INFINITY
BLOCKCHAIN LABS

Ethereum

for noobs

dApp basic

Hội anh em blockchain "thiện lành"

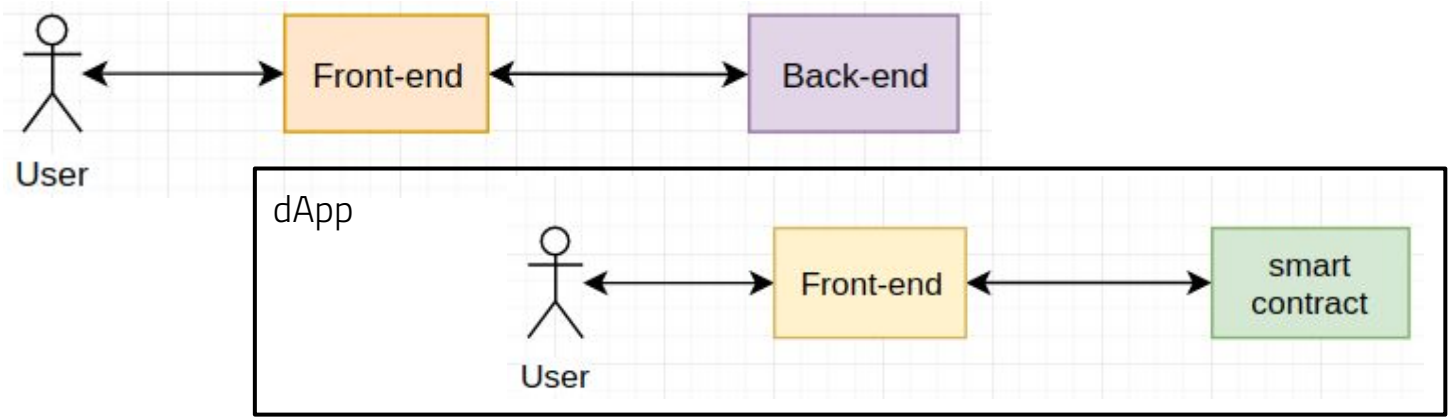
Contents

- DApp definition
- Ethereum transaction's data field
- Interacting with ethereum smart contract
- Example

DApp definition

A decentralized application (dapp, Dapp, dApp or DApp) is a computer application that runs on a distributed computing system.

(https://en.wikipedia.org/wiki/Decentralized_application)



Ethereum transaction

1. **nonce**: Nonce of sender.
2. **to**: The 160-bit address of recipient.
3. **value**: number of Wei to be transferred to recipient.
4. **v, r, s**: Values corresponding to the signature.
5. **data**: An unlimited size byte array specifying the input data of the message call.
6. **gasPrice**: cost of a gas.
7. **gaseLimit**: maximum gas.

(1) + (2) + (3) + (4) + ~~(5)~~ + (6) + (7)
=> Send ETH

A

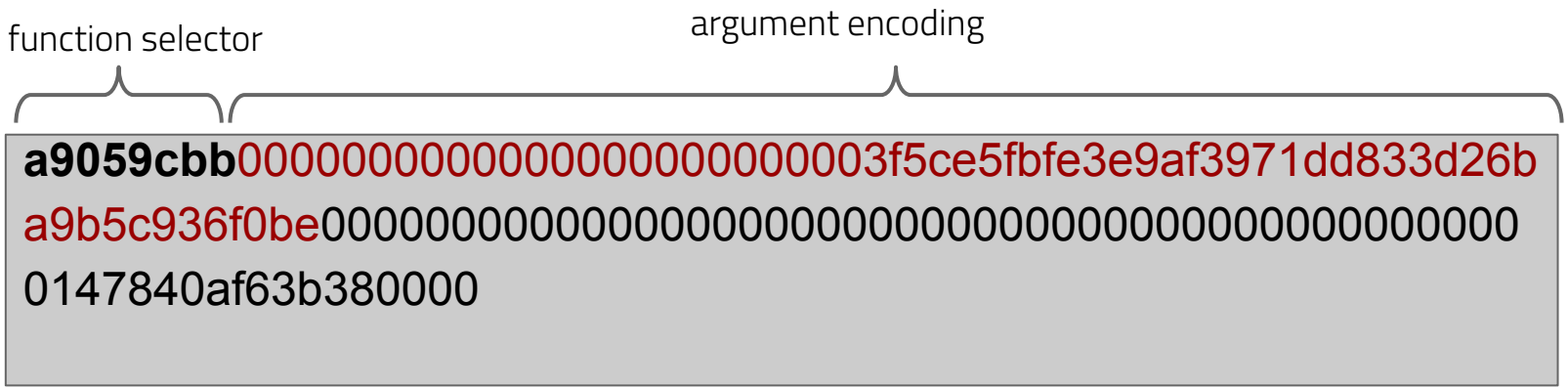
(1) + ~~(2)~~ + (3) + (4) + (5) + (6) + (7)
=> Create new smartcontract

B

(1) + (2) + (3) + (4) + (5) + (6) + (7)
=> Invoke a smartcontract

C

Data field of transaction



- **Function selector** is the first four bytes of the Keccak-256 (SHA-3) hash of the signature of the function.
- **Argument encoding** is the RLP encode of all parameters of the function.

transfer(address,uint256)

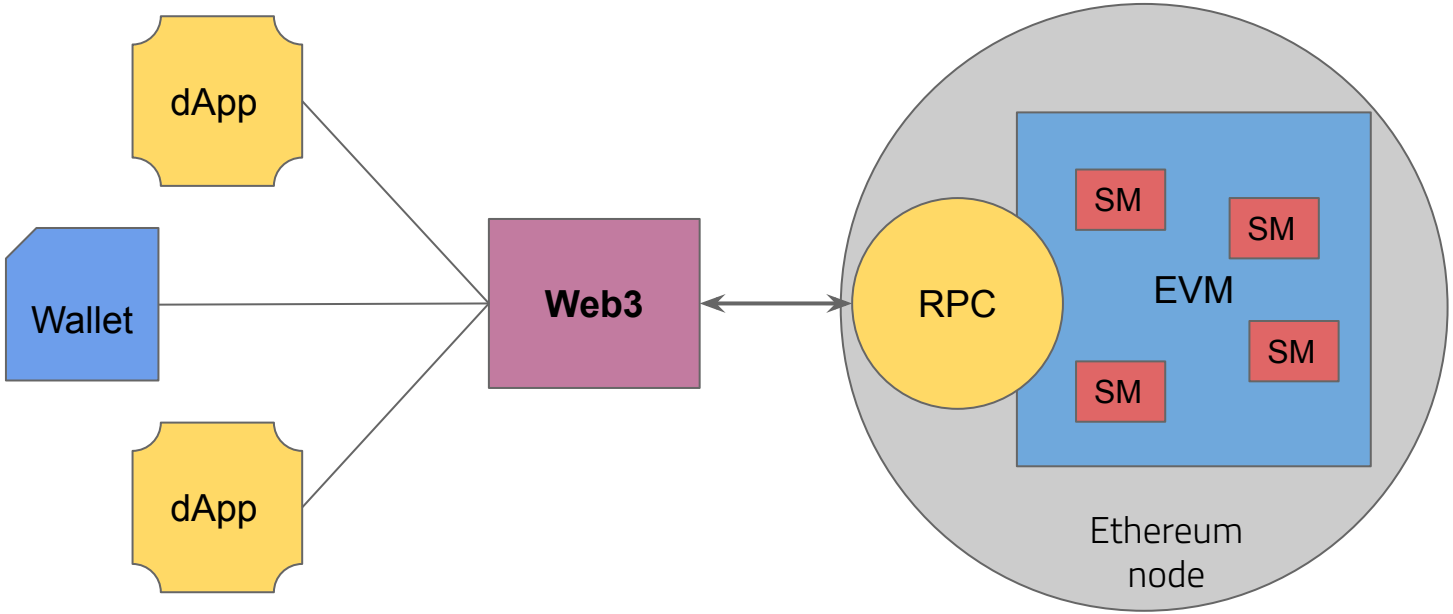
https://github.com/ethereum/wiki/wiki/RLP

Interact with smartcontract

Create transaction:

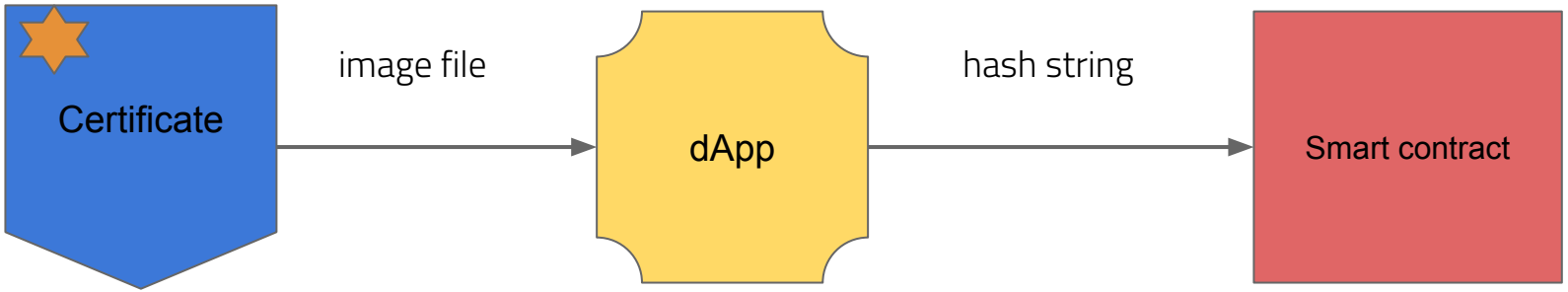
- Desktop -> Metamask, MyEtherwallet
- Mobile -> Infinito wallet
- Your own code -> EthereumJS library

Interact with smartcontract



Example

Create a simple dApp that helps universities or organizations summit their issued certificates to blockchain and let everyone verifies them later.



Source code:
https://github.com/phukq/ethnoob-dapp-basic