Blockchain and its application to the brazilian economy

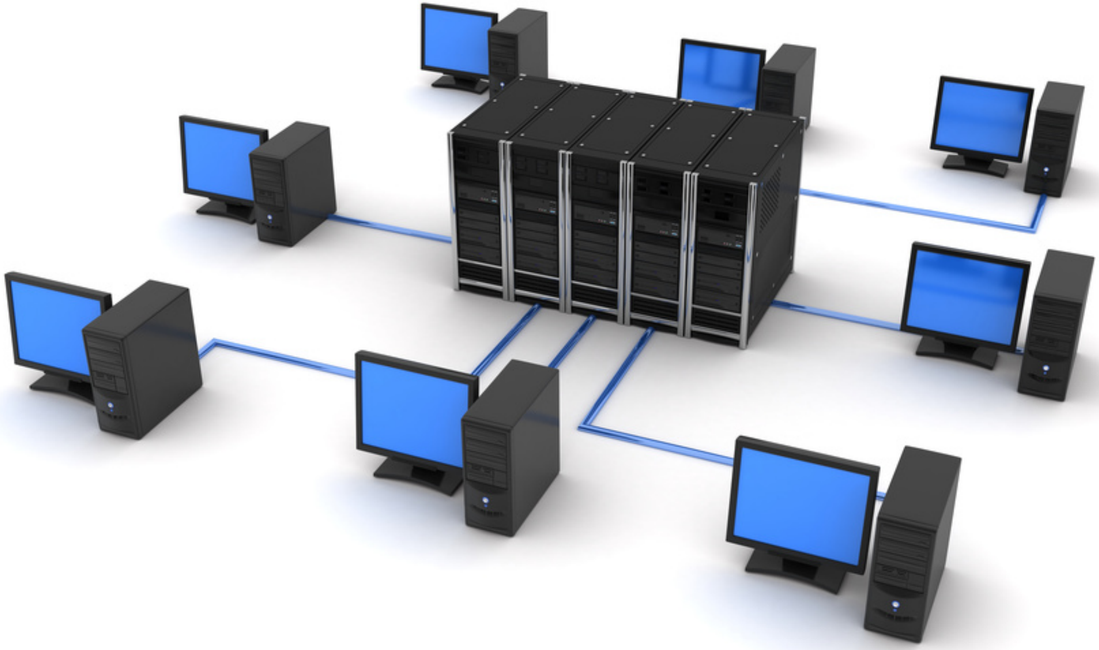
Luiz Pizano Fonseca
Prof. Dr. Paulo André Lima de Castro

Agenda

1. Introduction
   a. Blockchain
   b. Ethereum
   c. Capital market
   d. Objective
2. Programming contracts: solidity
3. Virtual asset exchange
4. Environment setup
   a. installation
   b. private network
   c. mining
5. Conclusions and future work

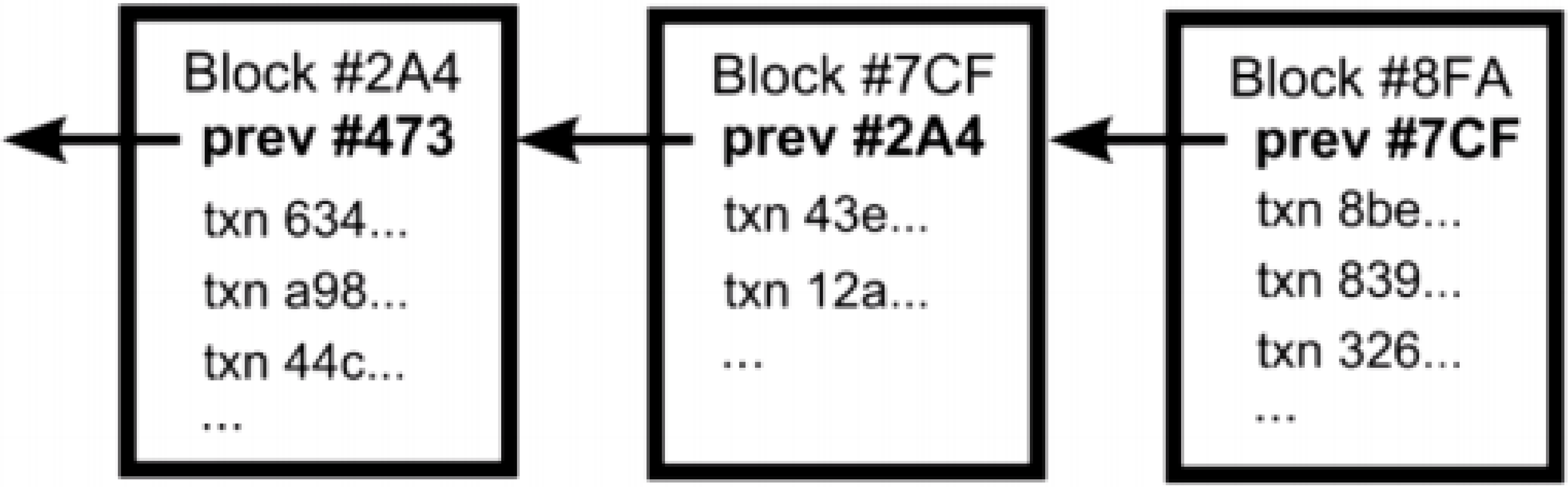
Introduction - Blockchain

Ban

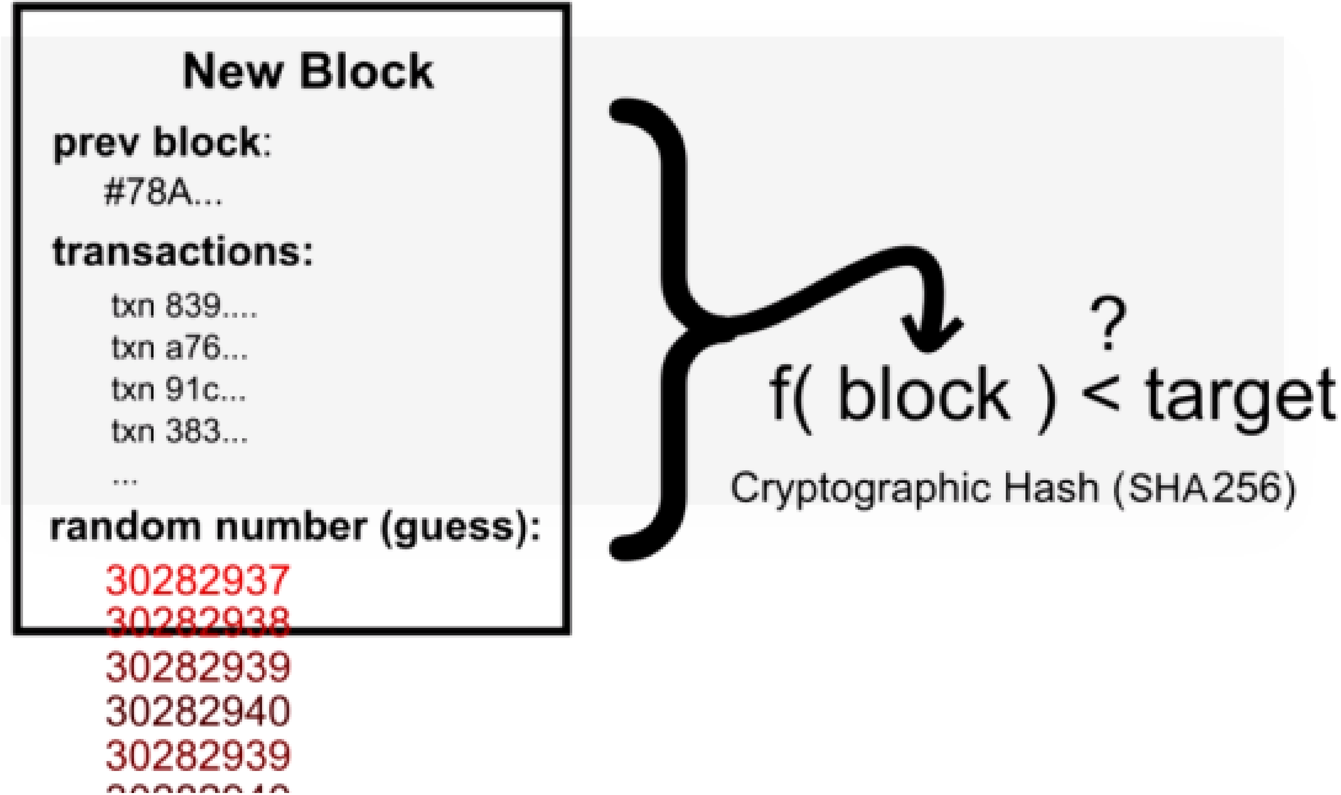


abase

Blockchain and the database decentralization



Blockchain section



New Block

prev block:

#78A...

transactions:

txn 839....
txn a76...
txn 91c...
txn 383...
...

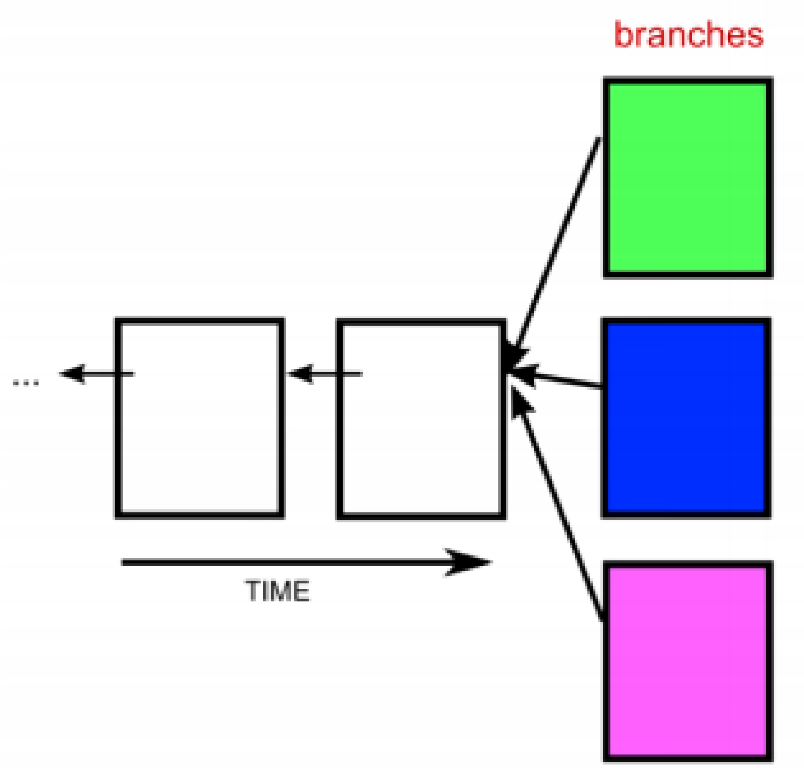
random number (guess):

30282937
30282938
30282939
30282940
30282939

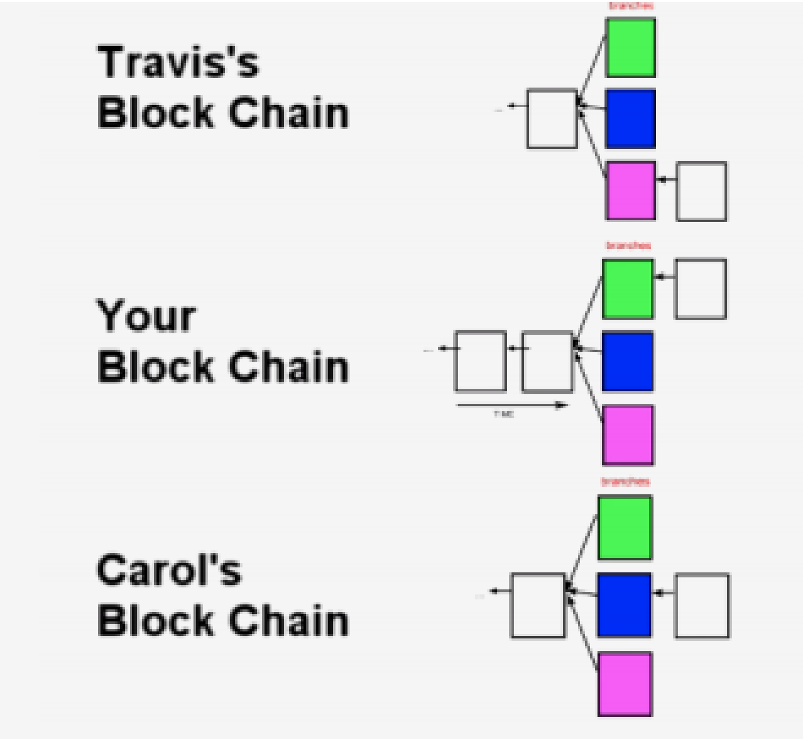
f(block) $\overset{?}{<}$ target

Cryptographic Hash (SHA256)

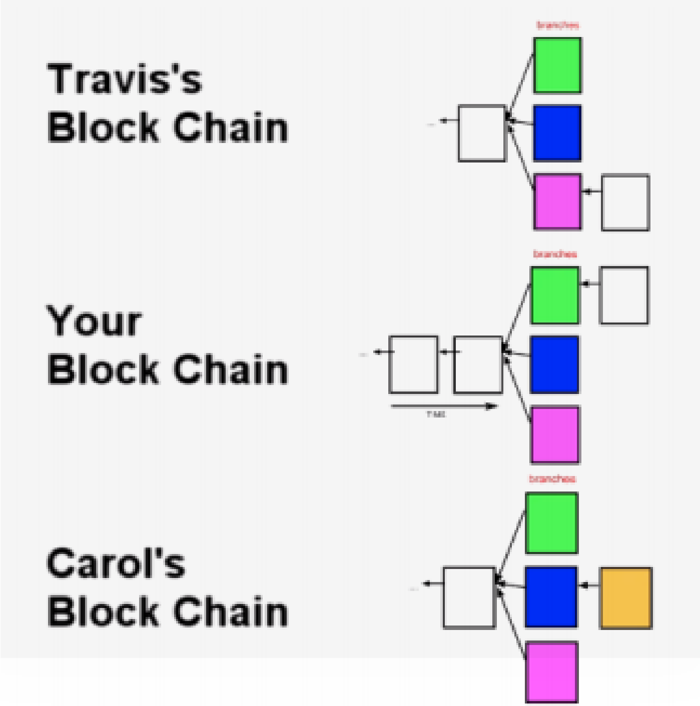
Trying to build a new valid block



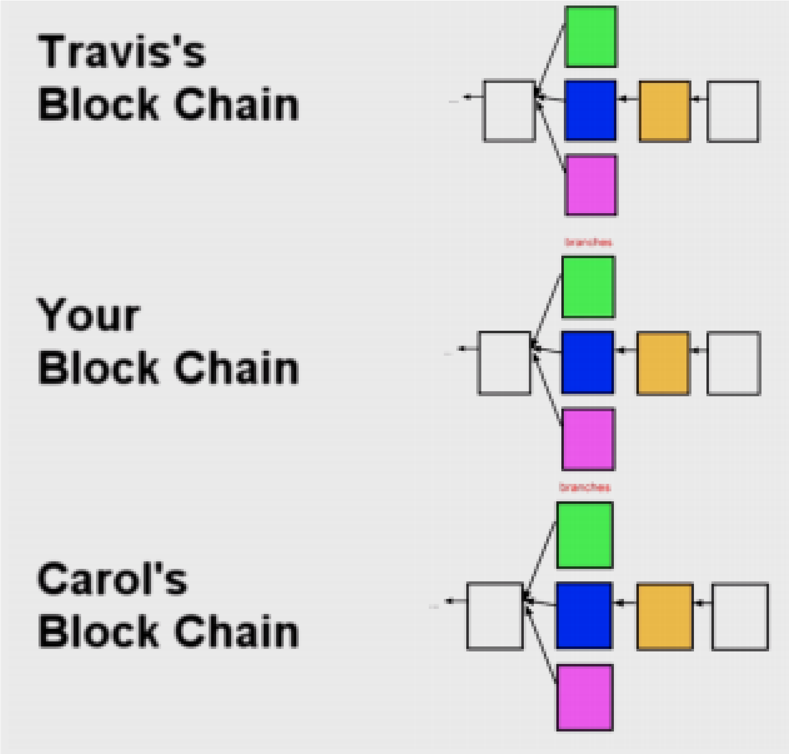
Multiple mined new valid blocks



First received block is different for each node



First node to build a valid block

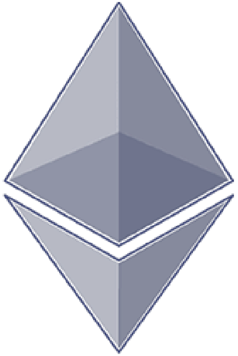


Miners start to mine over the longest ramification

Introduction - Ethereum

- not just decentralize a database, but a whole application
- smart-contracts
- Ethereum

NOKIA
LTE
8:50
Outlook
Cortana
Messaging
Skype
3
Internet Explorer
Quarterly Budget Review
Briefing Room 1940
Tomorrow 10:30-11:30 AM
Calendar
Mon 08
Office
NETFLIX
MixRadio+
London
Mostly Cloudy
20 °C
22°
14°
SSW 11 kmph
100%
Weather

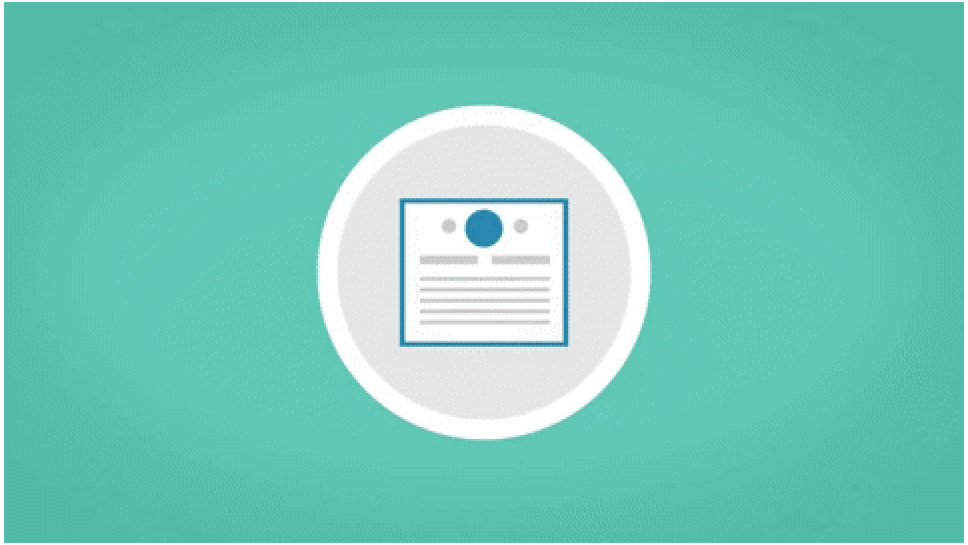


ethereum

“Clearly Ethereum is not about optimising efficiency of computation. Its parallel processing is redundantly parallel. This is to offer an efficient way to reach consensus on the system state without needing trusted third parties”

“With Ethereum, a piece of code could automatically transfer the home ownership to the buyer and the funds to the seller after a deal is agreed upon without needing a third party to execute on their behalf.”

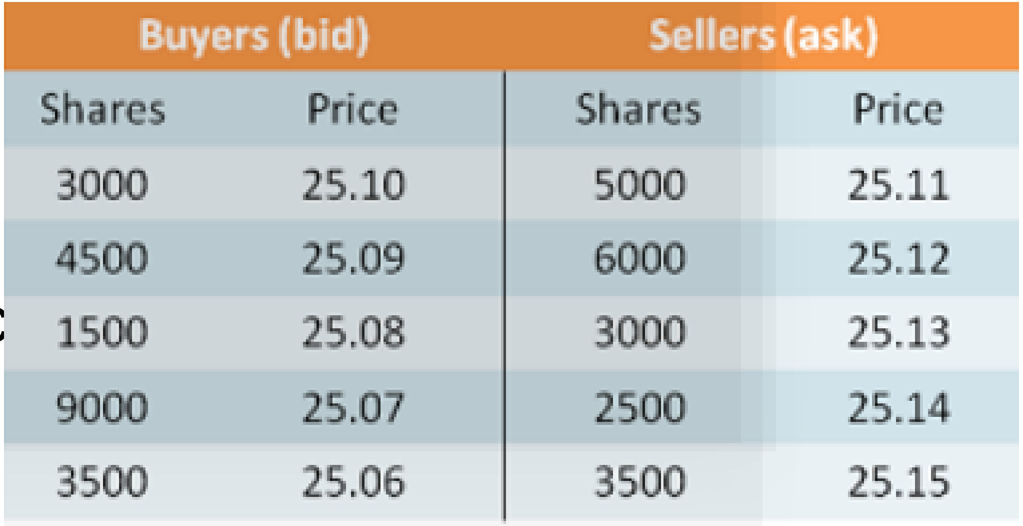
Introduction - capital market



Company Value
1,000,000 $

Introduction - capital market

- buy/sell o
- automatic

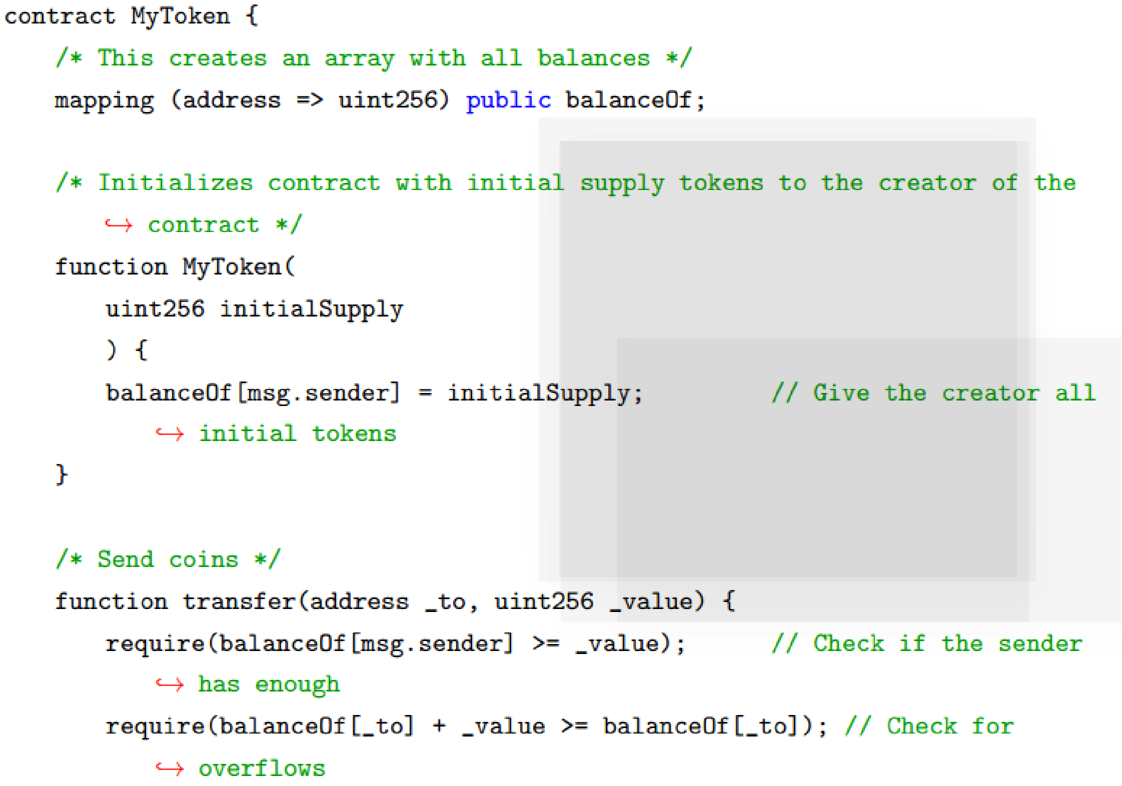


Buyers (bid)		Sellers (ask)	
Shares	Price	Shares	Price
3000	25.10	5000	25.11
4500	25.09	6000	25.12
1500	25.08	3000	25.13
9000	25.07	2500	25.14
3500	25.06	3500	25.15

Introduction - Objective

Implement asset exchange market on Ethereum

Programming contracts: Solidity

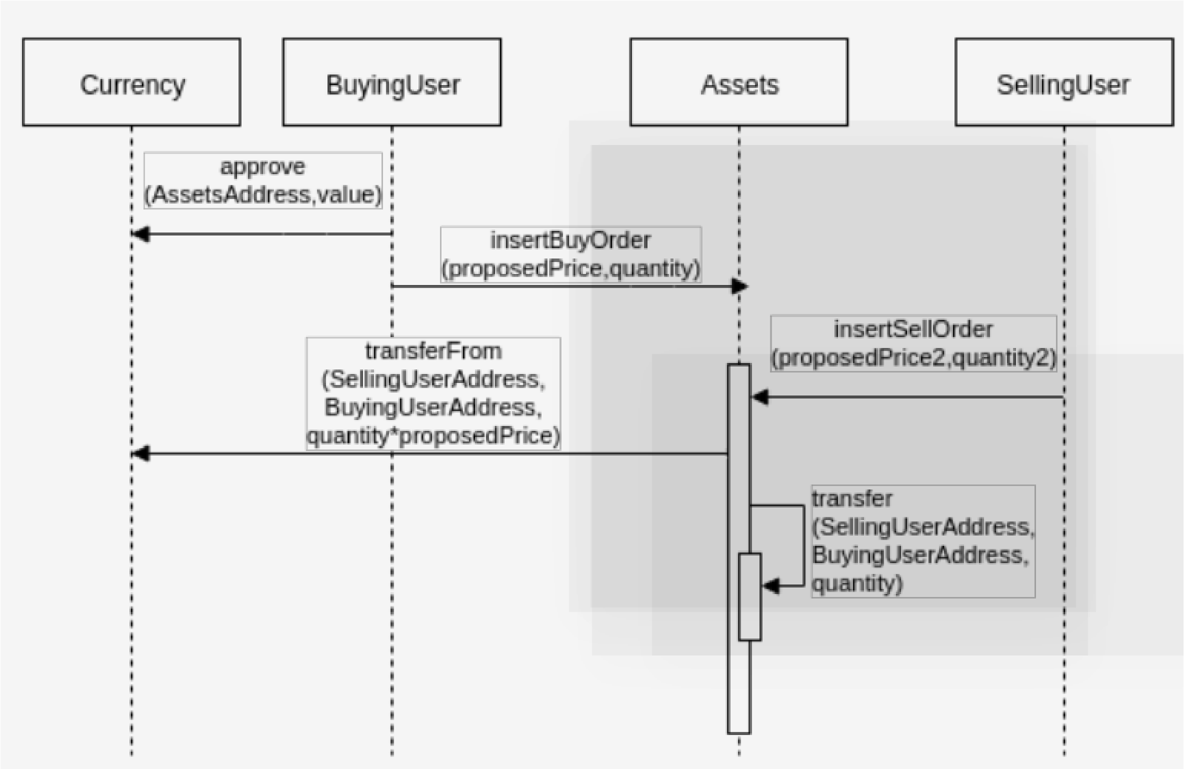


```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the
        ↪ contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;          // Give the creator all
            ↪ initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);      // Check if the sender
            ↪ has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for
            ↪ overflows
```

Virtual asset exchange



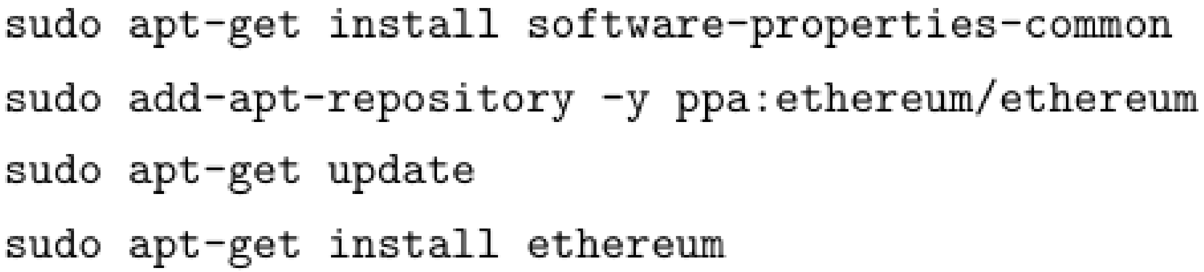
Virtual asset exchange

Watch system usage demonstration

Virtual asset exchange

Watch contract deployment demonstration

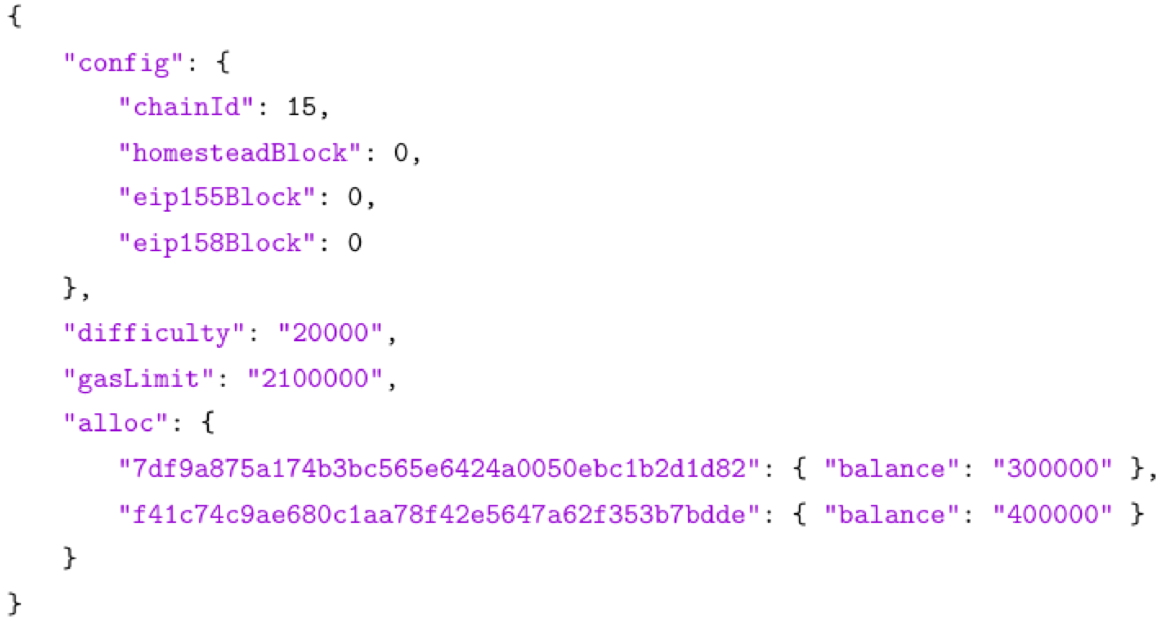
Environment setup: installation



```
sudo apt-get install software-properties-common
sudo add-apt-repository -y ppa:ethereum/ethereum
sudo apt-get update
sudo apt-get install ethereum
```

Ubuntu Geth node installation

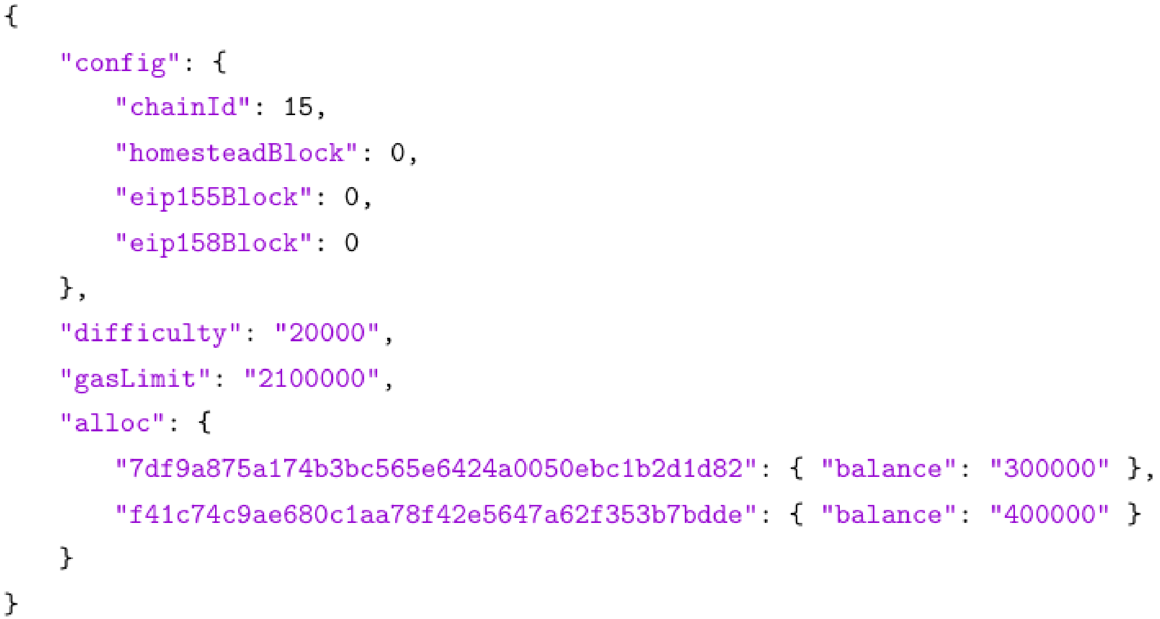
Environment setup: private network



```
{
    "config": {
        "chainId": 15,
        "homesteadBlock": 0,
        "eip155Block": 0,
        "eip158Block": 0
    },
    "difficulty": "20000",
    "gasLimit": "2100000",
    "alloc": {
        "7df9a875a174b3bc565e6424a0050ebc1b2d1d82": { "balance": "300000" },
        "f41c74c9ae680c1aa78f42e5647a62f353b7bdde": { "balance": "400000" }
    }
}
```

Genesis file to create private network

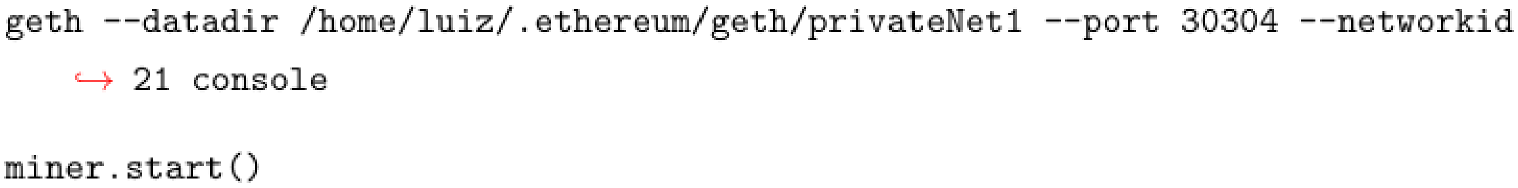
Environment setup: private network



```
{
    "config": {
        "chainId": 15,
        "homesteadBlock": 0,
        "eip155Block": 0,
        "eip158Block": 0
    },
    "difficulty": "20000",
    "gasLimit": "2100000",
    "alloc": {
        "7df9a875a174b3bc565e6424a0050ebc1b2d1d82": { "balance": "300000" },
        "f41c74c9ae680c1aa78f42e5647a62f353b7bdde": { "balance": "400000" }
    }
}
```

Genesis file to create private network

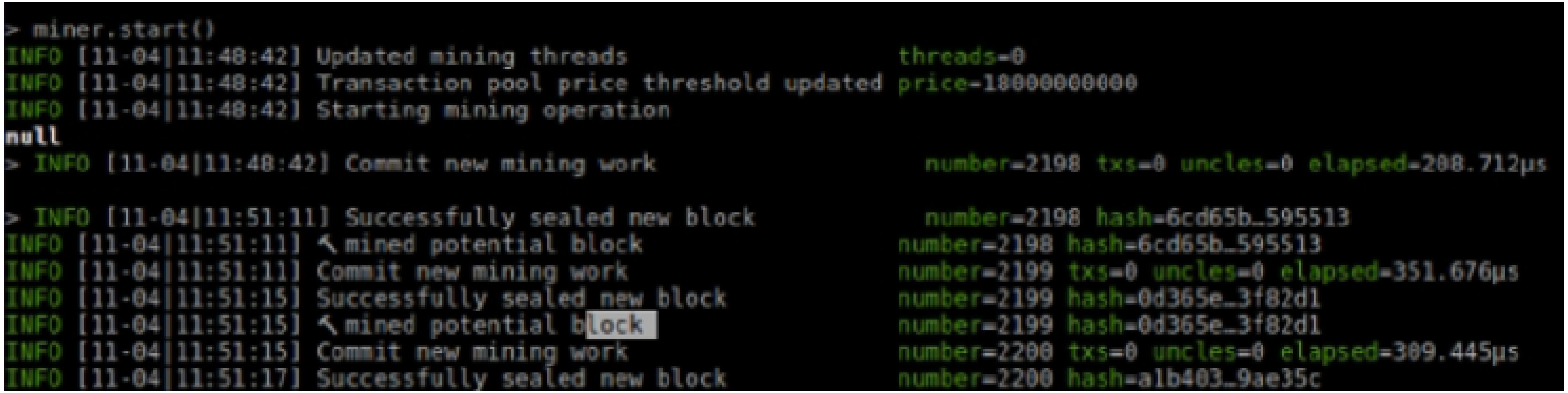
Environment setup: mining



```
geth --datadir /home/luiz/.ethereum/geth/privateNet1 --port 30304 --networkid
    ↪ 21 console

miner.start()
```

Environment setup: mining



```
> miner.start()
INFO [11-04|11:48:42] Updated mining threads                   threads=0
INFO [11-04|11:48:42] Transaction pool price threshold updated price=18000000000
INFO [11-04|11:48:42] Starting mining operation
null
> INFO [11-04|11:48:42] Commit new mining work                   number=2198 txs=0 uncles=0 elapsed=208.712µs

> INFO [11-04|11:51:11] Successfully sealed new block            number=2198 hash=6cd65b…595513
INFO [11-04|11:51:11] 🔨 mined potential block                  number=2198 hash=6cd65b…595513
INFO [11-04|11:51:11] Commit new mining work                   number=2199 txs=0 uncles=0 elapsed=351.676µs
INFO [11-04|11:51:15] Successfully sealed new block            number=2199 hash=0d365e…3f82d1
INFO [11-04|11:51:15] 🔨 mined potential block                  number=2199 hash=0d365e…3f82d1
INFO [11-04|11:51:15] Commit new mining work                   number=2200 txs=0 uncles=0 elapsed=309.445µs
INFO [11-04|11:51:17] Successfully sealed new block            number=2200 hash=a1b403…9ae35c
```

Conclusions and future work

- Implementation succeeded
- Watch Ethereum security along time
- Private network with more than one node communicating