

**STROM**DAO

# 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.

\$	10.00	From:	Anders	->	Sophia
----	-------	-------	--------	----	--------

# 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.

```
1 pragma solidity 0.4.18;
2 contract SimpleMultiSig {
3
4     uint public nonce;           // [only] mutable state
5     uint public threshold;       // immutable state
6     mapping (address => bool) isOwner; // immutable state
7     address[] public ownersArr;  // immutable state
8
9     function SimpleMultiSig(uint threshold_, address[] owners_) public {
10         require(owners_.length <= 10 && threshold_ <= owners_.length && threshold_ != 0);
11
12         address lastAdd = address(0);
13         for (uint i=0; i<owners_.length; i++) {
14             require(owners_[i] > lastAdd);
15             isOwner[owners_[i]] = true;
16             lastAdd = owners_[i];
17         }
18         ownersArr = owners_;
19         threshold = threshold_;
20     }
21
22     // Note that address recovered from signatures must be strictly increasing
23     function execute(uint8[] sigV, bytes32[] sigR, bytes32[] sigS, address destination, uint
value, bytes data) public {
24         require(sigR.length == threshold);
25         require(sigR.length == sigS.length && sigR.length == sigV.length);
26
27         // Follows ERC191 signature scheme: https://github.com/ethereum/EIPs/issues/191
28         bytes32 txHash = keccak256(byte(0x19), byte(0), address(this), destination, value, data,
nonce);
29
30         address lastAdd = address(0); // cannot have address(0) as an owner
31         for (uint i = 0; i < threshold; i++) {
32             address recovered = ecrecover(txHash, sigV[i], sigR[i], sigS[i]);
33             require(recovered > lastAdd && isOwner[recovered]);
34             lastAdd = recovered;
35         }
36
37         // If we make it here all signatures are accounted for
38         nonce = nonce + 1;
39         require(destination.call.value(value)(data));
40     }
41
42     function () public payable {}
43 }
```

# A block is a list of transactions

There is a maximum number of transactions per block.

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

# 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
\$	105.44	From:	Lady Cathor	->	Collins
\$	5.42	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 Cathor	->	Collins
\$	6.42	From:	Charlotte	->	Elizabeth

Prev:

00

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:

000078be183417844c14a9251ca246fb15df1074019873f5d85c1a6f

# Chaining blocks together

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

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:

00

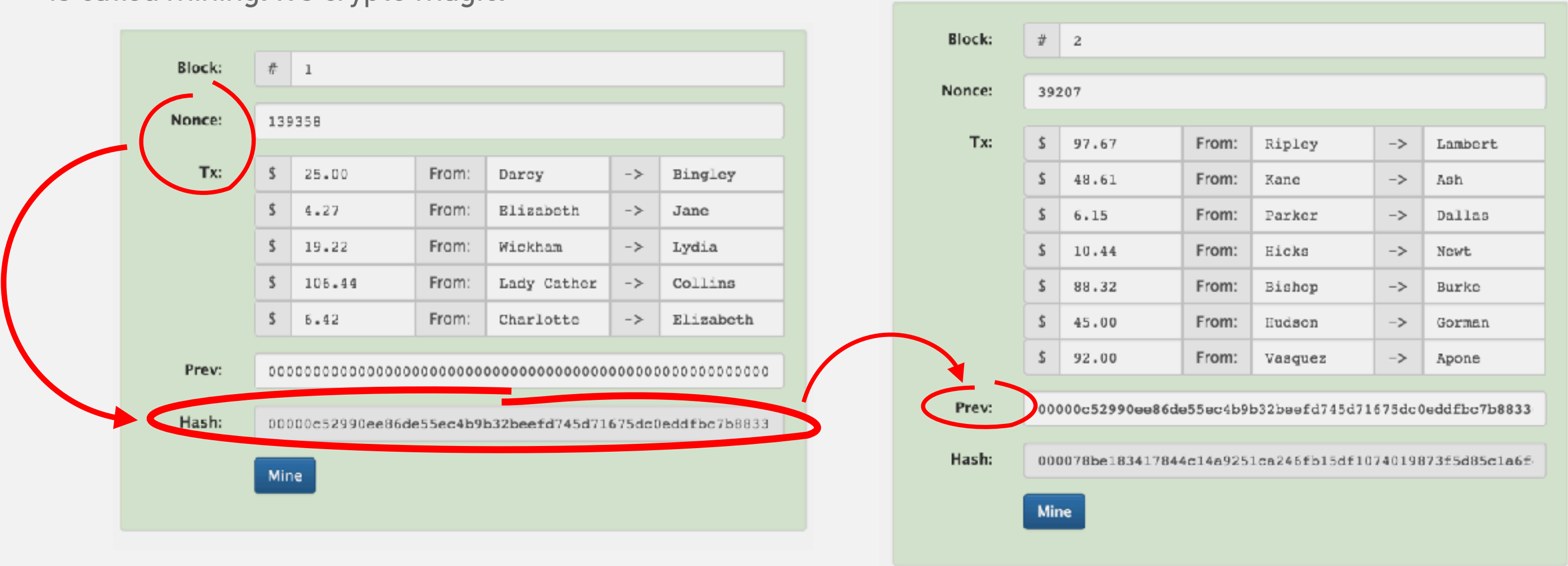
Hash:

00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b8833

Mine

# Chaining blocks together

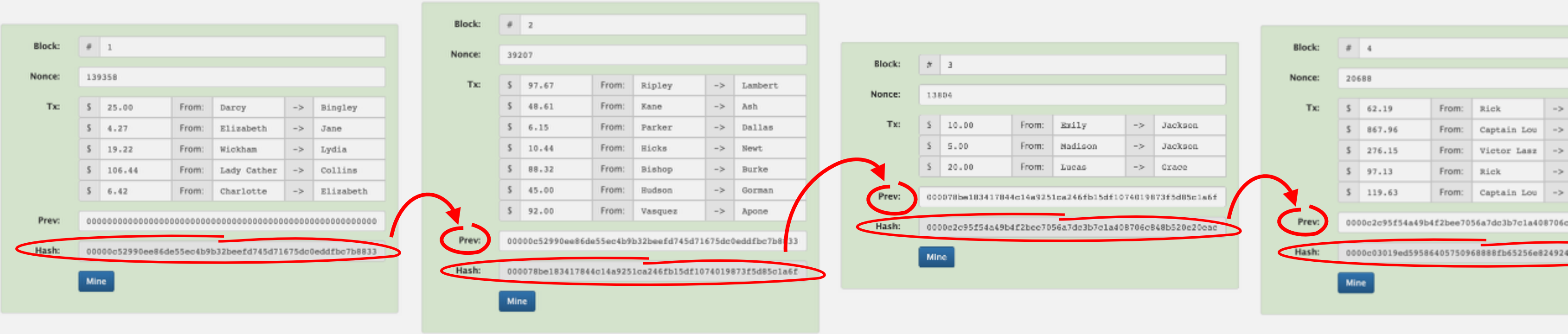
The process of validating and referencing the previous list is called mining. It's crypto magic.





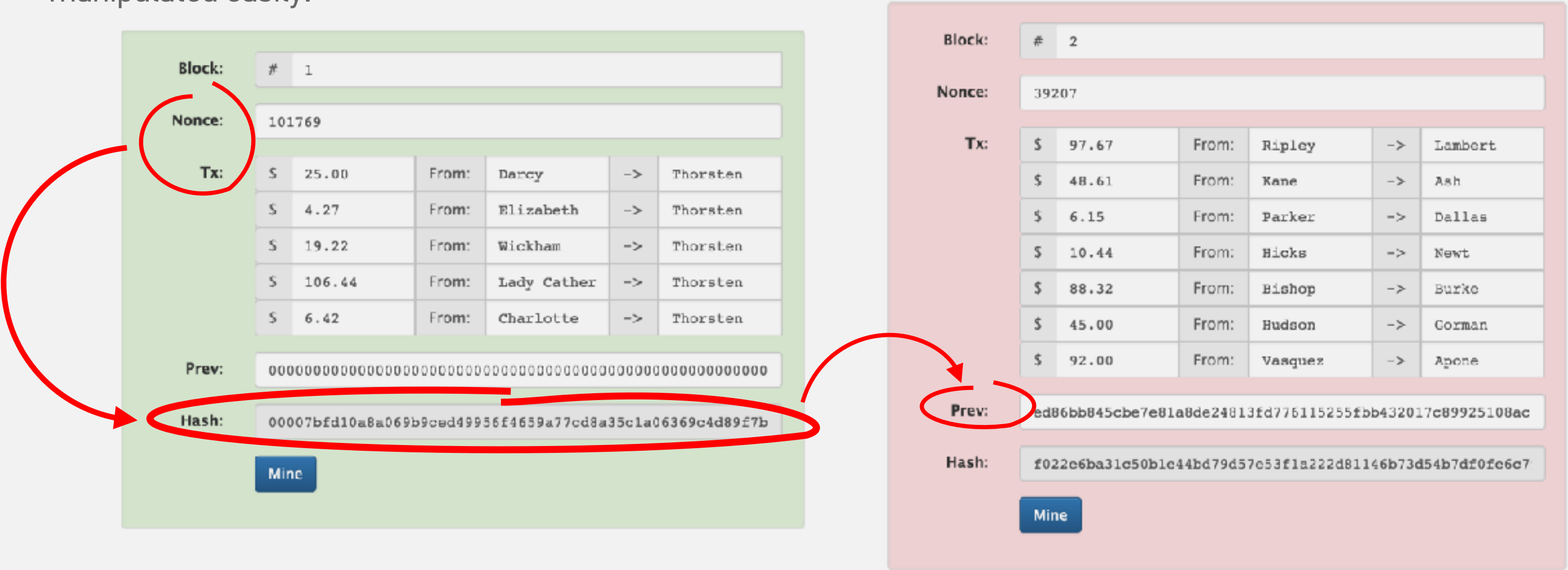
# Chaining blocks together

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

[illegible]

**Block:** # 2

**Header:** 20207

To:	From:	Amount:
5 91.67	From: wipiny	-> lamarr
5 48.51	From: Ware	-> Ash
5 6.15	From: Tenber	-> Dallas
5 10.44	From: Eakho	-> Hewa
5 88.31	From: Elnlow	-> Bucke
5 45.03	From: mearon	-> marmat
5 92.03	From: Vasquez	-> Apone

**Proof:** 0000e52993ee06d55ec4b9122ee4d715d71676dc0ed0e7b0223

**Hash:** 00078b133817044e34e523ec2c6b15d81d74019f71d5485e1a5d

**Mine**

**Block:** # 3

**Nums:** 13004

Tx	S	to	from	val	id
	\$ 10.00	From	colly	->	random
	\$ 5.00	From	radisson	->	Jackson
	\$ 20.00	From	Larson	->	Grace

**Prev:** 1034317044c34e9251ca2852e05d8094619172d6d8e1a6f811106d0

**Hash:** 0000e2c958f4e1094d2ba0773567de2b7e1c1097c6e848b320a29aa

[Mine](#)

**Block:**

**Nonce:**

To:	From:	Amount	Gas
5 42.19	From: Alice	->	1000
5 867.96	From: Captain Lee	->	Stranger
5 276.15	From: Victor Sean	->	Ellen
5 57.13	From: Rick	->	Sam
5 119.63	From: Captain Lee	->	Jon Brundel

**Prev:**

**Hash:**

[More](#)

[illegible]

[illegible]

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

[illegible][illegible]

Block # 1	Block # 2	Block # 3	Block # 4	Block # 5																																																																																																
Name: L30308	Name: 20297	Name: L3004	Name: 20688	Name: J0035																																																																																																
Tx: <table> <tr><td>S</td><td>25.10</td><td>Ferry</td><td>Harpy</td><td>-&gt;</td><td>Herring</td></tr> <tr><td>S</td><td>4.27</td><td>FERRY</td><td>Ellenburgh</td><td>-&gt;</td><td>June</td></tr> <tr><td>E</td><td>35.55</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>Leah</td></tr> </table>	S	25.10	Ferry	Harpy	->	Herring	S	4.27	FERRY	Ellenburgh	->	June	E	35.55	Ferry	William	->	Leah	Tx: <table> <tr><td>S</td><td>97.47</td><td>Ferry</td><td>Herring</td><td>-&gt;</td><td>Lambert</td></tr> <tr><td>S</td><td>49.18</td><td>FERRY</td><td>Bare</td><td>-&gt;</td><td>Jack</td></tr> <tr><td>E</td><td>6.18</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>William</td></tr> </table>	S	97.47	Ferry	Herring	->	Lambert	S	49.18	FERRY	Bare	->	Jack	E	6.18	Ferry	William	->	William	Tx: <table> <tr><td>S</td><td>11.00</td><td>Ferry</td><td>enup</td><td>-&gt;</td><td>William</td></tr> <tr><td>S</td><td>5.00</td><td>FERRY</td><td>William</td><td>-&gt;</td><td>William</td></tr> <tr><td>E</td><td>50.00</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>William</td></tr> </table>	S	11.00	Ferry	enup	->	William	S	5.00	FERRY	William	->	William	E	50.00	Ferry	William	->	William	Tx: <table> <tr><td>S</td><td>67.19</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>William</td></tr> <tr><td>S</td><td>167.91</td><td>FERRY</td><td>Captain Lee</td><td>-&gt;</td><td>Strasser</td></tr> <tr><td>E</td><td>252.15</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>William</td></tr> <tr><td>E</td><td>675.78</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>William</td></tr> </table>	S	67.19	Ferry	William	->	William	S	167.91	FERRY	Captain Lee	->	Strasser	E	252.15	Ferry	William	->	William	E	675.78	Ferry	William	->	William	Tx: <table> <tr><td>S</td><td>14.14</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>William</td></tr> <tr><td>S</td><td>2,760.28</td><td>FERRY</td><td>Lord Glands</td><td>-&gt;</td><td>John Henry</td></tr> <tr><td>E</td><td>675.78</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>William</td></tr> </table>	S	14.14	Ferry	William	->	William	S	2,760.28	FERRY	Lord Glands	->	John Henry	E	675.78	Ferry	William	->	William
S	25.10	Ferry	Harpy	->	Herring																																																																																															
S	4.27	FERRY	Ellenburgh	->	June																																																																																															
E	35.55	Ferry	William	->	Leah																																																																																															
S	97.47	Ferry	Herring	->	Lambert																																																																																															
S	49.18	FERRY	Bare	->	Jack																																																																																															
E	6.18	Ferry	William	->	William																																																																																															
S	11.00	Ferry	enup	->	William																																																																																															
S	5.00	FERRY	William	->	William																																																																																															
E	50.00	Ferry	William	->	William																																																																																															
S	67.19	Ferry	William	->	William																																																																																															
S	167.91	FERRY	Captain Lee	->	Strasser																																																																																															
E	252.15	Ferry	William	->	William																																																																																															
E	675.78	Ferry	William	->	William																																																																																															
S	14.14	Ferry	William	->	William																																																																																															
S	2,760.28	FERRY	Lord Glands	->	John Henry																																																																																															
E	675.78	Ferry	William	->	William																																																																																															

Block:	# 1		
Block:	# 2		
Block:	# 3		
Block:	# 4		
Block:	# 5		

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

This increases the consistency guarantee.

[illegible][illegible]

Block: # 1	Block: # 2	Block: # 3	Block: # 4	Block: # 5																																																																											
Name: L30038	Name: L30287	Name: L30004	Name: L30008	Name: L30033																																																																											
Tx: <table> <tr><td>\$ 25.10</td><td>Ferry</td><td>Barry</td><td>-&gt;</td><td>Herringay</td></tr> <tr><td>\$ 4.37</td><td>HQPC</td><td>Ellenburgh</td><td>-&gt;</td><td>June</td></tr> <tr><td>\$ 35.55</td><td>Ferry</td><td>William</td><td>-&gt;</td><td>Leith</td></tr> </table>	\$ 25.10	Ferry	Barry	->	Herringay	\$ 4.37	HQPC	Ellenburgh	->	June	\$ 35.55	Ferry	William	->	Leith	Tx: <table> <tr><td>\$ 97.87</td><td>Ferry</td><td>Herringay</td><td>-&gt;</td><td>Lambert</td></tr> <tr><td>\$ 49.11</td><td>HQPC</td><td>Baze</td><td>-&gt;</td><td>Jak</td></tr> <tr><td>\$ 6.18</td><td>Ferry</td><td>Wardlaw</td><td>-&gt;</td><td>Wickham</td></tr> </table>	\$ 97.87	Ferry	Herringay	->	Lambert	\$ 49.11	HQPC	Baze	->	Jak	\$ 6.18	Ferry	Wardlaw	->	Wickham	Tx: <table> <tr><td>\$ 11.00</td><td>Ferry</td><td>Chapin</td><td>-&gt;</td><td>Chapman</td></tr> <tr><td>\$ 5.00</td><td>HQPC</td><td>Adelaide</td><td>-&gt;</td><td>Jackman</td></tr> <tr><td>\$ 50.00</td><td>Ferry</td><td>Wardlaw</td><td>-&gt;</td><td>Wickham</td></tr> </table>	\$ 11.00	Ferry	Chapin	->	Chapman	\$ 5.00	HQPC	Adelaide	->	Jackman	\$ 50.00	Ferry	Wardlaw	->	Wickham	Tx: <table> <tr><td>\$ 67.19</td><td>Ferry</td><td>HQPC</td><td>-&gt;</td><td>Leith</td></tr> <tr><td>\$ 167.91</td><td>HQPC</td><td>Captain Lee</td><td>-&gt;</td><td>Strassner</td></tr> <tr><td>\$ 282.18</td><td>Ferry</td><td>Alphons Lee</td><td>-&gt;</td><td>Wickham</td></tr> </table>	\$ 67.19	Ferry	HQPC	->	Leith	\$ 167.91	HQPC	Captain Lee	->	Strassner	\$ 282.18	Ferry	Alphons Lee	->	Wickham	Tx: <table> <tr><td>\$ 14.12</td><td>Ferry</td><td>William Ward</td><td>-&gt;</td><td>Chapman Ward</td></tr> <tr><td>\$ 2,760.28</td><td>HQPC</td><td>Lord Glenda</td><td>-&gt;</td><td>John Henry</td></tr> <tr><td>\$ 675.78</td><td>Ferry</td><td>Wardlaw</td><td>-&gt;</td><td>Wickham</td></tr> </table>	\$ 14.12	Ferry	William Ward	->	Chapman Ward	\$ 2,760.28	HQPC	Lord Glenda	->	John Henry	\$ 675.78	Ferry	Wardlaw	->	Wickham
\$ 25.10	Ferry	Barry	->	Herringay																																																																											
\$ 4.37	HQPC	Ellenburgh	->	June																																																																											
\$ 35.55	Ferry	William	->	Leith																																																																											
\$ 97.87	Ferry	Herringay	->	Lambert																																																																											
\$ 49.11	HQPC	Baze	->	Jak																																																																											
\$ 6.18	Ferry	Wardlaw	->	Wickham																																																																											
\$ 11.00	Ferry	Chapin	->	Chapman																																																																											
\$ 5.00	HQPC	Adelaide	->	Jackman																																																																											
\$ 50.00	Ferry	Wardlaw	->	Wickham																																																																											
\$ 67.19	Ferry	HQPC	->	Leith																																																																											
\$ 167.91	HQPC	Captain Lee	->	Strassner																																																																											
\$ 282.18	Ferry	Alphons Lee	->	Wickham																																																																											
\$ 14.12	Ferry	William Ward	->	Chapman Ward																																																																											
\$ 2,760.28	HQPC	Lord Glenda	->	John Henry																																																																											
\$ 675.78	Ferry	Wardlaw	->	Wickham																																																																											

**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](mailto:kontakt@stromdao.com)

Backup



# Blockchain-Akteure & Adressen.

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

Rückschlüsse, ob es sich dabei um einen Marktakeur, 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.