgpdr4cjr3oz3evfyavhwq/`
- `https://example.com/my-web2-claim.json`



Google Cloud SDK wants to access your Google Account



bob@

This will allow Google Cloud SDK to:

- See, edit, configure and delete your Google Cloud data and see the email address for your Google Account. ⓘ
- View and sign in to your Google Cloud SQL instances ⓘ
- View and manage your Google Compute Engine resources ⓘ
- View and manage your applications deployed on Google App Engine ⓘ

Make sure that you trust Google Cloud SDK

You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

See Google Cloud SDK's privacy policy and Terms of Service.

Cancel

Allow

 Sign in with Ethereum

OpenSea wants to access your Ethereum Account

 pedrogomes.eth



Send and Receive NFT assets



Pay with ETH, USDC or DEGEN



Create and bid to NFT auctions



Make sure you trust OpenSea

Learn about how OpenSea will sign on the behalf of your Ethereum account by reviewing the permissions and policies being granted with this signature. You can always see or remove access to your [Ethereum Account](#) from your wallet.

[Learn about the risks](#)

Cancel

Allow

Connect



Sign

CAIP-222

Wallet Authenticate

~~Connect~~



Sign

Is that enough?

What about signing transactions?

Just close your eyes and approve! 😂

Balancing convenience and security

Less (clicks) is more!

Externally
Owned
Account
(EOAs)



Smart
Contract
Account
(SCAs)

External
Account



Smart
Account

Smart Account is deployed by
a Smart Contract

no key = no signature

ERC-1271

Signature Validation Method for Contracts



```
contract ERC1271 {  
  
    bytes4 constant internal MAGICVALUE = 0x1626ba7e;  
  
    function isValidSignature(  
        bytes32 _hash,  
        bytes memory _signature)  
        public  
        view  
        returns (bytes4 magicValue);  
}
```

Account = Signer + Payer + Crypto(graphy)

| | External Account | Smart Account |
|--------|------------------|------------------|
| Signer | Single Signer | Multiple Signers |
| Payer | Signer === Payer | Signer != Payer |
| Crypto | secp256k1 | Any curve |

Blockchain

App

App

Wallet

Wallet

App

App

Wallet

Wallet

Blockchain

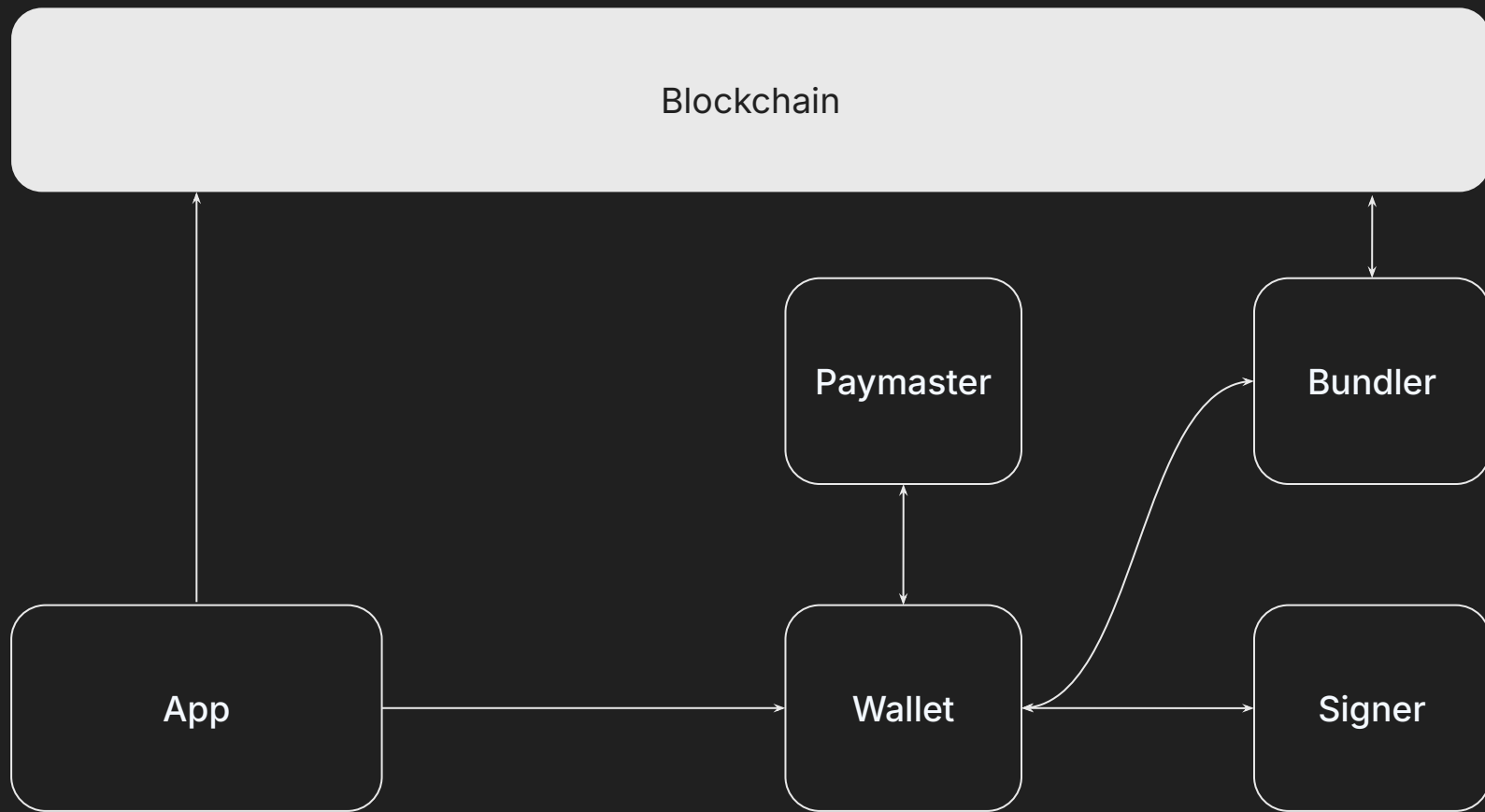
ONE SMART ACCOUNT EVERYWHERE

The diagram features a dark gray background with a grid of rounded rectangular blocks. At the top, a wide, dark gray horizontal bar contains the word 'Blockchain' in a small, light gray font. Below this bar, the central text 'ONE SMART ACCOUNT EVERYWHERE' is displayed in large, white, sans-serif capital letters. The background grid consists of several blocks: four light gray blocks labeled 'App' are arranged in a 2x2 pattern on the left side, and four dark blue blocks labeled 'Wallet' are arranged in a 2x2 pattern on the right side. The text is centered over the intersection of these two groups of blocks.

Account Abstraction

ERC-4337

Account Abstraction Using Alt Mempool



How to discover a Wallet supports
Smart Accounts?

ERC-5792

Wallet Call API Methods

wallet_getCapabilities

wallet_sendCalls

wallet_getCallsStatus

wallet_showCallsStatus

wallet_getCapabilities

wallet_sendCalls

wallet_getCallsStatus

wallet_showCallsStatus


```
[
  {
    "version": "1.0",
    "from": "0xd46e8dd67c5d32be8058bb8eb970870f07244567",
    "calls": [
      {
        "to": "0xd46e8dd67c5d32be8058bb8eb970870f07244567",
        "value": "0x9184e72a",
        "data": "0xd46e8dd67c5d32be8d46e8dd67c5d32be8058bb8eb970870f0724458767c5d32be8058bb8eb",
        "chainId": "0x01",
      },
      {
        "to": "0xd46e8dd67c5d32be8058bb8eb970870f07244567",
        "value": "0x182183",
        "data": "0xfbadbaf01",
        "chainId": "0x01",
      }
    ],
    "capabilities": {
      "paymasterService": {
        "url": "https://..."
      }
    }
  }
]
```

wallet_getCapabilities

wallet_sendCalls

wallet_getCallsStatus

wallet_showCallsStatus



```
// The capabilities below are for illustrative purposes.
```

```
{  
  "0x2105": {  
    "paymasterService": {  
      "supported": true  
    },  
    "sessionKeys": {  
      "supported": true  
    }  
  },  
  "0x14A34": {  
    "paymasterService": {  
      "supported": true  
    }  
  }  
}
```

1. Does this wallet support Paymasters?

2. Which Paymasters does it support?

3. What is the interface for PaymasterData?

ERC-7677

Paymaster Web Service Capability

pm_getPaymasterStubData

```
type GetPaymasterStubDataParams = [
  {
    sender: `0x${string}`;
    nonce: `0x${string}`;
    initCode: `0x${string}`;
    callData: `0x${string}`;
    callGasLimit: `0x${string}`;
    verificationGasLimit: `0x${string}`;
    preVerificationGas: `0x${string}`;
    maxFeePerGas: `0x${string}`;
    maxPriorityFeePerGas: `0x${string}`;
  }, // userOp
  `0x${string}`, // Entrypoint
  `0x${string}`, // Chain ID
  Record<string, any> // Context
];
```

pm_getPaymasterData

```
type GetPaymasterDataParams = [
  {
    sender: `0x${string}`;
    nonce: `0x${string}`;
    initCode: `0x${string}`;
    callData: `0x${string}`;
    callGasLimit: `0x${string}`;
    verificationGasLimit: `0x${string}`;
    preVerificationGas: `0x${string}`;
    maxFeePerGas: `0x${string}`;
    maxPriorityFeePerGas: `0x${string}`;
    signature: `0x${string}`;
  }, // userOp
  `0x${string}`, // Entrypoint
  `0x${string}`, // Chain ID
  Record<string, any> // Context
];
```

But what
happens if all
Smart Contracts
work differently?

ERC-7579

Minimal Modular Smart Accounts

What if we just signed user
operations in the Dapp?

How are `UserOperations` built before signing?

ERC-XXXX

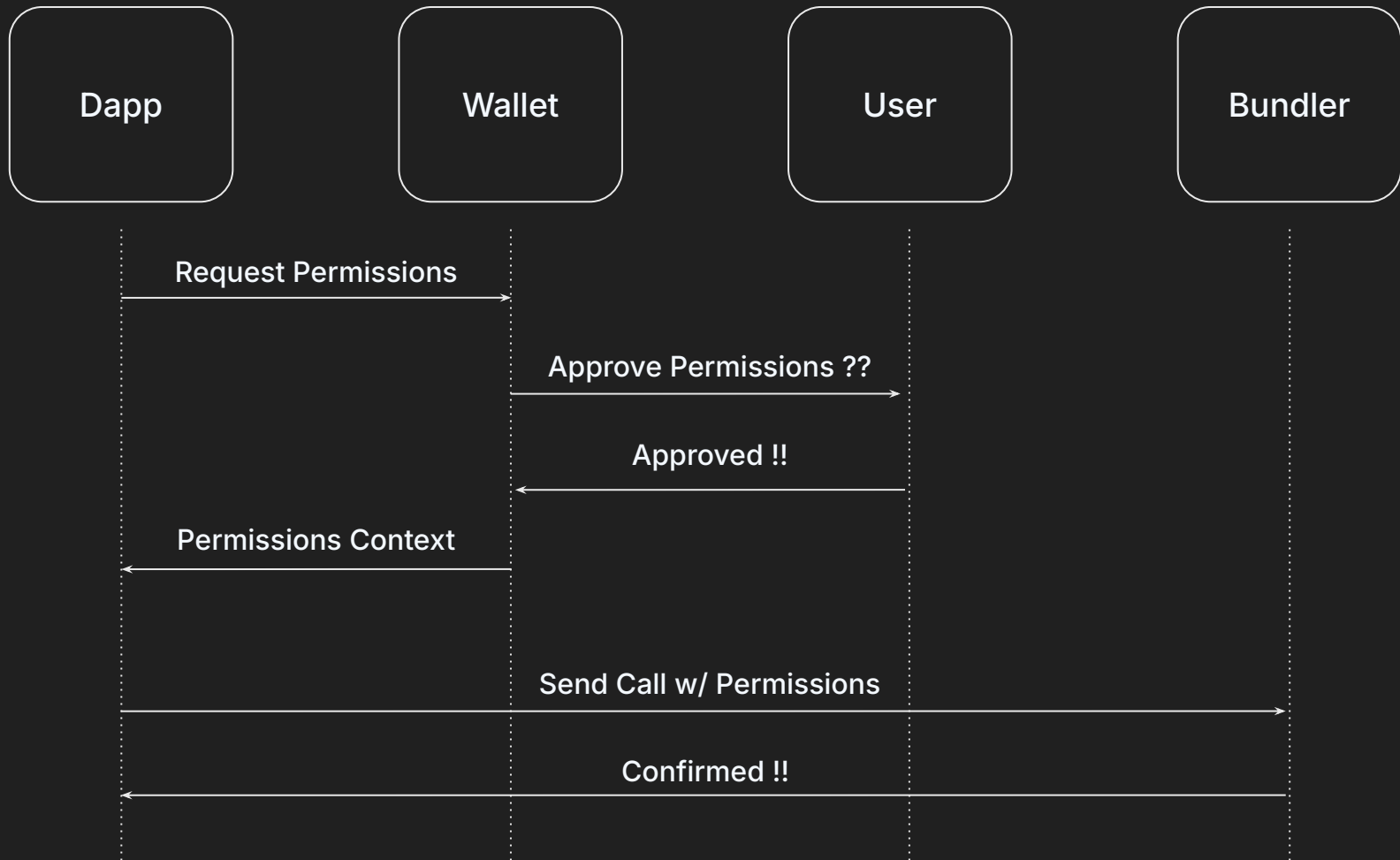
Wallet Prepare Calls API

SMART SESSIONS!

Less (clicks) is more!

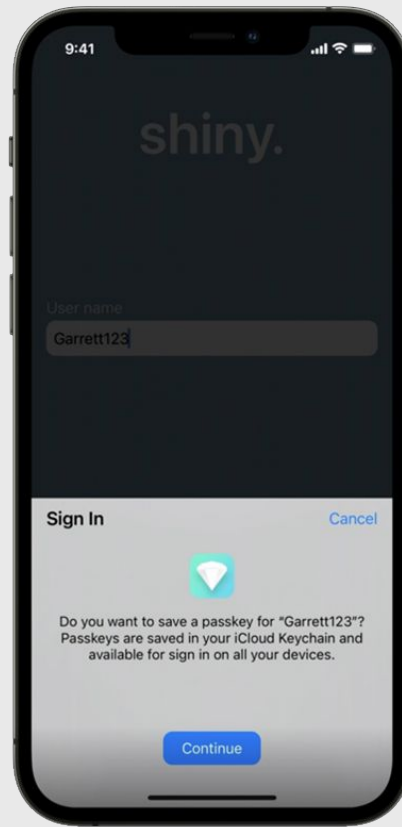
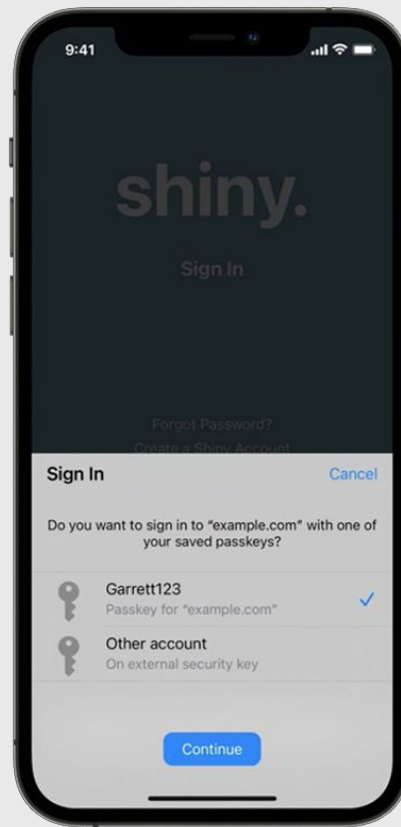
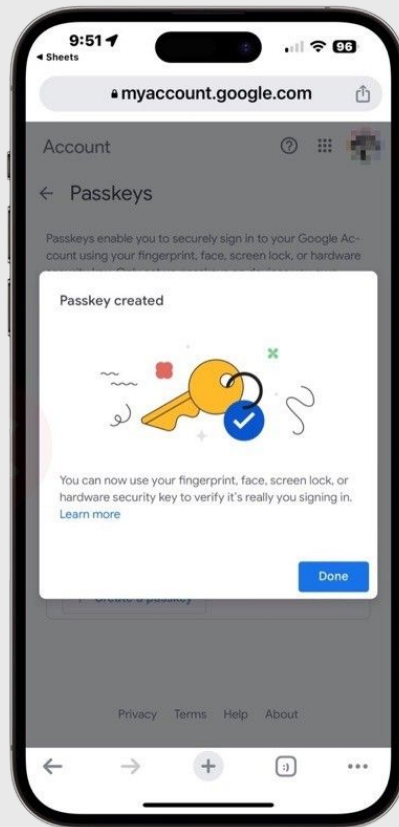
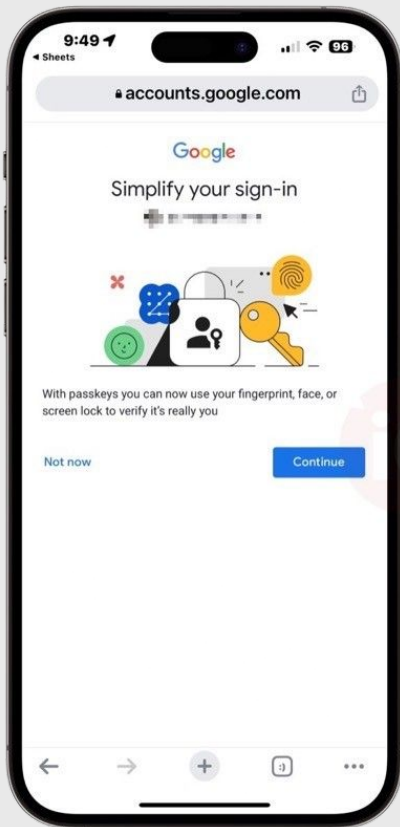
ERC-7715

Grant Permissions from Wallets



Can we secure Smart Sessions better?

PASSKEYS!



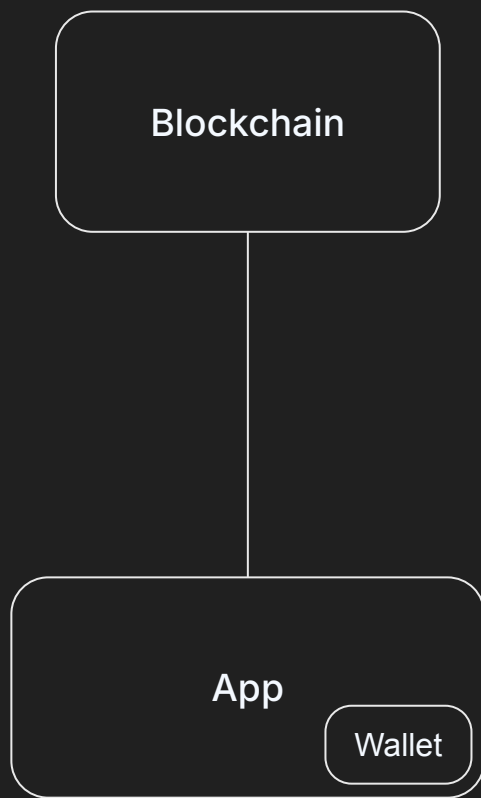
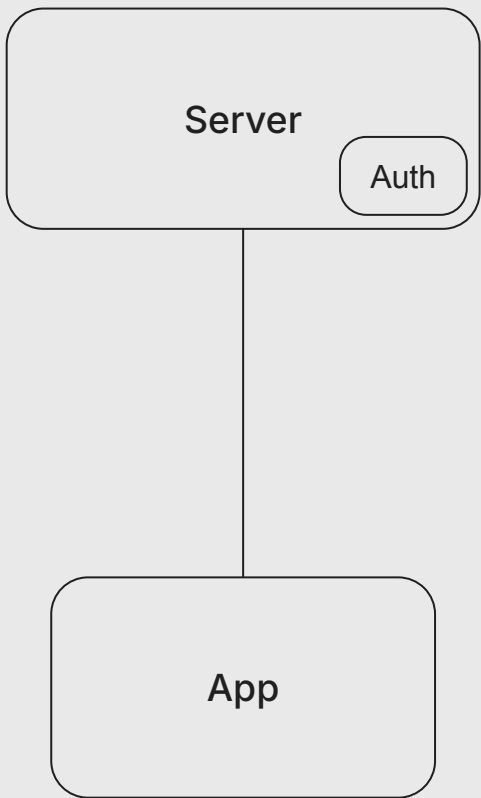
UPGRADE EVM



EIP-7212

Precompile for secp256r1 Curve Support

What is actually being “connected”?



Is this the
end game
for Wallets?

**What if Smart Sessions would
function across all chains?**

Chain Abstraction

**Interoperable Tokens
(ERC-7281 or ERC-7802)**

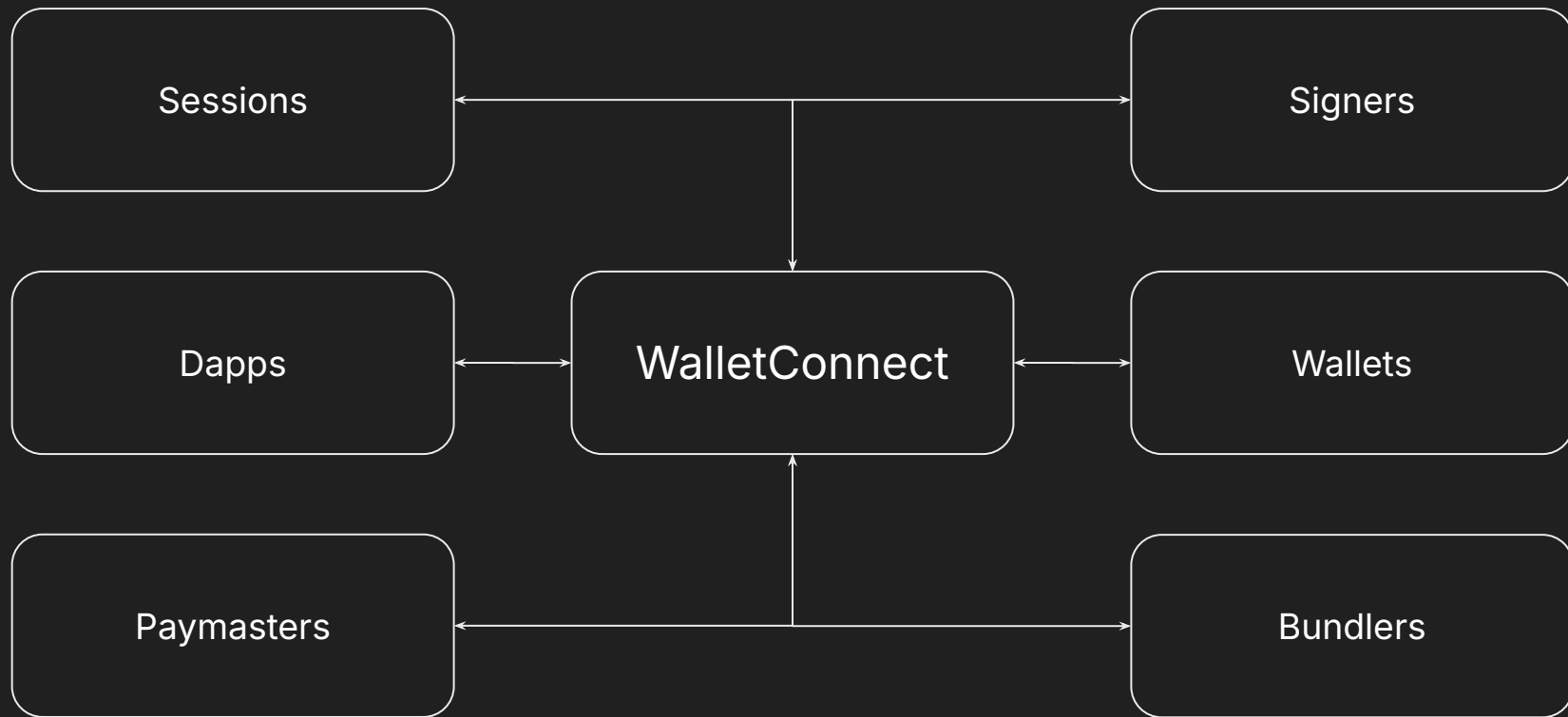
**MagicSpend™ or
Resource Locks**

**EIP-7702
Escrowed Vaults**

**Bridges & Solvers & Bundlers
(liquidity & clearing)**

What is a Wallet in the future?





Redefining the Wallet experience for Web3

Less (clicks) is more!