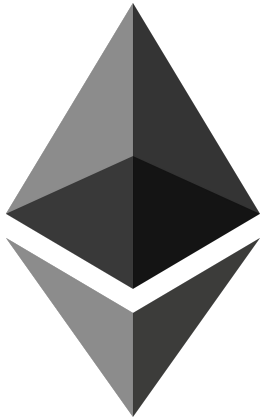
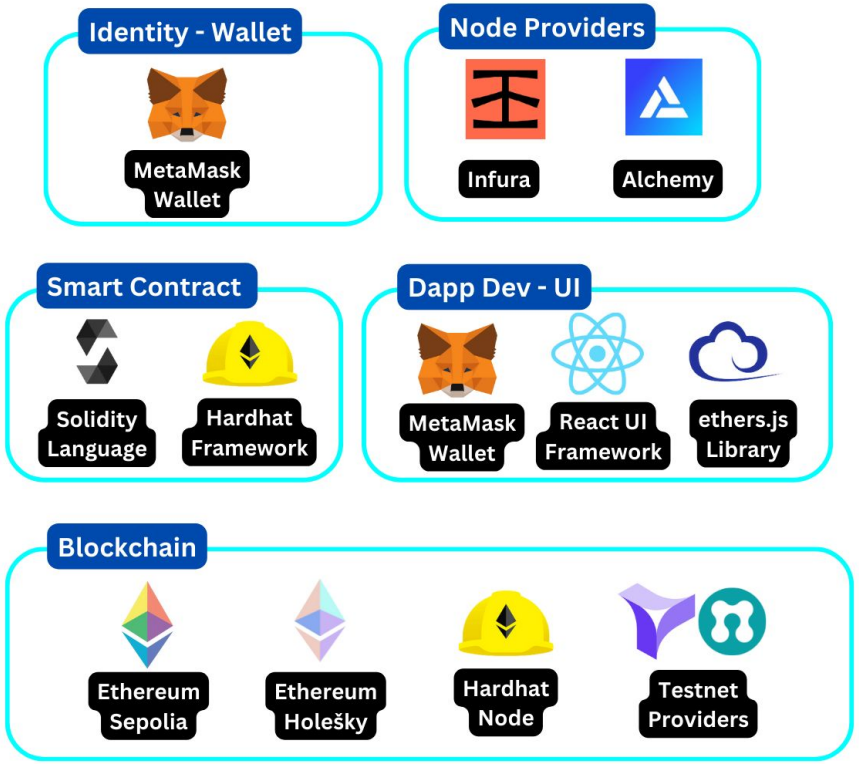
Building with Ethereum



General Dapp Components



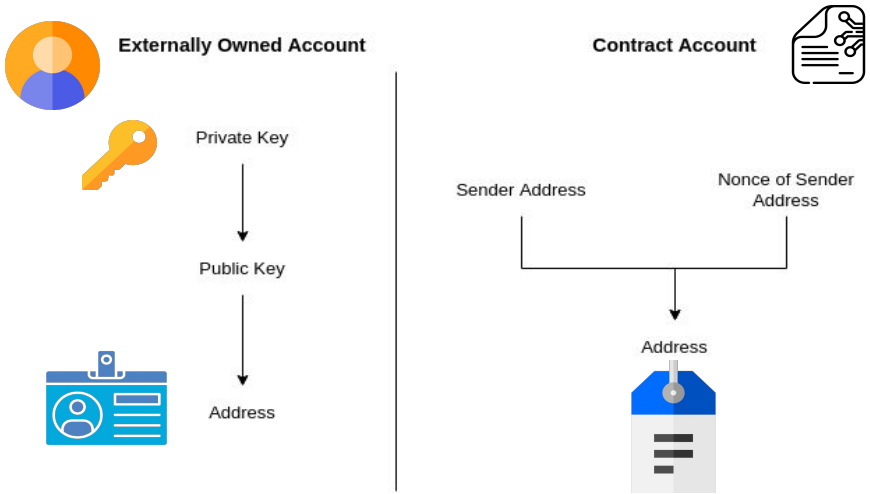
What can we do once we learned it….!

- **Crypto** Trading
  - Algorithmic Trading
- **R**eal **W**orld **A**sset Tokenization
- **Traceability** - **Provenance**
- **Data Analytics**

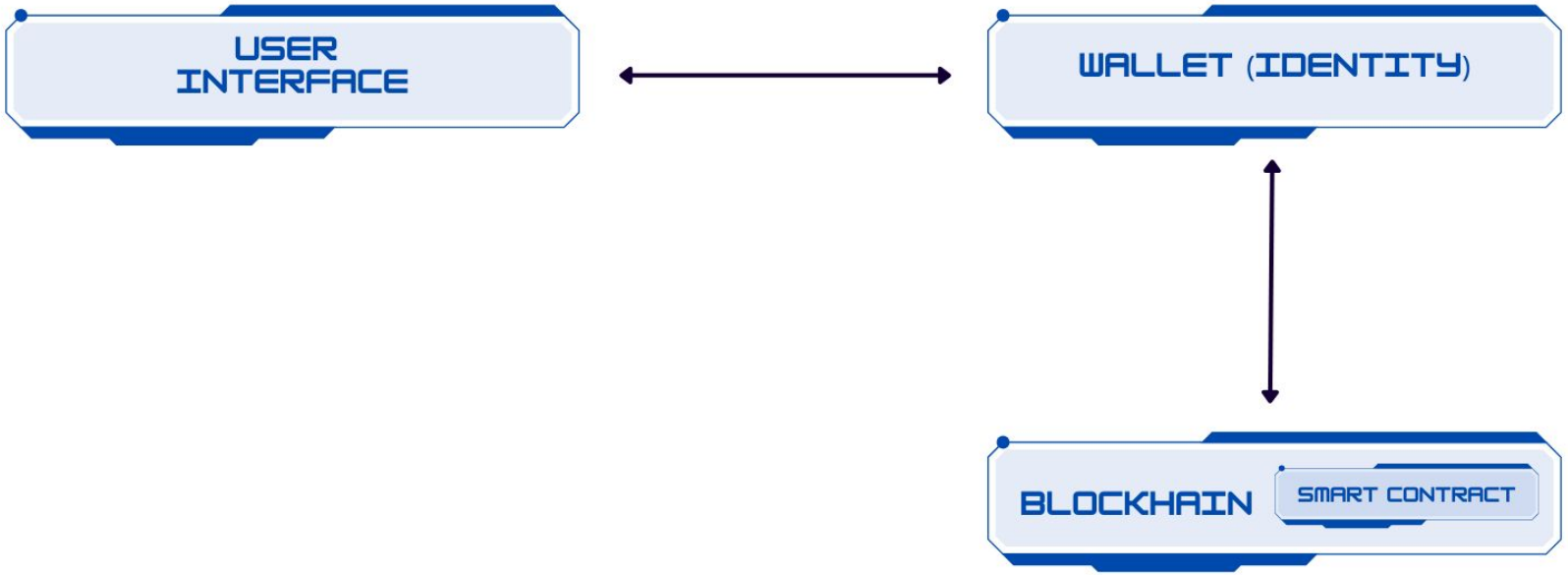
Identity: Accounts

An identity to interact with Ethereum network

0x6eB27Ca7727b7B57dE81df53b27B87b319c94E52



General DApp Architecture



Smart Contracts - Deployment & Interaction

Smart Contracts are used to define how the values are stored into the blockchain

- Analysis of Smart Contract Compilation Output
- Analysis of Contract Deployment Transaction
- Load the contract and interact

```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.20;

contract Storage {

    uint256 number;

    function store(uint256 num) public {
        number = num;
    }

    function retrieve() public view returns (uint256){
        return number;
    }
}
```

```
608060405234801561000f575f80fd5b506101438061001d5f395ff3fe608060405234801561
000f575f80fd5b5060043610610034575f3560e01c80636057361d14610038578063b05784b
814610054575b5f80fd5b610052600480360381019061004d91906100ba565b610072565b0
05b61005c61007b565b60405161006991906100f4565b60405180910390f35b805f81905550
50565b5f8054905090565b5f80fd5b5f819050919050565b6100998161008756 5b81146100a
3575f80fd5b50565b5f813590506100b481610090565b92915050565b5f6020828403121561
00cf576100ce610083565b5b5f6100dc84828501610 0a6565b91505092915050565b6100ee8
1610087565b82525050565b5f602082019050610101075f8301846100e5565b9291505056fea2
64697066735822122 0e8373da02612ef3252b7fb5afeeacd7d01952b550a61f097299504784e
0bff2964736f6c63430008140033
```

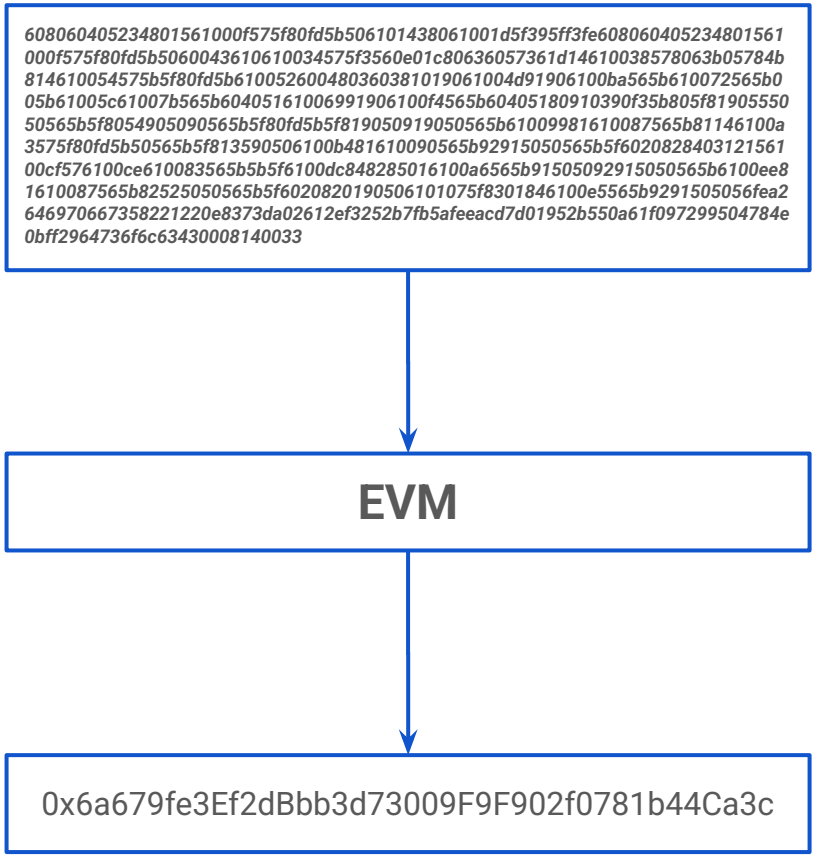
```
[
  {
    "inputs": [],
    "name": "retreive",
    "outputs": [
      {
        "internalType": "uint256",
        "name": "",
        "type": "uint256"
      }
    ],
    "stateMutability": "view",
    "type": "function"
  },
  {
    "inputs": [
      {
        "internalType": "uint256",
        "name": "num",
        "type": "uint256"
      }
    ],
    "name": "store",
    "outputs": [],
    "stateMutability": "nonpayable",
    "type": "function"
  }
]
```

```
.code
  PUSH 80                 contract Storage {\n\n    uint...
  PUSH 40                 contract Storage {\n\n    uint...
  MSTORE                  contract Storage {\n\n    uint...
  CALLVALUE                       contract Storage {\n\n    uint...
  DUP1                    contract Storage {\n\n    uint...
  ISZERO                  contract Storage {\n\n    uint...
  PUSH [tag] 1                    contract Storage {\n\n    uint...
  JUMPI                   contract Storage {\n\n    uint...
  PUSH 0                  contract Storage {\n\n    uint...
  DUP1                    contract Storage {\n\n    uint...
  REVERT                  contract Storage {\n\n    uint...
tag 1                     contract Storage {\n\n    uint...
  JUMPDEST                        contract Storage {\n\n    uint...
  POP                     contract Storage {\n\n    uint...
.....................
```

Bytecode

ABI

Assembly Code


6080604052348015610000f575f80fd5b506101438061001d5f395ff3fe608060405234801561000f575f80fd5b50600436106100345760e01c80636057361d14610038578063b05784b8146100545760e5b5f80fd5b6100526004803603810190610004d91906100ba565b610072565b005b61005c61007b565b6040516100699190610100f4565b6040518091039035b805f81905550565b5f8054905090565b5f80fd5b5f819050919050565b61009981610087565b81146100a3575f80fd5b50565b5f813590506100b481610090565b92915050565b5f60208284031215610100cf576100ce610083565b5b5f6100dc848285016100a6565b91505092915050565b6100ee81610087565b82525050565b5f6020820190506101075f8301846100e5565b9291505056fea26469706673582212208373da02612ef3252b7fb5afeeacd7d01952b550a61f097299504784e0bff2964736f6c63430008140033
Bytecode
EVM
0x6a679fe3Ef2dBbb3d73009F9F902f0781b44Ca3c
Address

We want to call store()

Address

0x6a679fe3Ef2dBbb3d73009F9F902f0781b44Ca3c


```
{
        "inputs": [
                {
                        "internalType": "uint256",
                        "name": "num",
                        "type": "uint256"
                }
        ],
        "name": "store",
        "outputs": [],
        "stateMutability": "nonpayable",
        "type": "function"
}
```


ABI

Create a message call

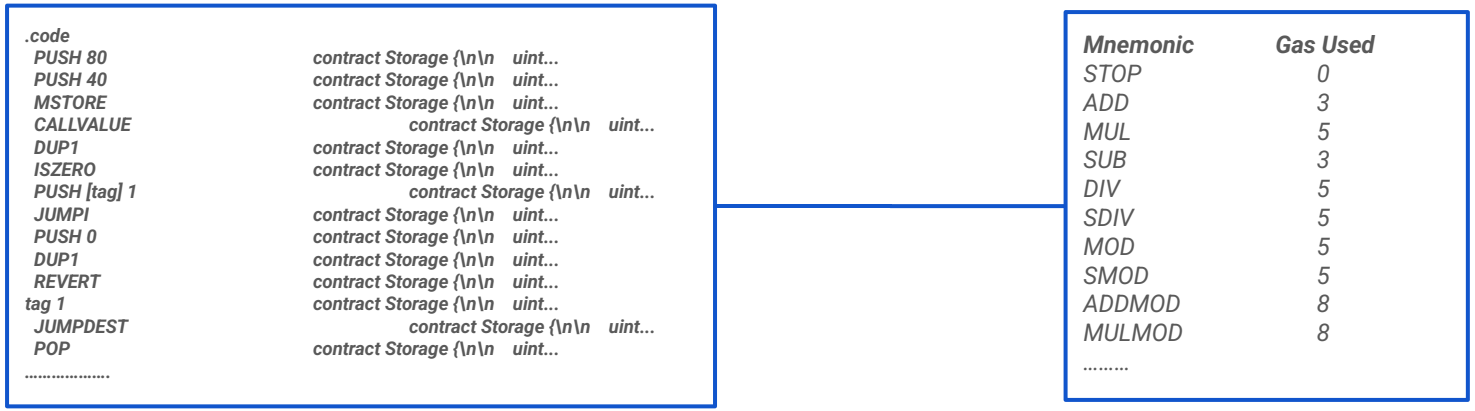
Bytecode


```
608060405234801561000f575f80fd5b506101438061001d5f395ff3fe6080
6040523480156100f575f80fd5b5060043610610034575f3560e01c80636
057361d14610038578063b05784b814610054575b5f80fd5b61005260048
036038101906100d91906100ba565b610072565b005b61005c61007b56
5b604051610069919061100f4565b60405180910390f35b805f8190555050
565b5f8054905090565b5f80fd5b5f819050919050565b610099816100875
65b81146100a3575f80fd5b50565b5f813590506100b481610090565b929
15050565b5f602082840312156100cf576100ce610083565b5b5f6100dc84
8285016100a6565b91505092915050565b6100ee81610087565b8252505
0565b5f602082019050610107f8301846100e5565b9291505056fea2646
97066735822122 0e8373da02612ef3252b7fb5afeeacd7d01952b550a61f0
97299504784e0bff2964736f6c63430008140033
```


EVM

Transaction Hash

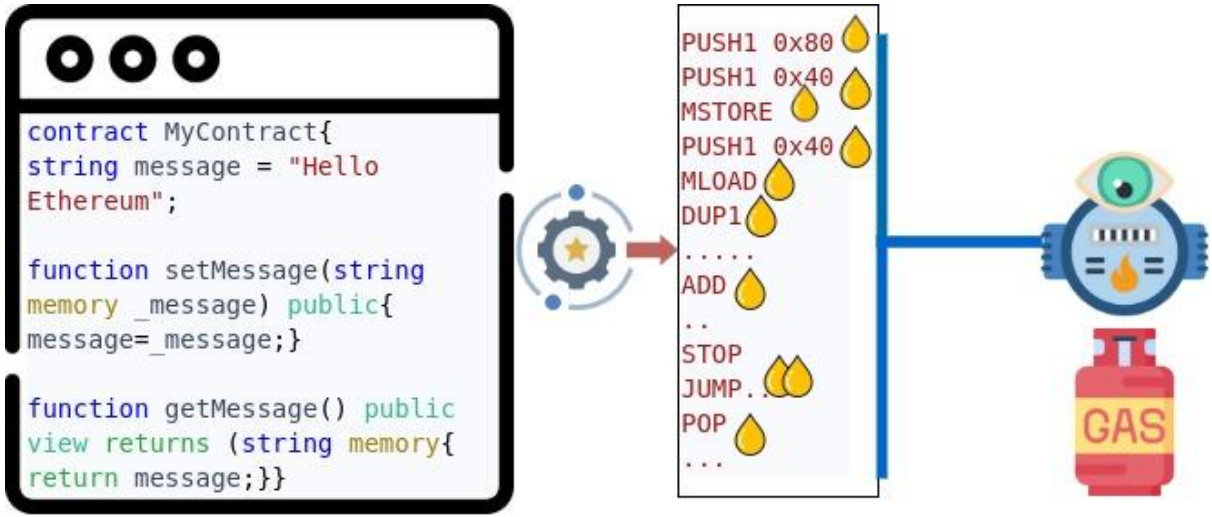
Result



Gas Cost Calculation

Gas

Estimates the amount of computational work required for executing specific operations under the EVM



https://pbs.twimg.com/media/GcsV3t1WoAALgAW?format=jpg&name=4096x4096

Transaction Fee

Gas Limit refers to the maximum measure of gas you are happy to spend on a specific transaction.

Transaction Fee = Gas Limit * (Base fee + Tip)

Smart Contract: Deployment & Interaction

Initial Deployment

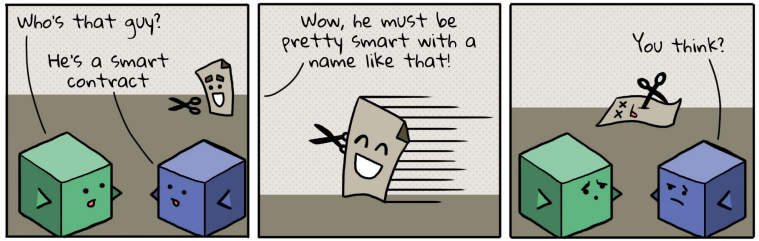
1. Write the Code
2. Compile Contract => Bytecode and ABI
3. Deploy Bytecode to EVM => Address

Interacting with Smart Contract

1. Use ABI to create function call
2. Use address to call deployed contract

Development Phases of Smart Contract + DApp

1. Product roadmap
2. Usability Research
3. Architecture design of the smart contract
4. Development Phase
5. Manual Testing
6. Unit Testing
7. 3rd Party security audit
8. Bug Bounty
9. Final Deployment



Reference

- Ethereum Developer Program Wiki
- Ethereum Developer Program Videos
- Initial Coin Offering (ICO): A Beginner’s Take
- The Story Of An Ethereum Smart Contract | by Kerala Blockchain Academy
- NFTs: How Do They Work?
- DeFi:
  - Decentralized Finance In Three Minutes | by Kerala Blockchain Academy
  - Decentralized Exchanges: A Path of Peer-To-Peer Trading
  - DeFi: Lending and Borrowing

THANKS!

Any questions?