# PX 2018: Blockchain - Endterm Presentation

Johannes Schneider, Julian Weise

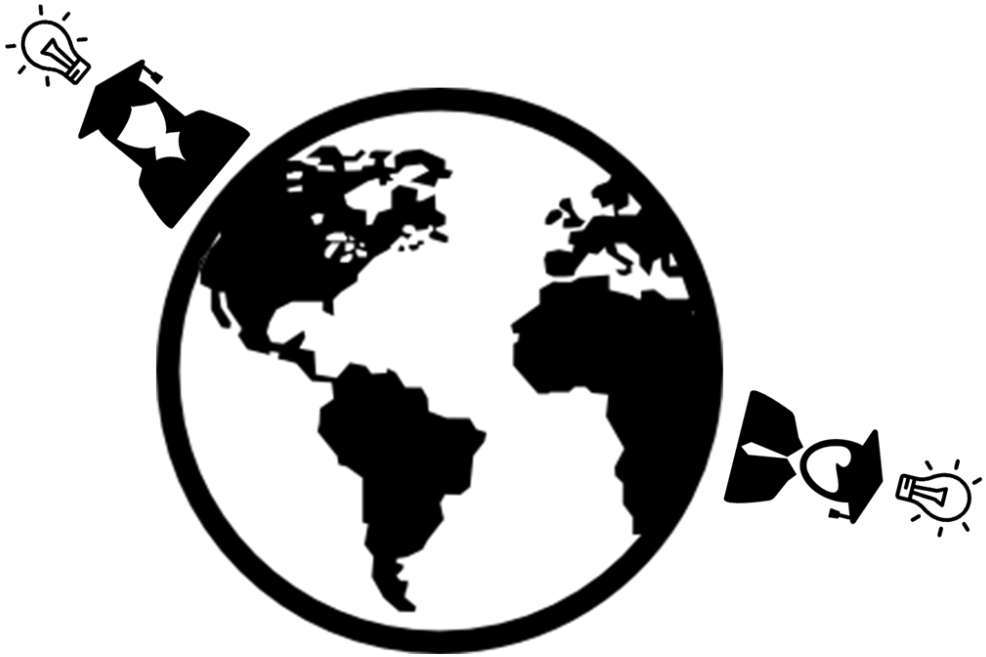
Software Architecture Group
Hasso Plattner Institute
University of Potsdam, Germany

print

# Introduction

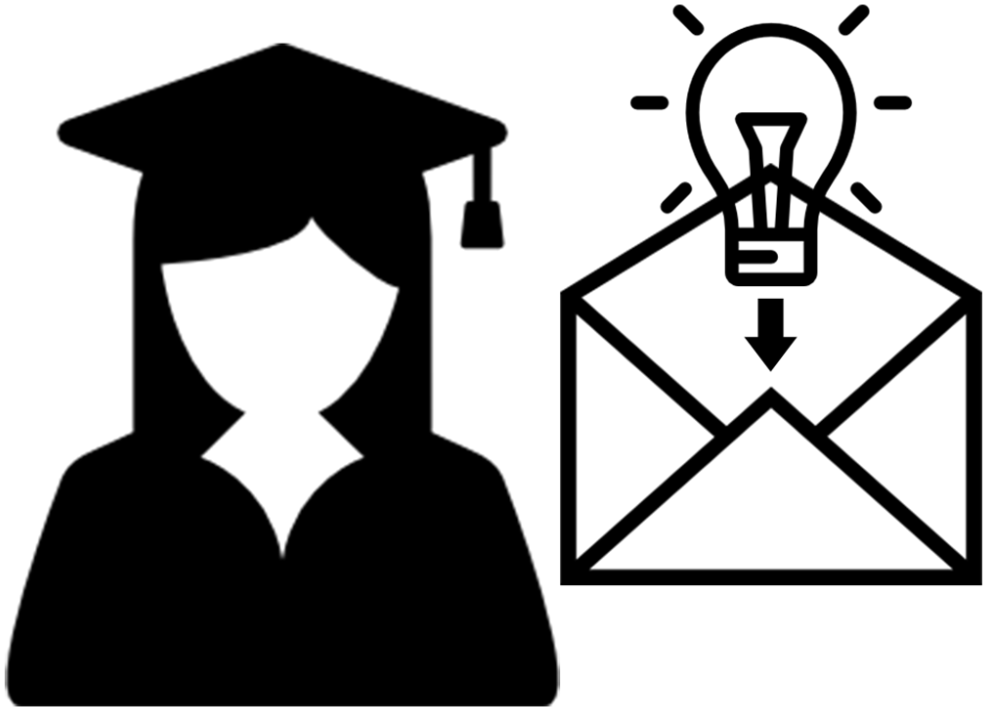
Previous century: researches invented continuously

Icons made by Freepik from www.flaticon.com



Problem: same ideas by multiple researchers

Icons made by Freepik from www.flaticon.com



Solution: write down idea and send to yourself

Icons made by Freepik from www.flaticon.com


Post office clerk will stamp each letter with timestamp

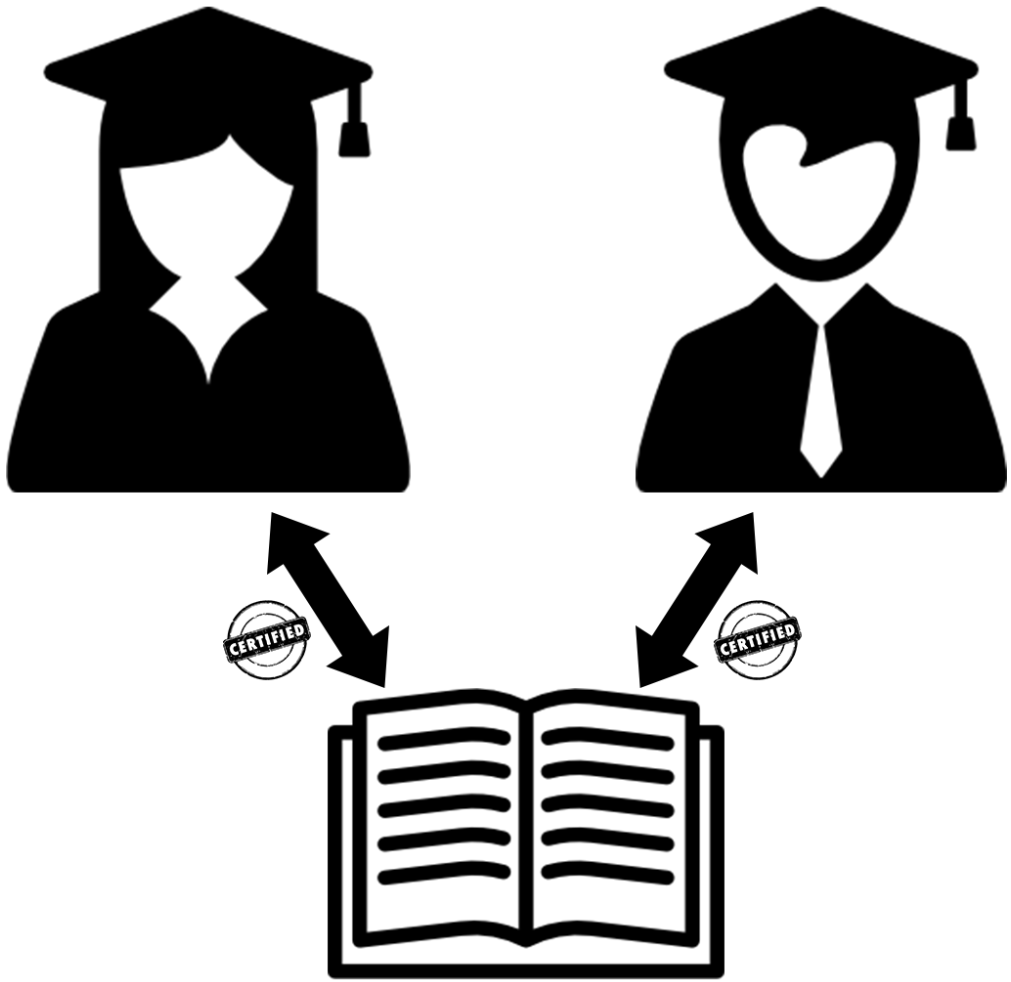
Icons made by Freepik from www.flaticon.com


Researcher has proof for invention at specific point of time

Icons made by Freepik from www.flaticon.com


Problem: Post office clerk might not be reliable

Icons made by Freepik from www.flaticon.com




Idea: Researchers maintain ledger collaboratively

Icons made by Freepik from www.flaticon.com

# Blockchain

"Decentralized, chronological updated database with a network based consensus mechanism for permanent confirmation of ownership."

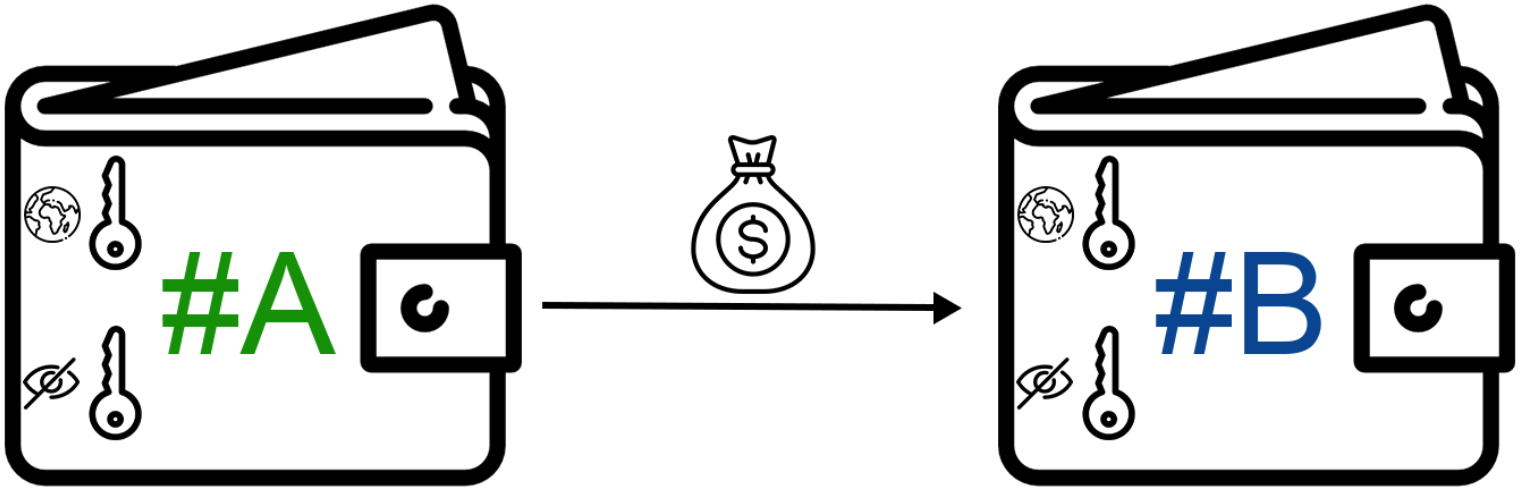
Prof. Dr. Andreas Mitschele

# Bitcoin

- digital crypto currency
  - value skyrocketed from basically $0 (2009) to ~$18.000 (2017)
- concept published by Satoshi Nakamoto (pseudonym) in 2008
  - shared ledger to keep track of all transactions
  - aims to remove necessity of banks to clear transactions
- first stable implementation in 2009

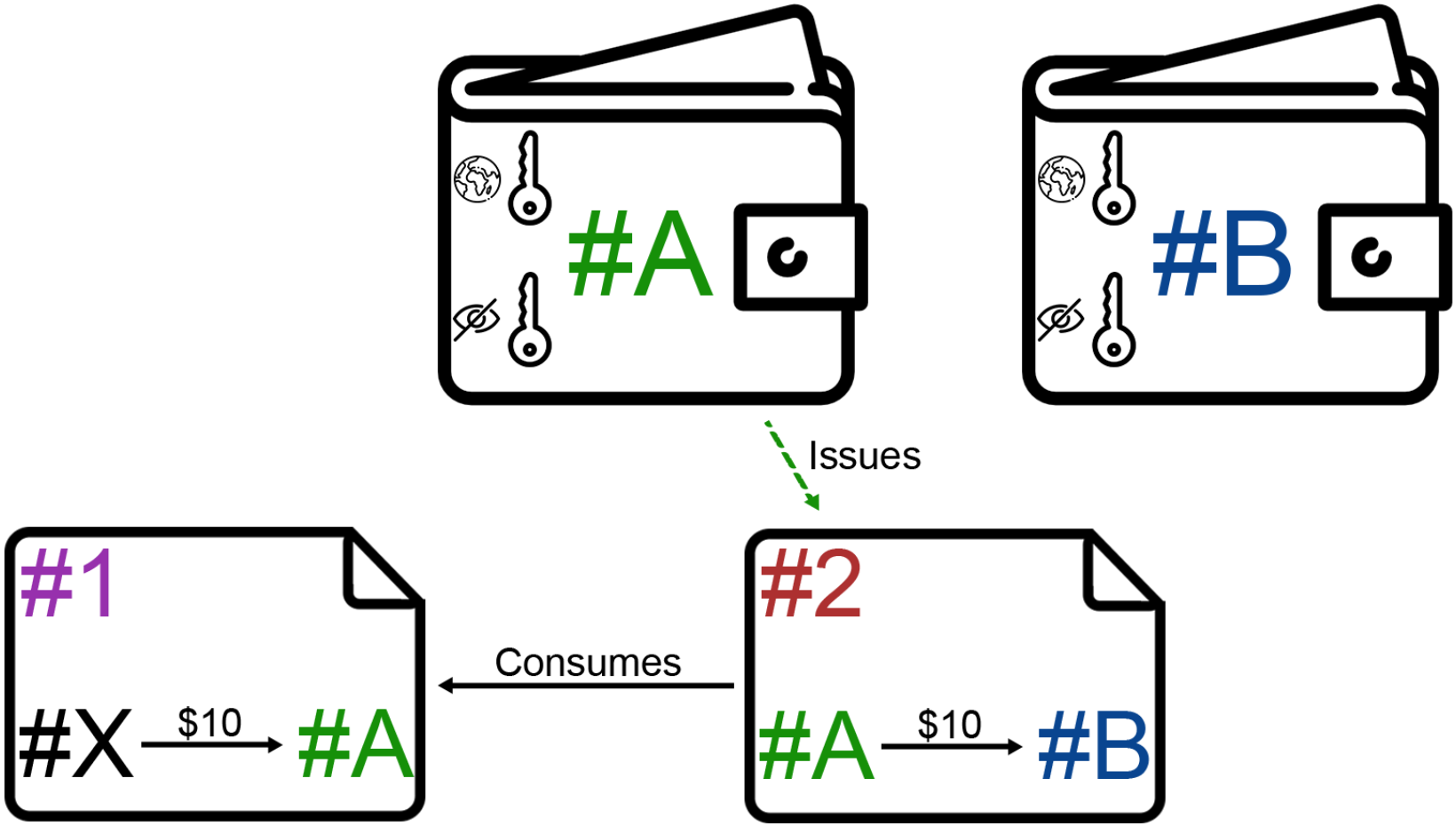
# Concepts

# Wallets transfer money



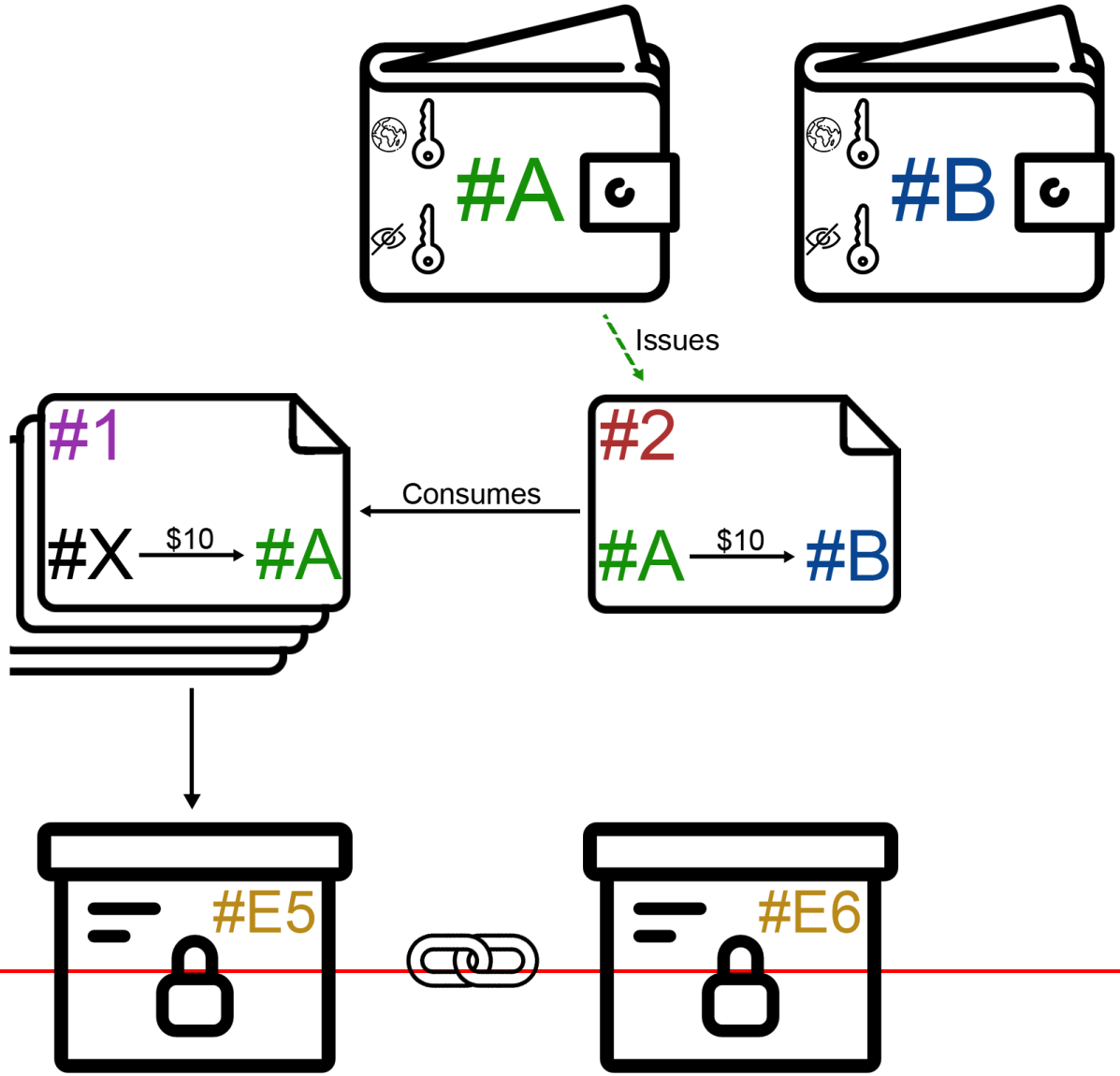

Icons made by Freepik from www.flaticon.com

# Transactions gather financials




Icons made by Freepik from www.flaticon.com

# Blocks keep track of transactions




Icons made by Freepik from www.flaticon.com

# Wallet

- necessary to participate in payment transactions
  - send transactions
  - receive transactions
- basically set of private & public key
  - used to sign transactions
  - public key as identifier in payment network

Display Implementation

## Usage

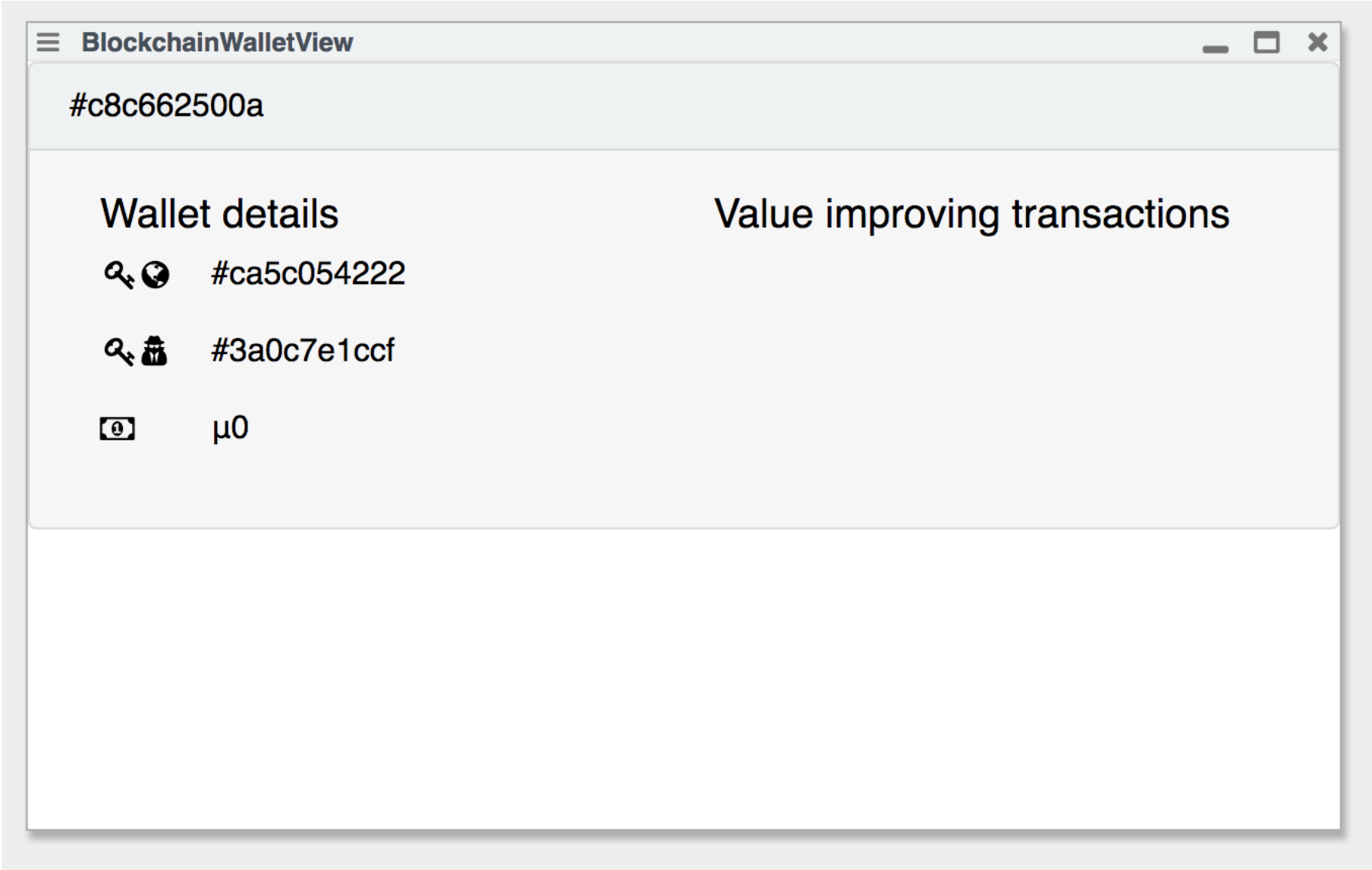
```
import Wallet from 'src/blockchain/model/wallet/wallet.js';
const wallet = new Wallet();
```

Display Wallet

## Receive payment

```
wallet.receive(transaction);
```

Receive Transaction


BlockchainWalletView
#c8c662500a
Wallet details
Value improving transactions
#ca5c054222
#3a0c7e1ccf
µ0

BlockchainWalletView

#f62182afe6

## Wallet details

#c93600d340

#1a51d71851

µ5

## Value improving transactions

#722fa54243 *µ5*

# Transaction

- fundamental atomic component of blockchain data structure
- describes **one** timestamped change within ecosystem
  - Bitcoin: single payment flow reserving some value on a wallet
- issued and signed by one wallet
- consumes outputs of other transactions → produces new outputs, which can be consumed
  - transactions form an acyclic, directed graph
  - Bitcoin: cash flow can be reconstructed

Display Implementation

## Visualization

Display Transaction

# Block

- periodically encapsulates transactions
- comparable to a ledger's page
- transactions summarized into a block are interpreted as valid
- creation of a block is called *mining*
  - requires resource intensive / time consuming work to be done
  - mining is rewarded (mining-reward and fees)

Display Implementation

## Mining Challenge

```
import forge from 'node_modules/node-forge/dist/forge.min.js';

const sha256 = forge.md.sha256.create();

const block = {'prevHash': "#3eFg7FA", "data": "...", "nonce": 0};
```

Setup Mining-Challenge

```
1
block['nonce'] = block['nonce'] + 1;
sha256.update(block);
sha256.digest().toHex();
 => 36928ee16f30168b4982f5f26f21a4acdc4e9d8d2aa891460fbaa2fd58a3daec
```

# Blockchain

- each block refers it's preceding block (chain of blocks → chronological order)
- blockchain as overall ledger: furnishes proof of any change
  - Bitcoin: any financial transaction

Display Implementation

## Formation of a Blockchain

Setup Environment

Wallet details

Value improving transactions

## Formation of a Blockchain

Setup Environment

### #0d99761b95

Wallet details

#c6c619cf2f

#c3941f156e

µ60

Value improving transactions

#78a4de8ea3 µ10

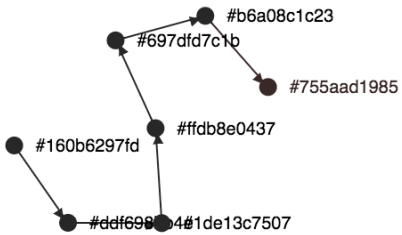
#6105314517 µ10

#14fd6d5883 µ10

#02dd38c646 µ10

#03b86ab111 µ10

#c665b3596c µ10

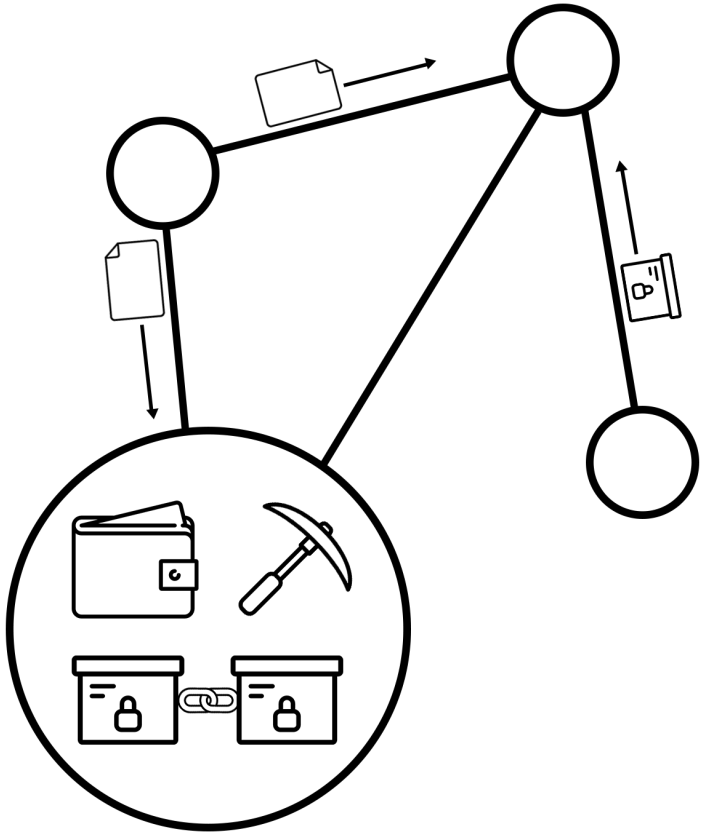



Mine Block

# Networking

# Nodes

- participants within network are called nodes
- each node can perform several actions
  - mine new blocks → Miner
  - propagate Transactions → NetworkComponent
  - maintain it's own Blockchain copy → Storage



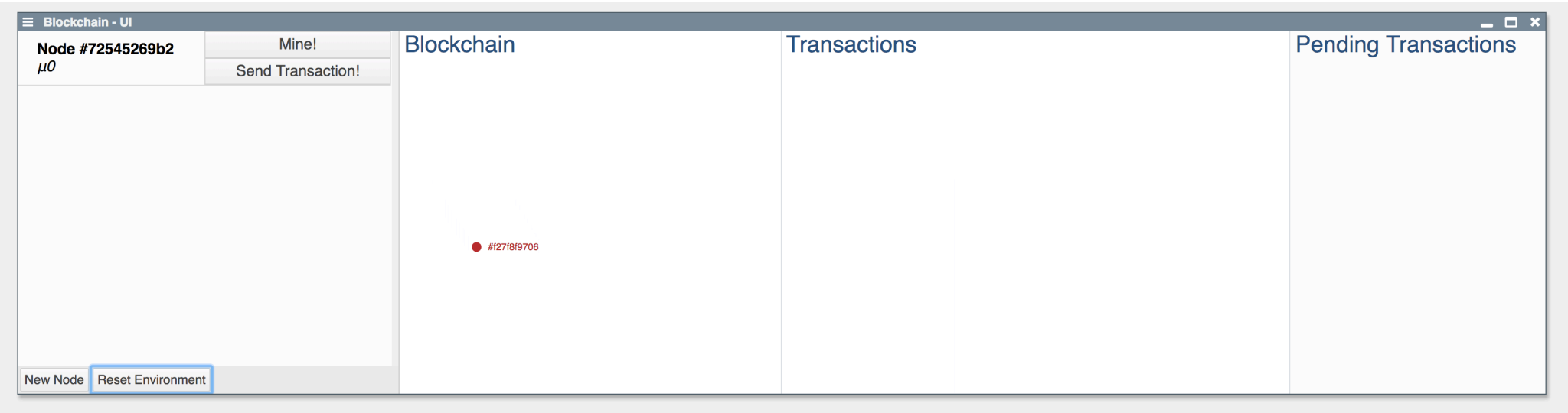
Display Implementation

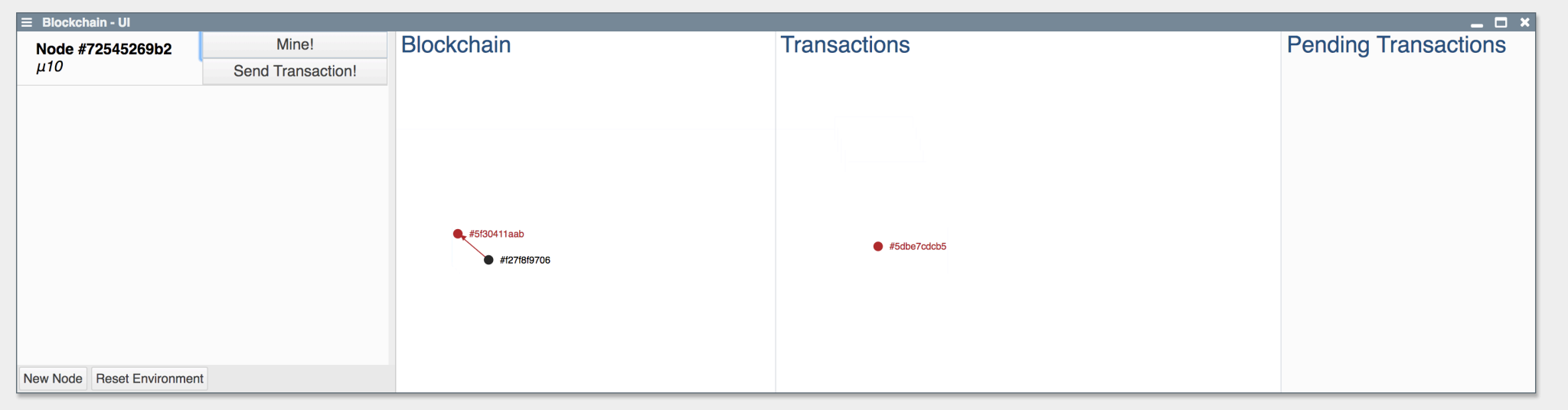
Icons made by Freepik from www.flaticon.com

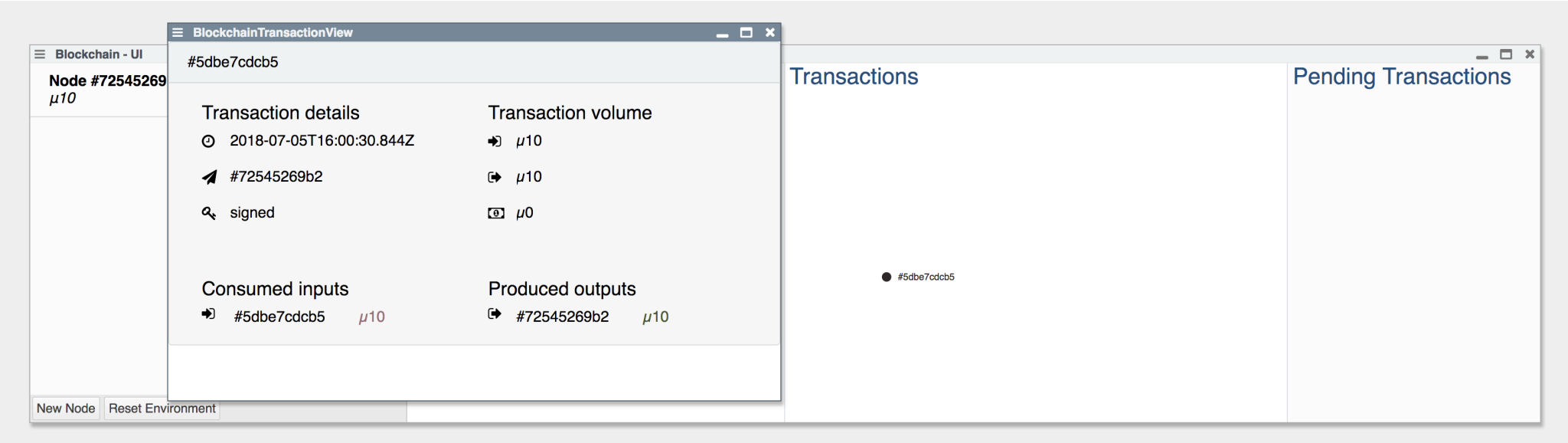
# Peer-To-Peer

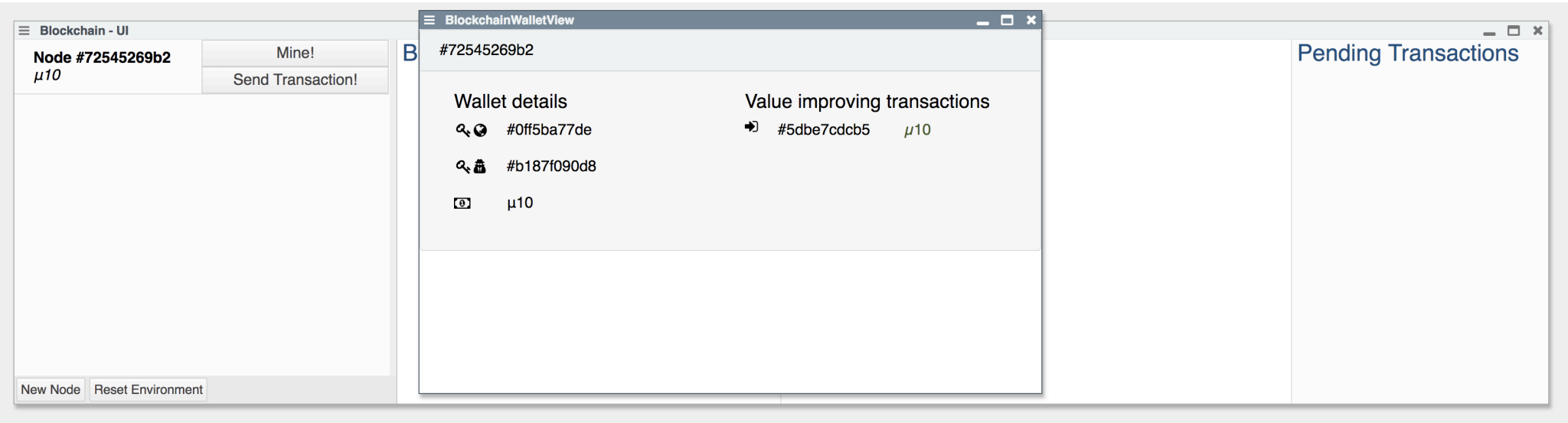
- new nodes contact long-established ones to get initial information
  - other peers
  - already existing blockchain
- consensus rules ensure same Blockchain on majority of nodes
  - blocks with solved mining-challenge are valid
  - each transaction can only be spent once
  - ...
- nodes / miner compete against each other while solving the mining challenge

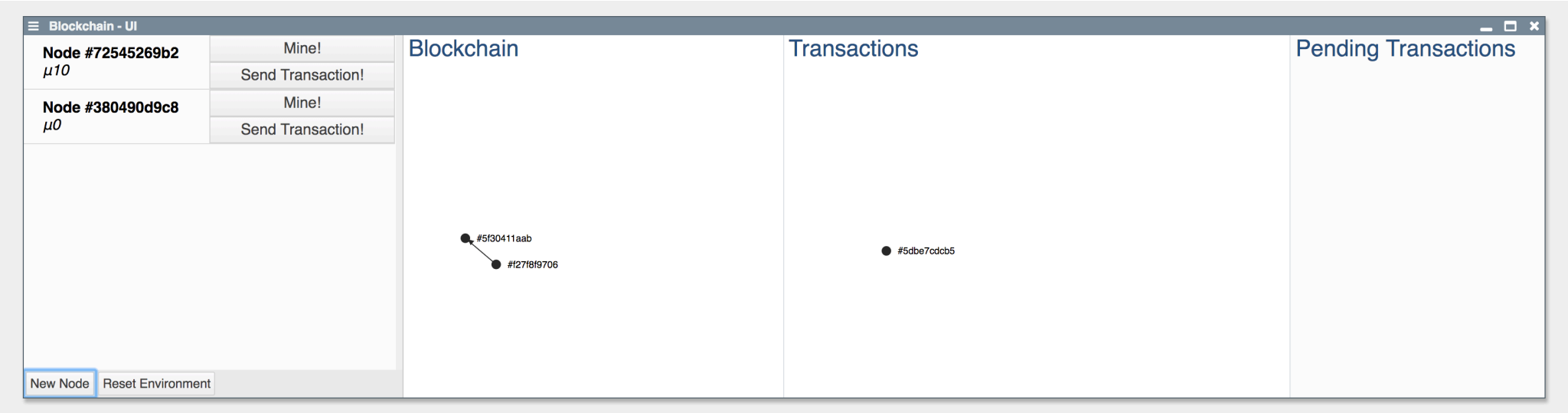
Run full Demo

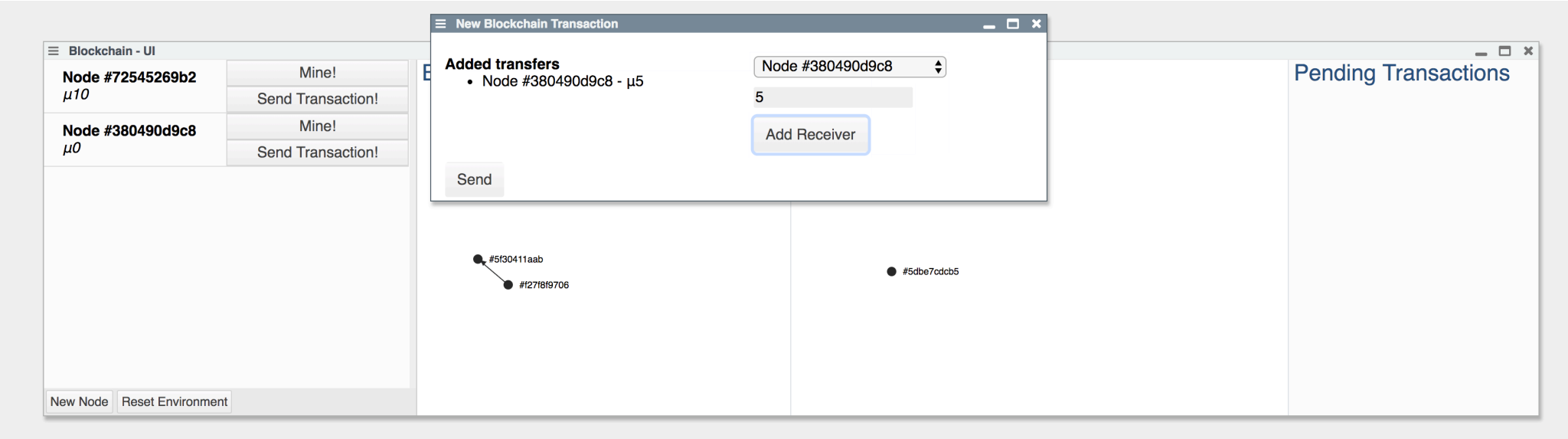

Blockchain - UI
Node #72545269b2
μ0
Mine!
Send Transaction!
New Node
Reset Environment
Blockchain
#f27f8f9706
Transactions
Pending Transactions

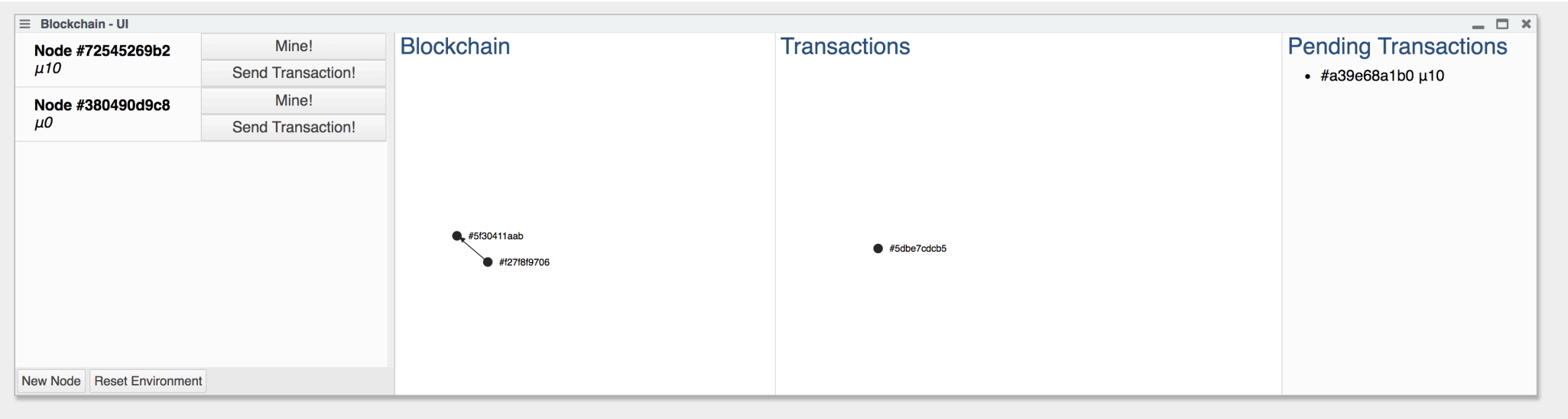

Blockchain - UI
Node #72545269b2
μ10
Mine!
Send Transaction!
New Node
Reset Environment
Blockchain
#5f30411aab
#f27f8f9706
Transactions
#5dbe7cdcb5
Pending Transactions

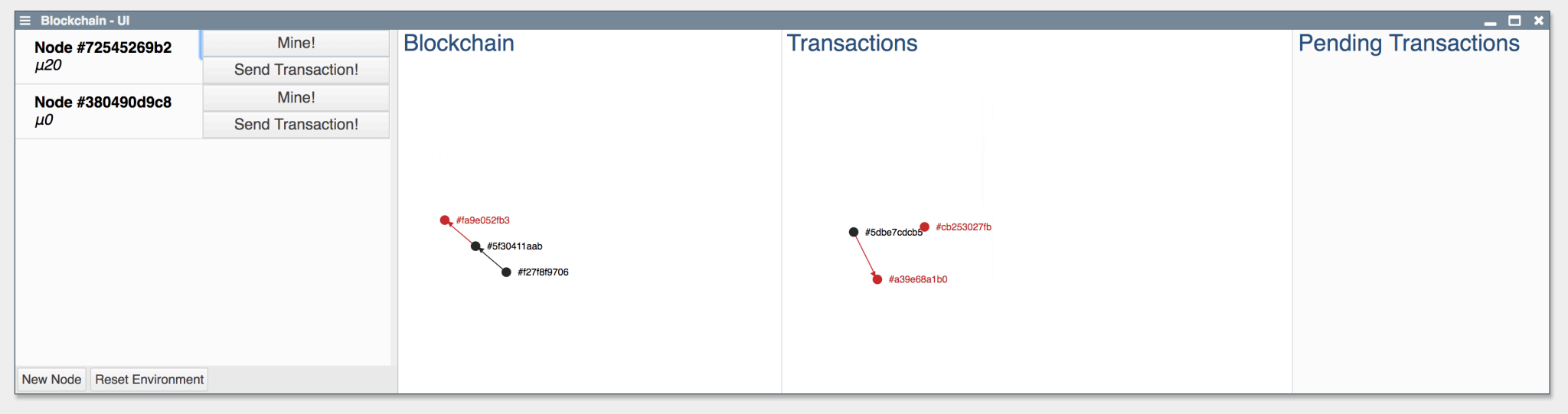

BlockchainTransactionView
#5dbe7cdcb5
Transaction details
2018-07-05T16:00:30.844Z
#72545269b2
signed
Transaction volume
μ10
μ10
μ0
Consumed inputs
#5dbe7cdcb5 μ10
Produced outputs
#72545269b2 μ10
Blockchain - UI
Node #72545269
μ10
New Node
Reset Environment
Transactions
#5dbe7cdcb5
Pending Transactions

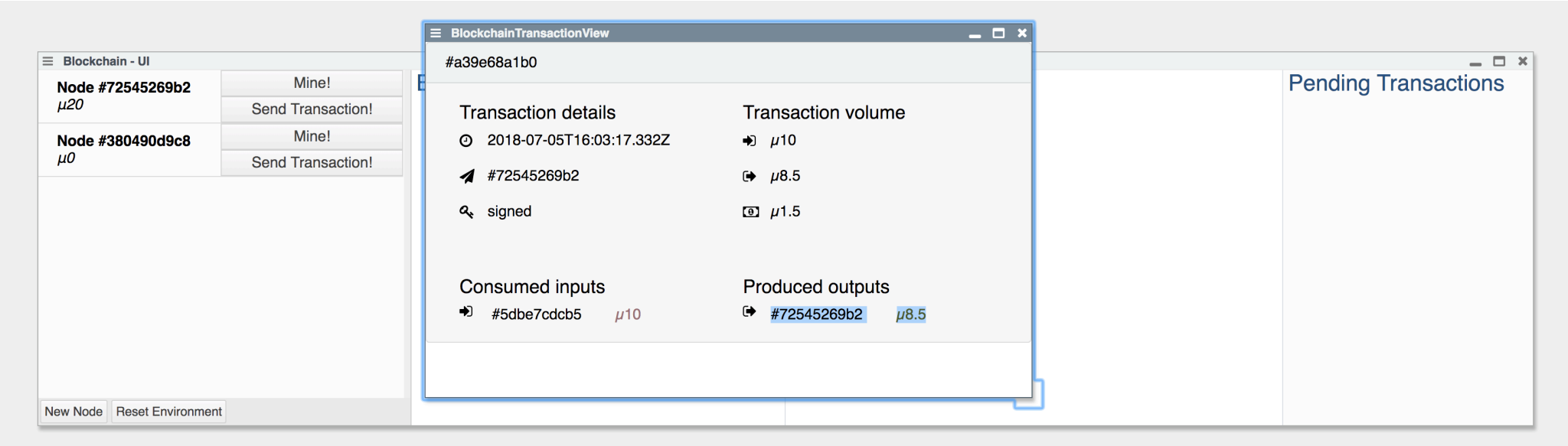

Blockchain - UI
Node #72545269b2
μ10
Mine!
Send Transaction!
New Node
Reset Environment
BlockchainWalletView
#72545269b2
Wallet details
#0ff5ba77de
#b187f090d8
μ10
Value improving transactions
#5dbe7cdcb5
μ10
Pending Transactions

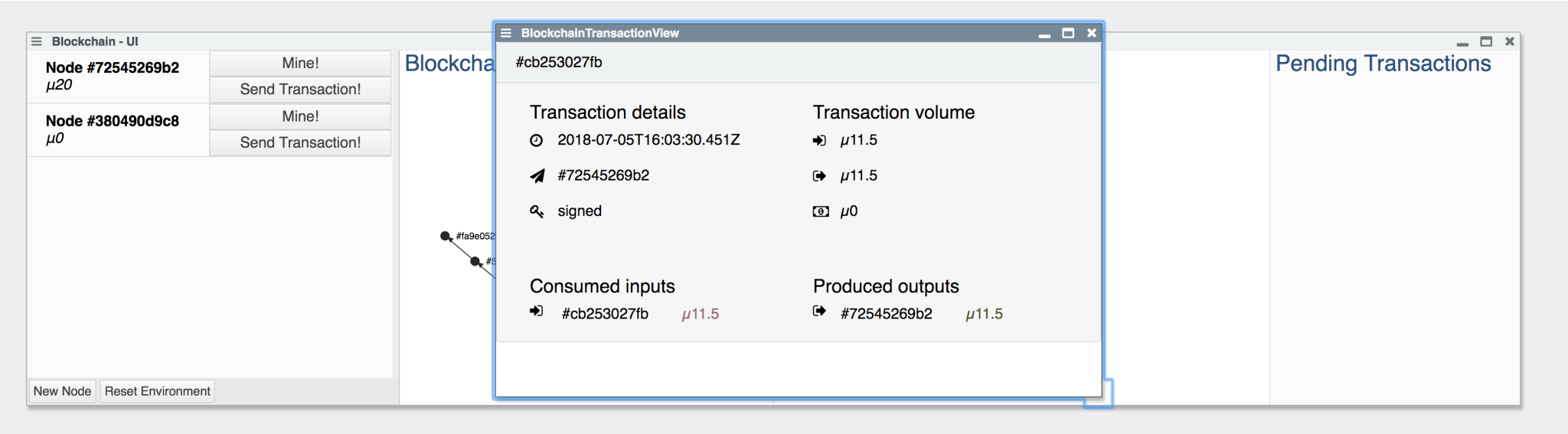

Blockchain - UI
Node #72545269b2
μ10
Mine!
Send Transaction!
Node #380490d9c8
μ0
Mine!
Send Transaction!
New Node
Reset Environment
Blockchain
#5f30411aab
#f27f8f9706
Transactions
#5dbe7cdcb5
Pending Transactions


New Blockchain Transaction
Blockchain - UI
Node #72545269b2
µ10
Mine!
Send Transaction!
Node #380490d9c8
µ0
Mine!
Send Transaction!
Added transfers
• Node #380490d9c8 - µ5
Node #380490d9c8
5
Add Receiver
Send
#5f30411aab
#f27f8f9706
#5dbe7cdcb5
Pending Transactions
New Node
Reset Environment


Blockchain - UI
Node #72545269b2
μ10
Mine!
Send Transaction!
Node #380490d9c8
μ0
Mine!
Send Transaction!
New Node
Reset Environment
Blockchain
#5f30411aab
#f27f8f9706
Transactions
#5dbe7cdcb5
Pending Transactions
#a39e68a1b0 μ10


Blockchain - UI
Node #72545269b2
μ20
Mine!
Send Transaction!
Node #380490d9c8
μ0
Mine!
Send Transaction!
New Node
Reset Environment
Blockchain
#fa9e052fb3
#5f30411aab
#f27f8f9706
Transactions
#5dbe7cdcb5
#cb253027fb
#a39e68a1b0
Pending Transactions


Blockchain - UI
Node #72545269b2
μ20
Mine!
Send Transaction!
Node #380490d9c8
μ0
Mine!
Send Transaction!
New Node
Reset Environment
BlockchainTransactionView
#a39e68a1b0
Transaction details
2018-07-05T16:03:17.332Z
#72545269b2
signed
Transaction volume
μ10
μ8.5
μ1.5
Consumed inputs
#5dbe7cdcb5 μ10
Produced outputs
#72545269b2 μ8.5
Pending Transactions


Blockchain - UI
Node #72545269b2
μ20
Mine!
Send Transaction!
Node #380490d9c8
μ0
Mine!
Send Transaction!
New Node
Reset Environment
Blockcha
Pending Transactions
BlockchainTransactionView
#cb253027fb
Transaction details
2018-07-05T16:03:30.451Z
#72545269b2
signed
Transaction volume
μ11.5
μ11.5
μ0
Consumed inputs
#cb253027fb μ11.5
Produced outputs
#72545269b2 μ11.5

# Distributed Trust

- blocks and transactions are timestamped → data is stored sequentially
- every block contains hash of prevoius block → tampering impossible
- thousands of nodes store their copy of the blockchain independently
- fundamental assumption: Majority of nodes operates trustworthy
  - enough computational power to assert always providing longest chain

## Trust experiment

```
blockchain.isValid();
 => true
```

Validate Blockchain

```
2
blockchain.headOfChain.timestamp = 123456789;
blockchain.isValid();
 => false
```

Validate Blockchain

# Blockchain validation

- ✚ novel approach to persist data tamper proof without need for central authority
  - researcher: Proof for authorship of ideas / inventions without dependence on mail service
  - bitcoin: Financial transactions without need for (central) banks clearing every transaction
- ➖ requires large number of peers to ensure security and tamper-resistants
- ➖ proof-of-Work-Concept consumes a lot of resources ~ 71 TWh / year → Energy consumption Czech Republic
- ➖ waste of storage: Blockchain is duplicated multiple times over all nodes
- ➖ bad throughput in comparison to conventional (distributed) storage solutions

# Active Essay / Interactive presentation

### What we did within Lively

- implemented a basic blockchain (wallet, transactions, -input and -outputs, blocks)
- simulated an entire peer-to-peer network
- built multiple visualizations
- created this interactive presentation

### How does the audience profit from this approach?

- interactive approach lets user apply gained knowledge
- visualizations make complex concept more tangible
- demonstration in separate UI makes collaboration of single concepts better understandable