STROMDAO

Distributed ledger technology
An introduction

Thorsten Zoerner

A transaction is a transfer of value

A transferable value is an asset. A digitally transferable values is a Digital Asset.

Blockchain Technology is Value Technology rather than Information Technology.

Transfers of value must adhere to rules to be effective

A transfer of value requires irrevocable and verifiable proof of the transfer itself and of its necessary preconditions.

Transaction rules are enshrined in (Smart) Contracts. Contracts effect the transfer of value.

```
pragma solidity 0.4.18;
contract SimpleMultiSig {

  uint public nonce;                // [only] mutable state
  uint public threshold;            // immutable state
  mapping (address => bool) isOwner; // immutable state
  address[] public ownersArr;        // immutable state

  function SimpleMultiSig(uint threshold_, address[] owners_) public {
    require(owners_.length <= 10 && threshold_ <= owners_.length && threshold_ != 0);

    address lastAdd = address(0);
    for (uint i=0; i<owners_.length; i++) {
      require(owners_[i] > lastAdd);
      isOwner[owners_[i]] = true;
      lastAdd = owners_[i];
    }
    ownersArr = owners_;
    threshold = threshold_;
  }

  // Note that address recovered from signatures must be strictly increasing
  function execute(uint8[] sigV, bytes32[] sigR, bytes32[] sigS, address destination, uint
value, bytes data) public {
    require(sigR.length == threshold);
    require(sigR.length == sigS.length && sigR.length == sigV.length);

    // Follows ERC191 signature scheme: https://github.com/ethereum/EIPs/issues/191
    bytes32 txHash = keccak256(byte(0x19), byte(0), address(this), destination, value, data,
nonce);

    address lastAdd = address(0); // cannot have address(0) as an owner
    for (uint i = 0; i < threshold; i++) {
        address recovered = ecrecover(txHash, sigV[i], sigR[i], sigS[i]);
        require(recovered > lastAdd && isOwner[recovered]);
        lastAdd = recovered;
    }

    // If we make it here all signatures are accounted for
    nonce = nonce + 1;
    require(destination.call.value(value)(data));
  }

  function () public payable {}
]
```

A block is a list of transactions

There is a maximum number of transactions per block.

$	25.00	From:	Darcy	->	Bingle
$	4.27	From:	Elizab	->	Jane
$	19.22	From:	Wickha	->	Lydia
$	106.44	From:	Lady C	->	Collin
$	6.42	From:	Charlo	->	Elizab

A block chain consists of multiple lists (or blocks) of transaction

Block: # 1

Tx:

$	25.00	From:	Darcy	->	Bingley
$	4.27	From:	Elizabeth	->	Jane
$	19.22	From:	Wickham	->	Lydia
$	106.44	From:	Lady Cather	->	Collins
$	6.42	From:	Charlotte	->	Elizabeth

Block: # 2

Tx:

$	97.67	From:	Ripley	->	Lambert
$	48.61	From:	Kane	->	Ash
$	6.15	From:	Parker	->	Dallas
$	10.44	From:	Hicks	->	Newt
$	88.32	From:	Bishop	->	Burke
$	45.00	From:	Hudson	->	Gorman
$	92.00	From:	Vasquez	->	Apone

Chaining blocks together

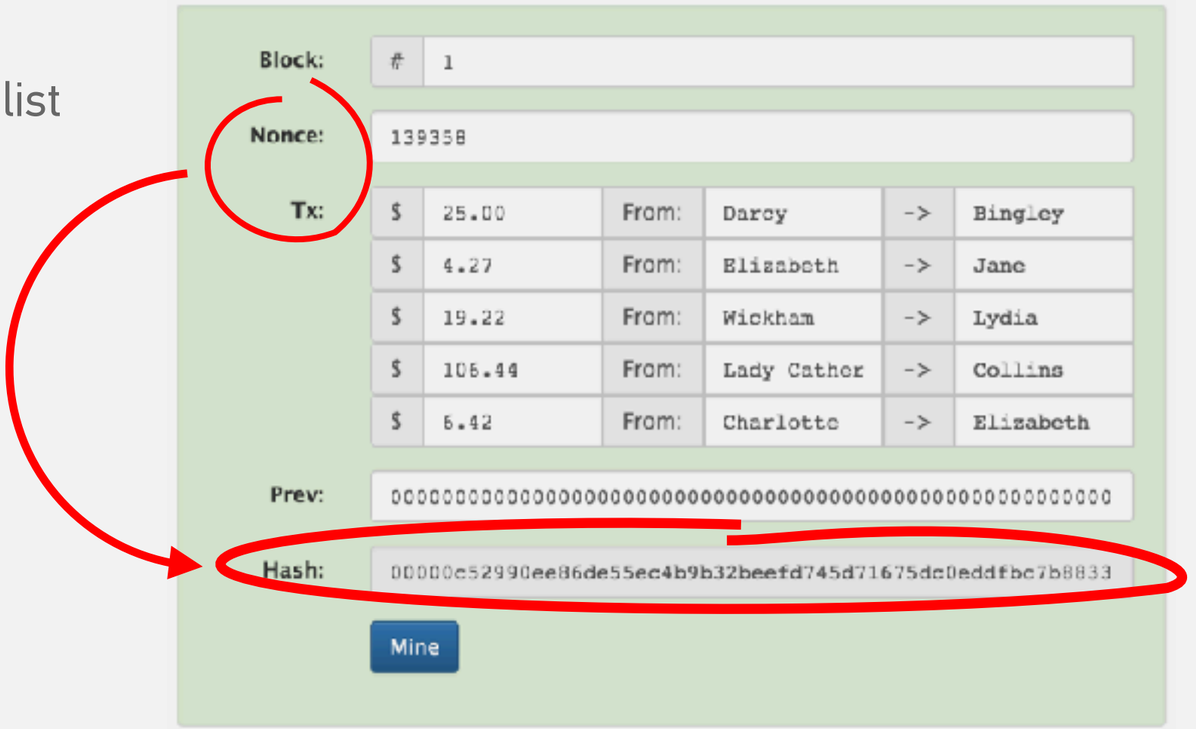
Transaction lists are chained together by each list referencing its previous list.

Block:	#	1				
Nonce:	139358					
Tx:	$	25.00	From:	Darcy	->	Bingley
	$	4.27	From:	Elizabeth	->	Jane
	$	19.22	From:	Wickham	->	Lydia
	$	106.44	From:	Lady Cather	->	Collins
	$	6.42	From:	Charlotte	->	Elizabeth
Prev:	00000000000000000000000000000000000000000000000000000000000000000					
Hash:	00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b8833					

Block:	#	2				
Nonce:	39207					
Tx:	$	97.67	From:	Ripley	->	Lambert
	$	48.61	From:	Kane	->	Ash
	$	6.15	From:	Parker	->	Dallas
	$	10.44	From:	Hicks	->	Newt
	$	88.32	From:	Bishop	->	Burke
	$	45.00	From:	Hudson	->	Gorman
	$	92.00	From:	Vasquez	->	Apone
Prev:	00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b8833					
Hash:	000078be183417844c14a9251ca245fb15df1074019873f5d85c1a6f					

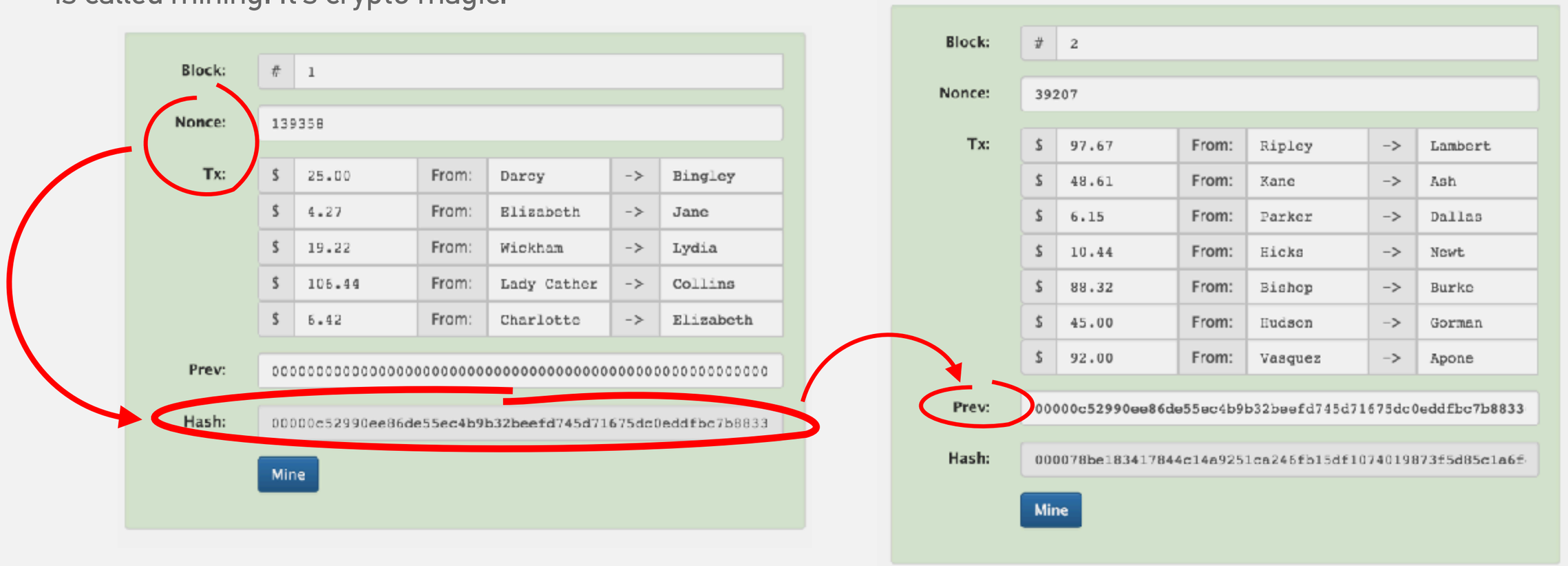
Chaining blocks together

The process of validating and referencing the previous list is called mining. It's crypto magic.



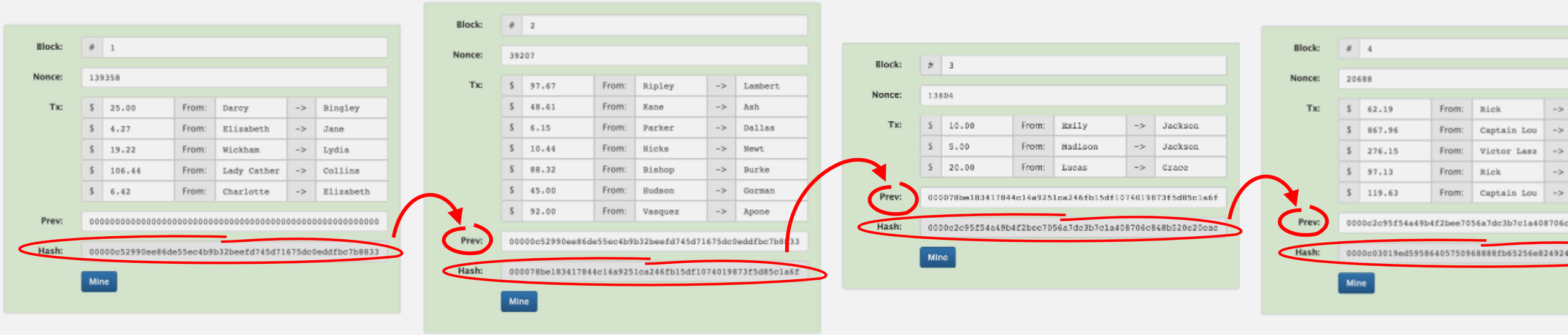
Chaining blocks together

The process of validating and referencing the previous list is called mining. It's crypto magic.



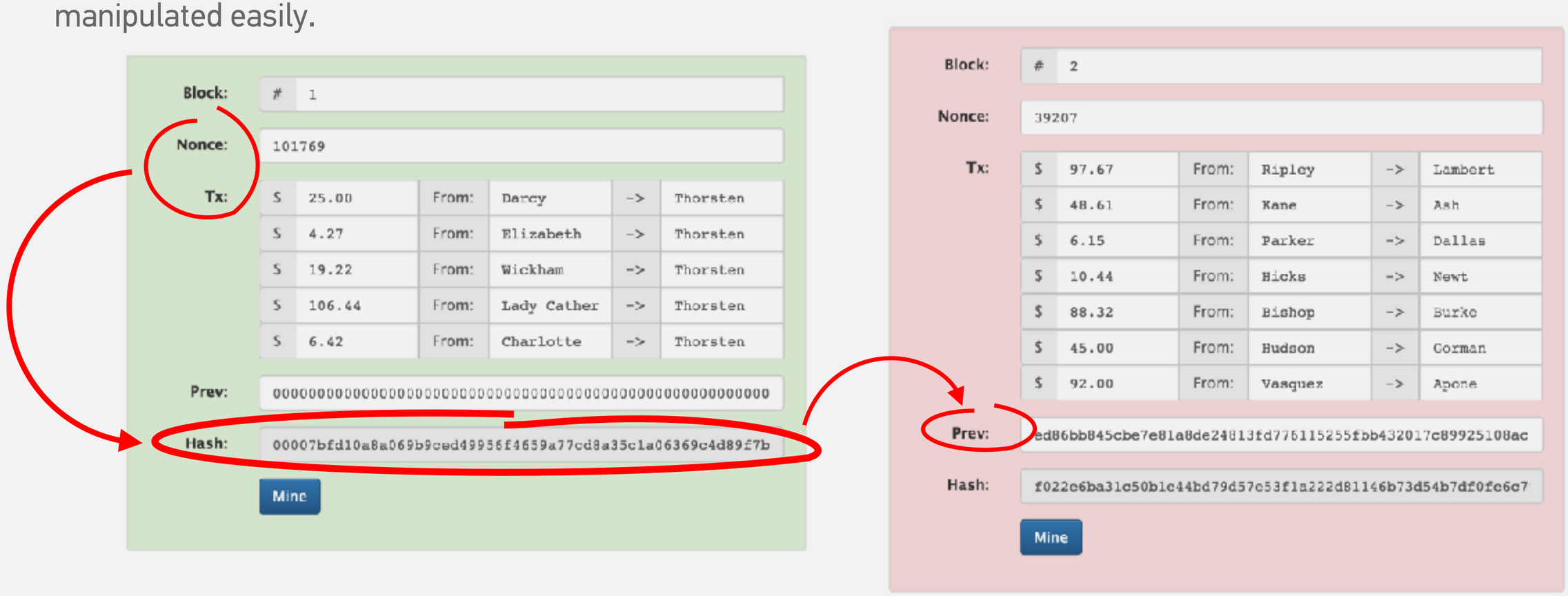
Chaining blocks together

This allows to store an unlimited number of Transactions within a chain structure.



Data consistency

Once validated and chained, transactions can not be manipulated easily.



Data redundancy

Each user (peer) works with her own copy of the full chain.

Peer A

Negotiating consensus

Each user (peer) works with her own copy of the full chain.

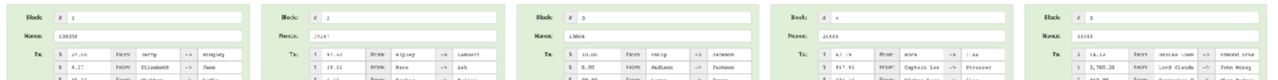
The validity of transactions is negotiated simultaneously across all peers.

Peer A

Peer B

Peer C

Peer D



Negotiating consensus

Each user (peer) works with her own copy of the full chain.

The validity of transactions is negotiated simultaneously across all peers.

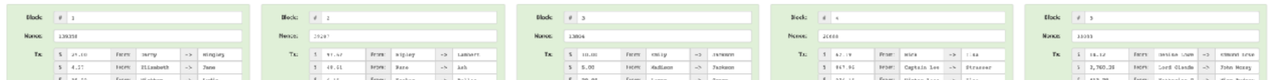
This increases the consistency guarantee.

Peer A

Peer B

Peer C

Peer D



A fault tolerant, highly redundant transaction store...

...to establish & maintain irrevocable consensus among market participants.

A value machine

Blockchain technology can be utilised to facilitate and enshrine any kind of transaction between market participants.

STROMDAO

A consensus system
for energy markets

kontakt@stromdao.com

Backup

Blockchain-Akteure & Adressen.

Jedes Objekt, das eine Transaktion in der Blockchain vornehmen kann, hat eine eineindeutige Adresse.

Rückschlüsse, ob es sich dabei um einen Marktakteur, SmartContract, oder Token handelt, sind nicht möglich.

Adressen sind (unveränderlich). Ein Smart Contract mit einer bestimmten Adresse kann nicht mehr nachträglich in seiner Funktion verändert werden.