Smart Contracts

Setup

- Nothing to install
- Code will come from https://github.com/CryptoSoc/CryptoSocCoin

- And: https://github.com/CryptoSoc/Workshop-2

Smart Contracts

- Actually an old concept (1997)
- Only recently could be realized in a decentralized, trustless manner
- Implemented and run on the blockchain

The Blockchain

Where does this come in?

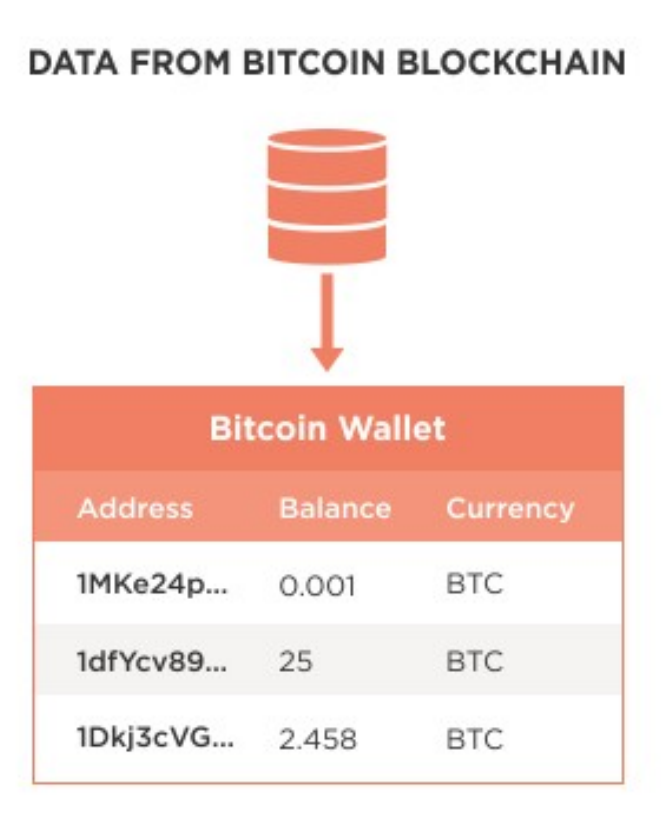
- Enabler of decentralized trust
- Executor of smart contracts

How does it work?

- A distributed ledger.
- A validator
- An executor

As a Consumer

- You submit a transaction to the network
- The transaction is confirmed by the network
- The person you sent it to can verify

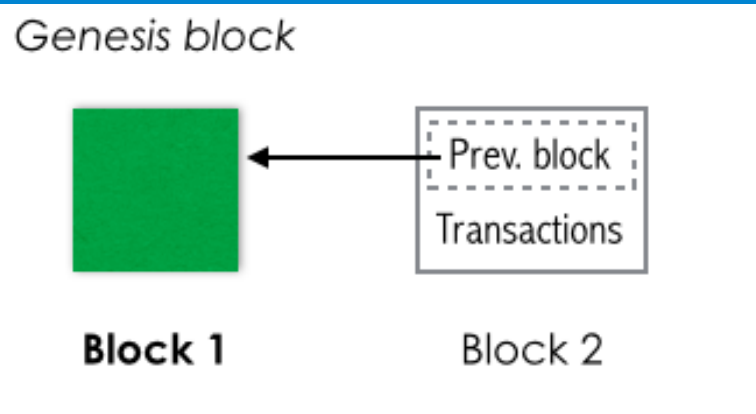


As a Miner/Network

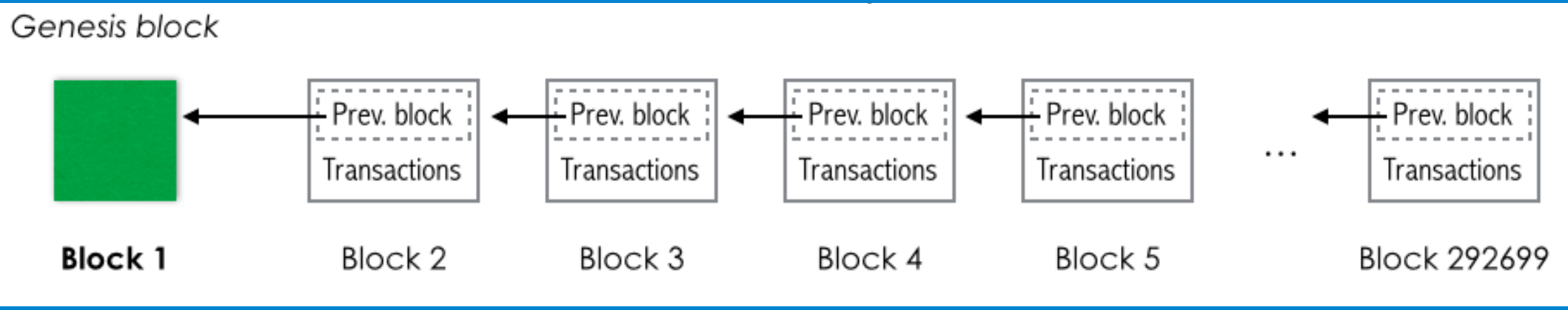
Genesis block

Block 1

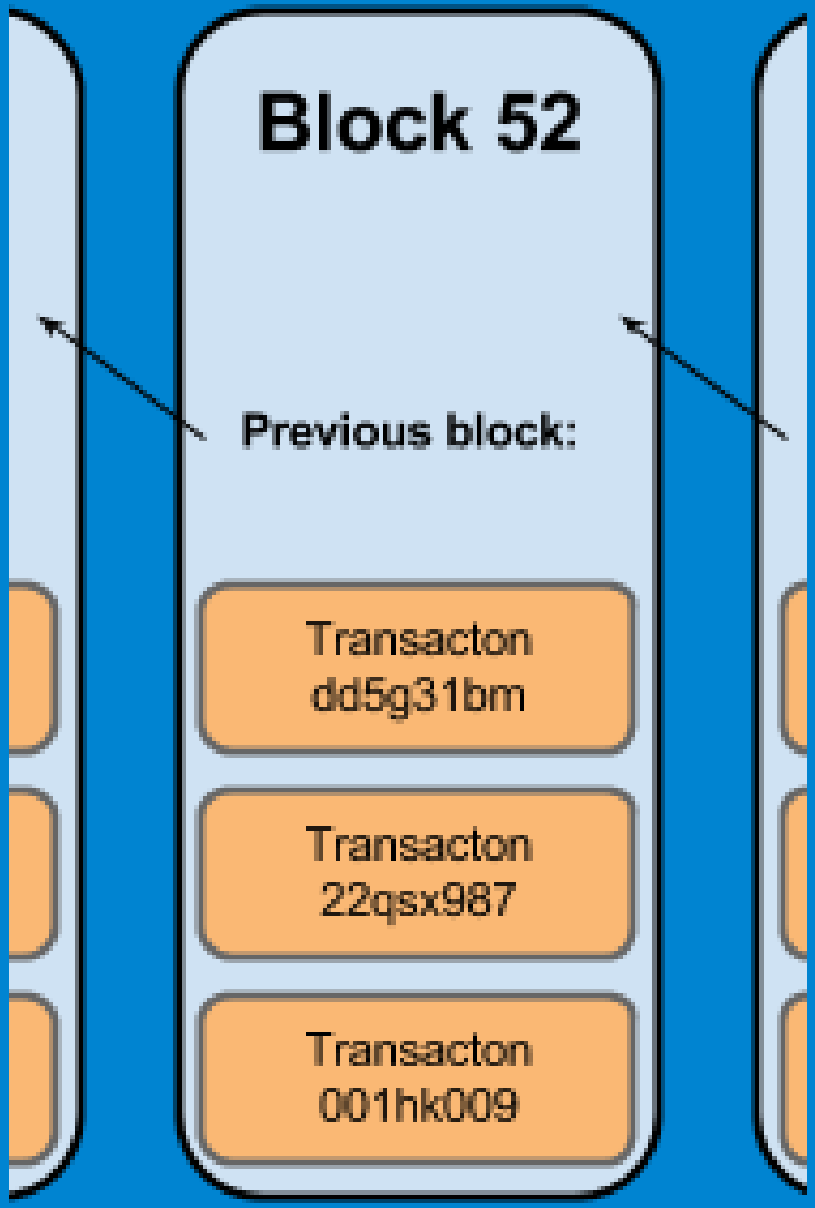
As a Miner



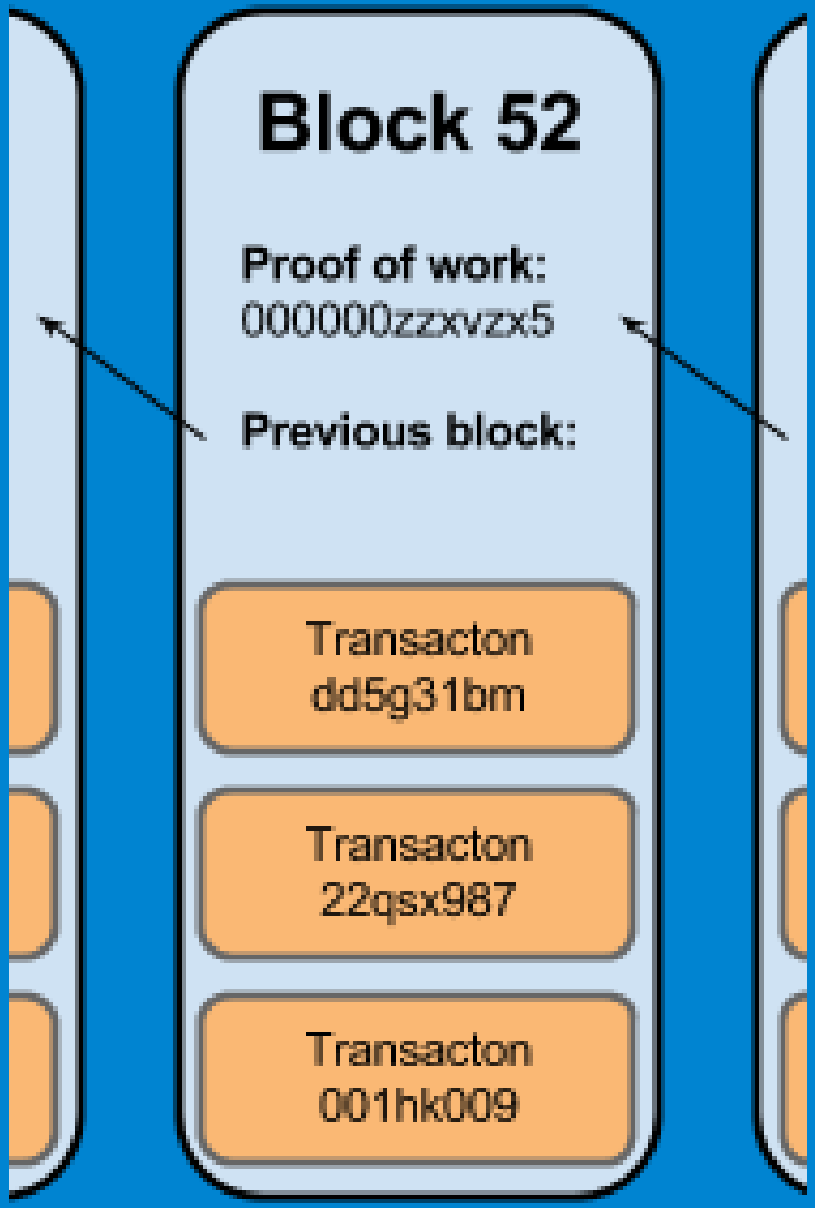
As a Miner


Genesis block
Prev. block
Transactions
Prev. block
Transactions
Prev. block
Transactions
Prev. block
Transactions
...
Prev. block
Transactions
Block 1
Block 2
Block 3
Block 4
Block 5
Block 292699

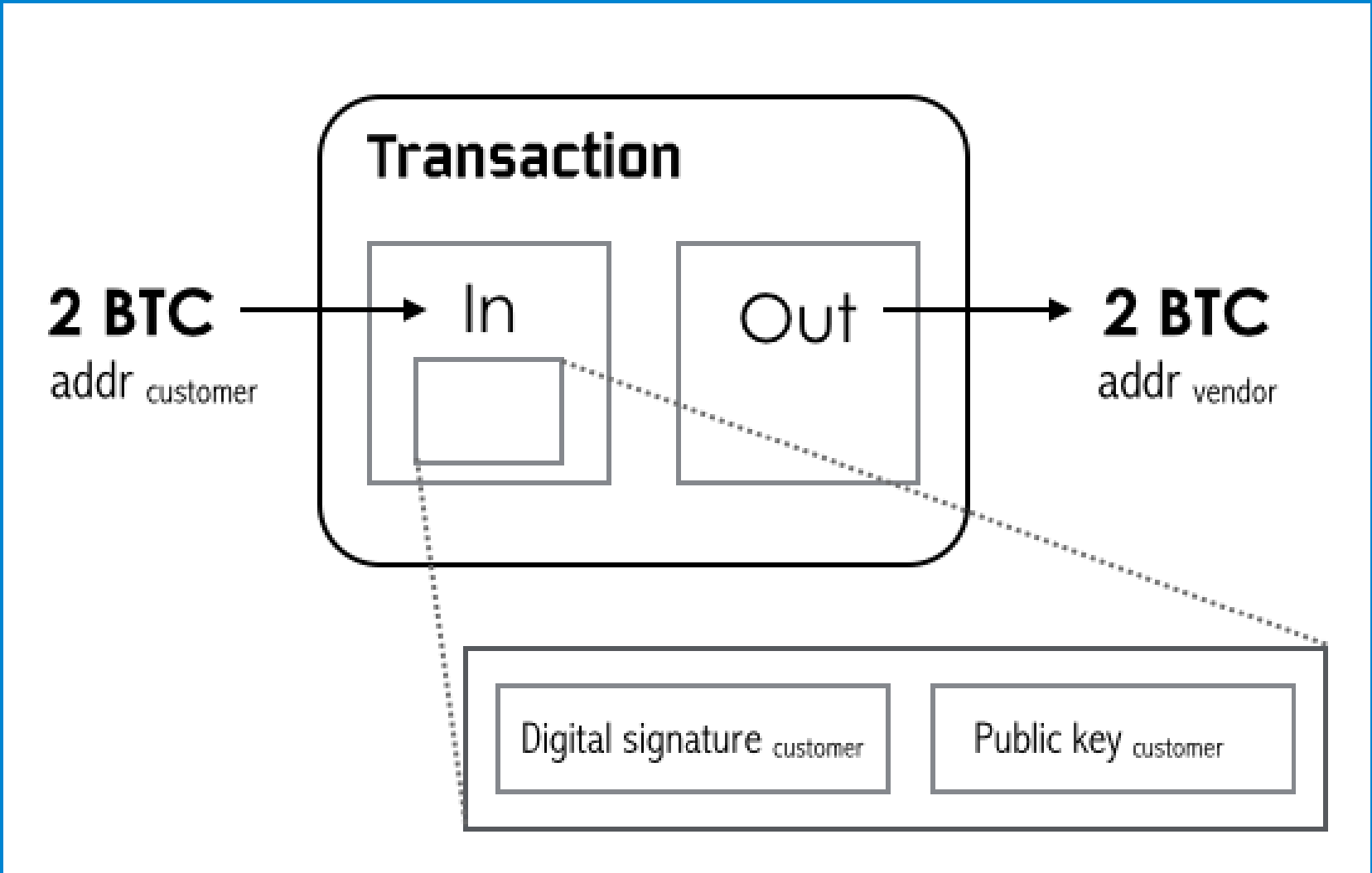
As a Block


Block 52
Previous block:
Transacton
dd5g31bm
Transacton
22qsx987
Transacton
001hk009

As a Block


Block 52
Proof of work:
000000zzxvzx5
Previous block:
Transacton
dd5g31bm
Transacton
22qsx987
Transacton
001hk009

A transaction



You Don’t Own Bitcoin, You Own Unspent Transaction Outputs

Distributed Consensus

- Proof of Work
- Another day

Smart Contracts

- Execute when a pre-programmed condition is triggered
- Execute exactly as programmed

So What Does this All Look Like?

What Does a Smart Contract Actually Look Like?

Solidity

```
contract Example{

  // Transfer tokens to an address

  function transfer(address _to, uint _value) public returns
(bool) {

   // Do something

  }

}
```

Still Plenty can go Wrong

- Security
- Immutability

- E.g. The DAO

Interacting with a Smart Contract

- DApp – Decentralized application

What can they be used for?

- Provide trustless banking
- Apartment leases
- Decentralized cloud computing/storage
- Will and Testament
- Automate insurance payments
- Business contract between partners
- Payments in a mobile game
- CryptoKitties
- …

To the Code!

So you Wanna Create your Own?

- Copy our code and try out the Remix IDE
- Make your own Dapp with “Truffle”: http://truffleframework.com/tutorials/pet-shop
- Learn good smart contract practices from Open Zeppelin
- Read the Docs ⏸

Feedback

- https://goo.gl/oUn6PR
- Any suggestions or comments are welcome.