TNG TECHNOLOGY CONSULTING

Blockchain

Manipulationssicherung von Enterprise-Datenbanken mittels öffentlicher Blockchains

Martin Kreidenweis

2018-05-18, Big Techday, München

Blockchain

Private Blockchains

Wann Blockchain nutzen?

Manipulationssicherung privater Datenbanken

Blockchain

Was bringt uns das wirklich?

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

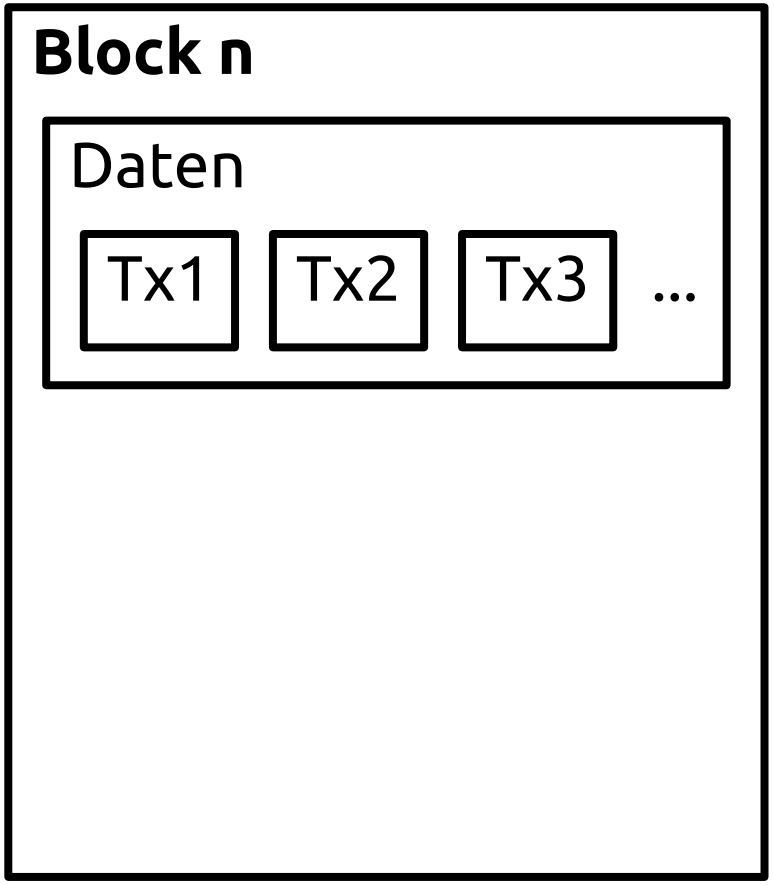
bitcoin

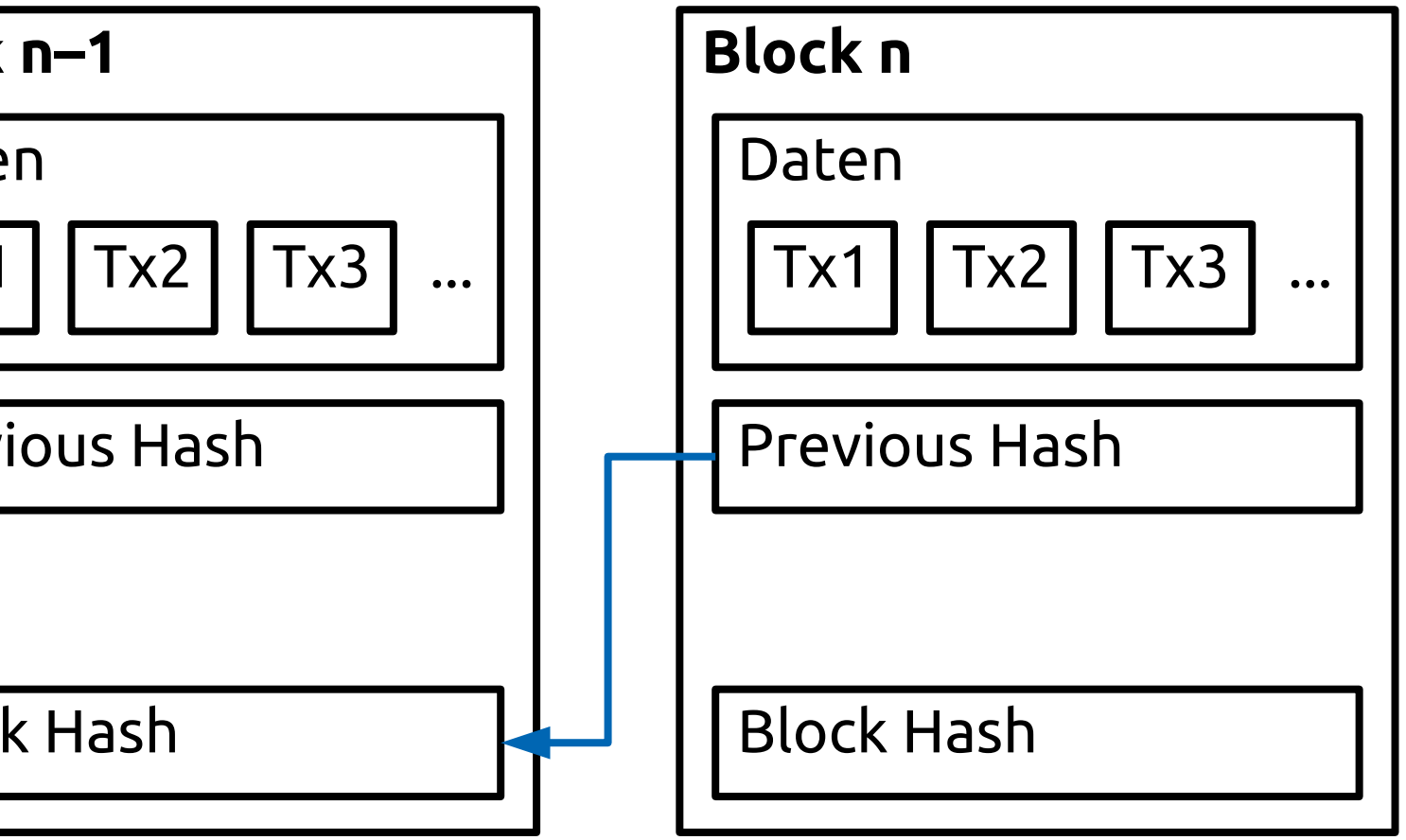
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

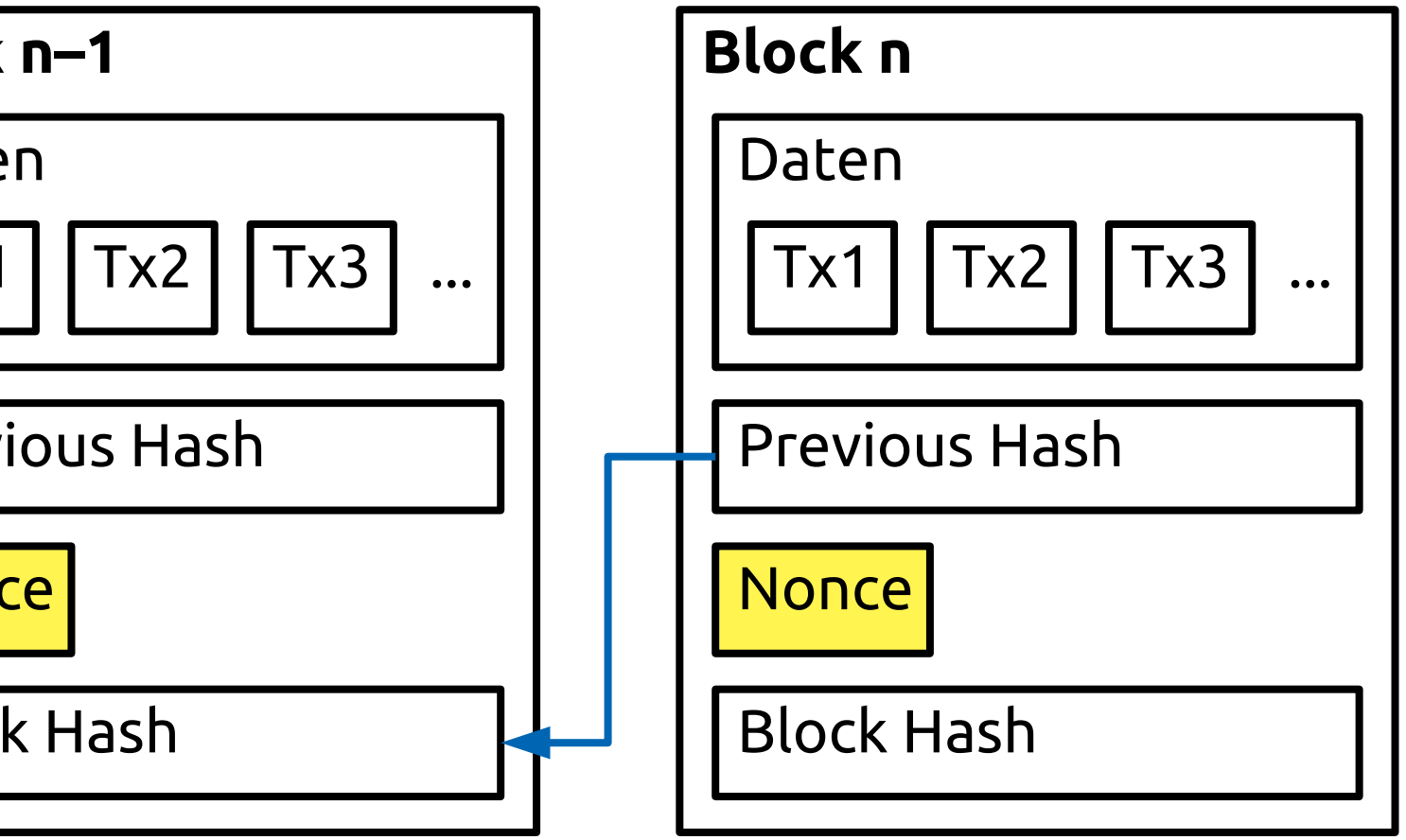
bitcoin

dezentral

Blockchain


Block n
Daten
Tx1
Tx2
Tx3
...


k n–1
en
Tx2
Tx3
...
ious Hash
k Hash
Block n
Daten
Tx1
Tx2
Tx3
...
Previous Hash
Block Hash


n–1
en
Tx2
Tx3
...
ious Hash
ce
k Hash
Block n
Daten
Tx1
Tx2
Tx3
...
Previous Hash
Nonce
Block Hash

Proof of Work

Proof of Work

"Hello, world!**0**" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

Proof of Work

"Hello, world!**0**" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello, world!**1**" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

Proof of Work

"Hello, world!**0**" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello, world!**1**" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

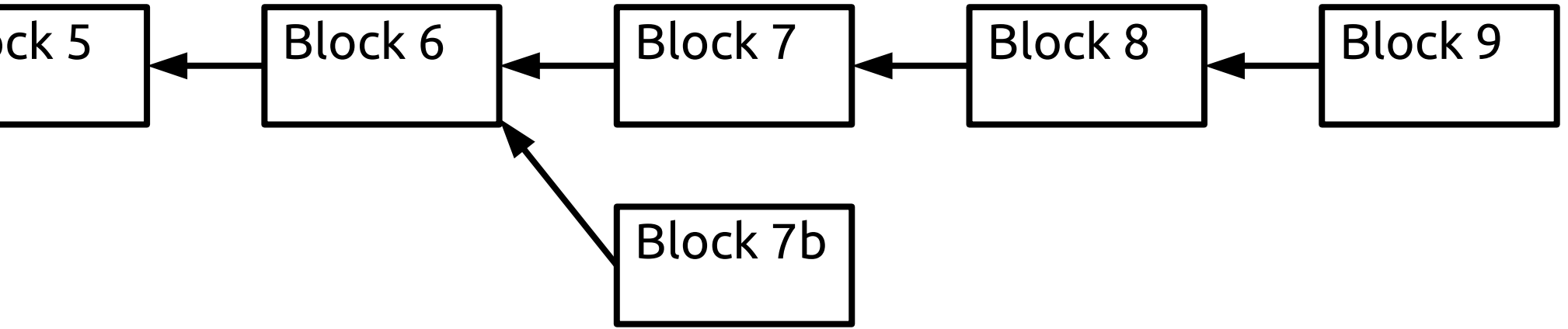
...

"Hello, world!**4249**" =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6

"Hello, world!**4250**" =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

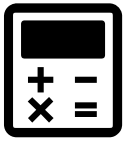
wahrscheinlich

Blockchain



Konsens

Konsens-Modelle



Proof of Work

Proof of Stake

Proof of Authority “Signing instead of Mining”

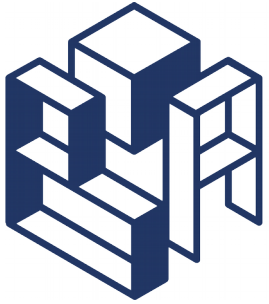
…

Private Blockchains

Blockchains for Business

HYPERLEDGER

c·rda



BlockApps™

...

HYPERLEDGER

Frameworks

HYPERLEDGER
FABRIC

HYPERLEDGER
IROHA

HYPERLEDGER
SAWTOOTH

HYPERLEDGER
INDY

Tools

HYPERLEDGER
COMPOSER

HYPERLEDGER
EXPLORER

HYPERLEDGER
QUILT

HYPERLEDGER
CELLO


HYPERLEDGER
FABRIC


HYPERLEDGER
COMPOSER

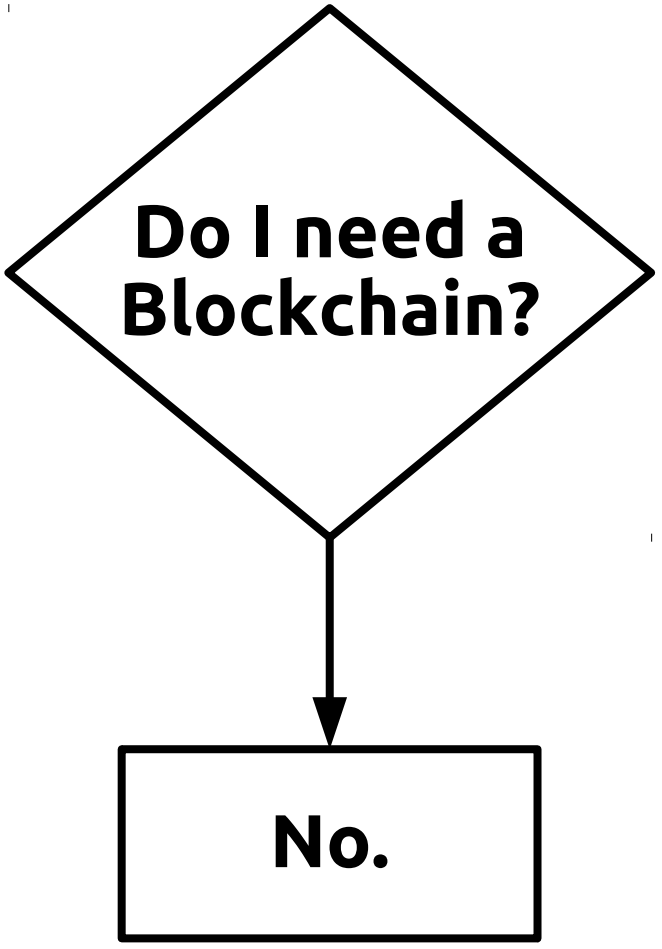
Proof of Elapsed Time


c·rda

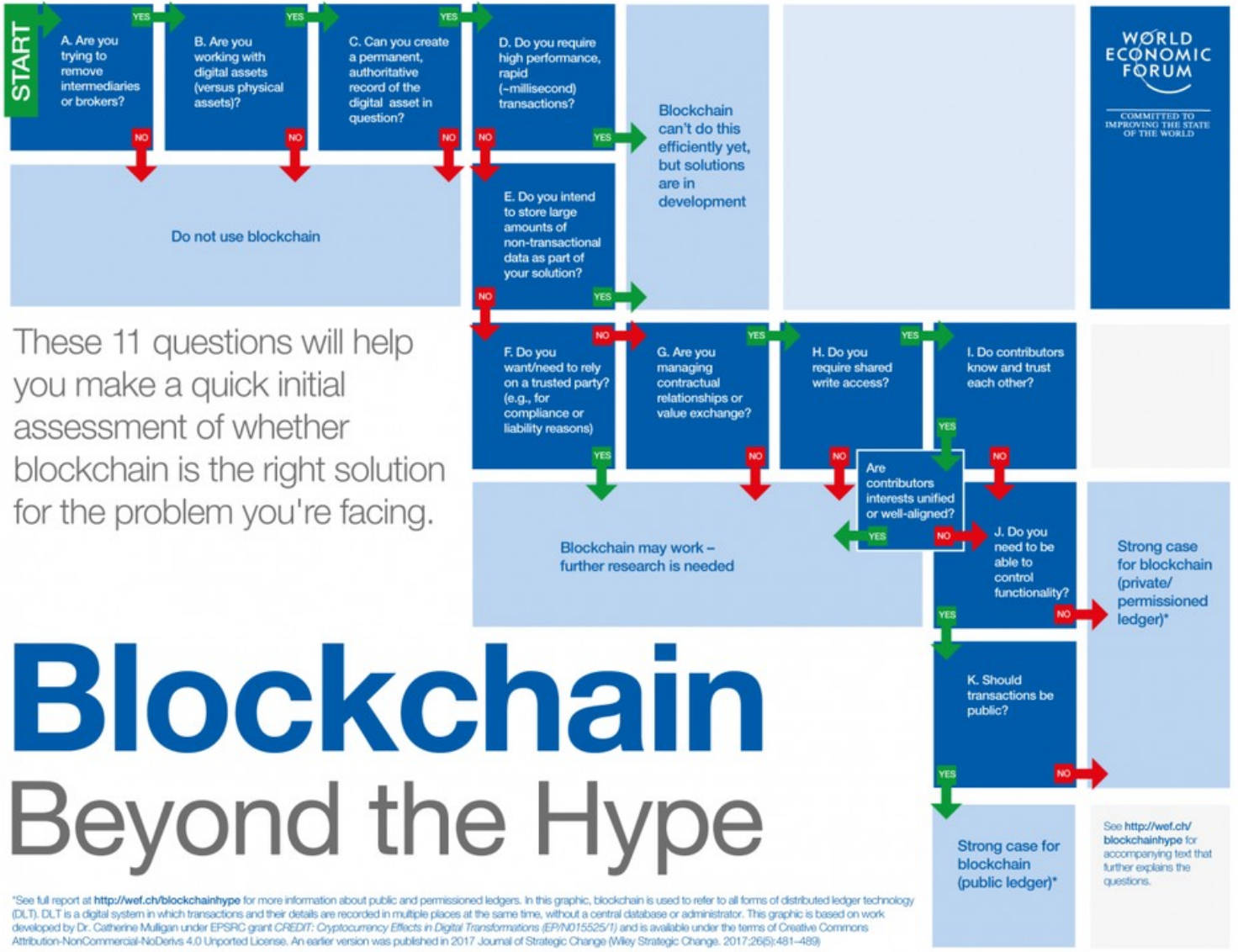
Notaries

Zentralisierung

Wann ist Blockchain sinnvoll?



David Birch Blockchain Decision Model – https://twitter.com/dgwbirch/status/757976191487934464



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.

Blockchain

Beyond the Hype

See http://wef.ch/blockchainhype for accompanying text that further explains the questions.

*See full report at **http://wef.ch/blockchainhype** for more information about public and permissioned ledgers. In this graphic, blockchain is used to refer to all forms of distributed ledger technology (DLT). DLT is a digital system in which transactions and their details are recorded in multiple places at the same time, without a central database or administrator. This graphic is based on work developed by Dr. Catherine Mulligan under EPSRC grant *CREDIT: Cryptocurrency Effects in Digital Transformations (EP/N015525/1)* and is available under the terms of Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Unported License. An earlier version was published in 2017 Journal of Strategic Change (Wiley Strategic Change. 2017;26(5):481–489)

Dezentralisierung

Disintermediation

Gründe für Blockchain

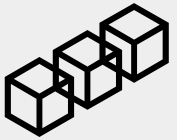
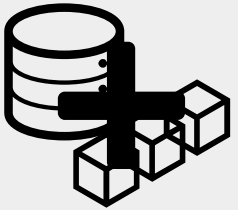
- Notwendigkeit Zustand zu speichern
- Geteilter Schreibzugriff
- Interaktion zwischen Transaktionen
- Kein Vertrauen zwischen den Parteien
- Kein vertrauter Intermediär
- Marketing

Konnten wir das Problem auch schon vor Blockchain lösen?

Können wir das Problem mit Blockchain 10x besser lösen?

Manipulationssicherung privater Datenbanken mittels öffentlicher Blockchains

Warum?

	Blockchain	Datenbank	Kombination
			
Manipulationssicherheit	✓		✓
Datenschutz		✓	✓
Kosten		✓	✓
Performance		✓	✓

Wie?

1. **Daten → Hash**
2. **Hash → Blockchain**
3. **fertig**

Transaction View information about a bitcoin transaction

a83b021fb1033c65749416831a4f52a5a4cae970fa94e1e92a5df4cac41bee39

3KaDVRxq7NjFLBkU82qdLLL9KhodzsfoXV (0.00442736 BTC - Output)	1734HkZaKJqCoA3utLTmYs8Kr5TcG55RMB - (Unspent)	0.00002 BTC
	3KaDVRxq7NjFLBkU82qdLLL9KhodzsfoXV - (Spent)	0.00438536 BTC
	Unable to decode output address - (Unspent)	0 BTC
		0.00440536 BTC

Summary	
Size	341 (bytes)
Weight	1037
Received Time	2018-04-06 21:55:50
Included In Blocks	516948 (2018-04-06 22:01:46 + 6 minutes)
Confirmations	5602 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.00442736 BTC
Total Output	0.00440536 BTC
Fees	0.000022 BTC
Fee per byte	6.452 sat/B
Fee per weight unit	2.122 sat/WU
Estimated BTC Transacted	0 BTC
Scripts	Hide scripts & coinbase

Input Scripts

ScriptSig: PUSHDATA(22)[0014...
Witness:
02473044022061f7f2d54b...9262ca...

Output Scripts

DUP HASH160 PUSHDATA(20)[423454fd267102b0ba7d5d14e20f0127fca30e7a] EQUALVERIFY CHECKSIG

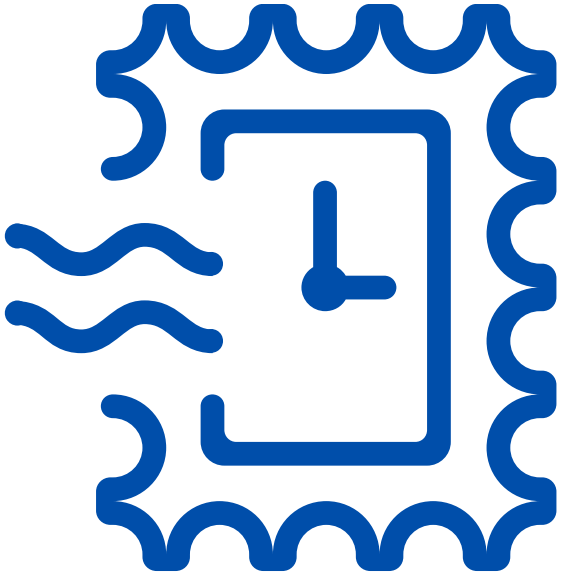
HASH160 PUSHDATA(20)[c429020f059f5cf91a69baad624dc480e5169cbc] EQUAL

RETURN
PUSHDATA1[2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e536565207468652066756...
(decoded) .....See the full picture at TDAmeritrade.com/Blockchain.....

RETURN
PUSHDATA1[2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e536565207468652066
(decoded) .....See the full picture at TDAmeritrade.com/Blockchain

Verifizierung

1. **Daten → Hash**
2. **Blockchain → Hash**
3. **Vergleich**



OpenTimestamps

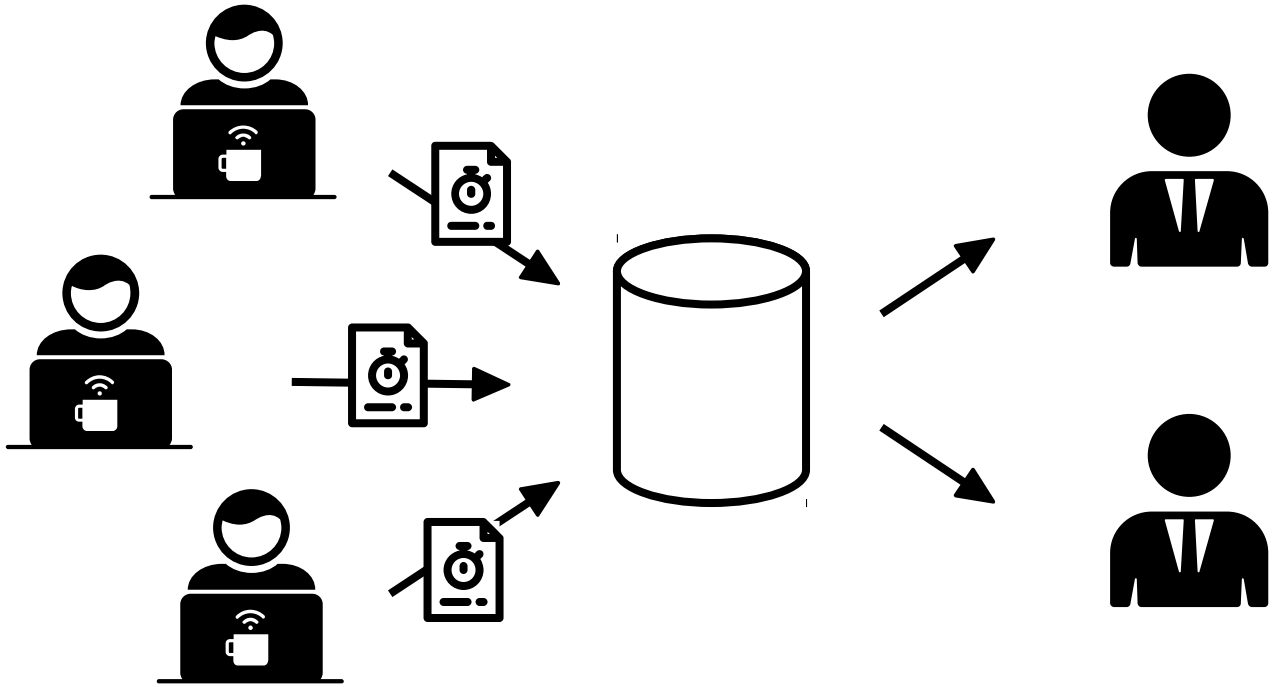
OpenTimestamps

```
const detached = OpenTimestamps.DetachedTimestampFile
    .fromBytes(new OpenTimestamps.Ops.OpSHA256(), buffer);

OpenTimestamps.stamp(detached).then(() => {
    const fileOts = detached.serializeToBytes();
});
```

Beispiel:
Zeitbuchung für Freelancer

Beispiel:
Zeitbuchung für Freelancer

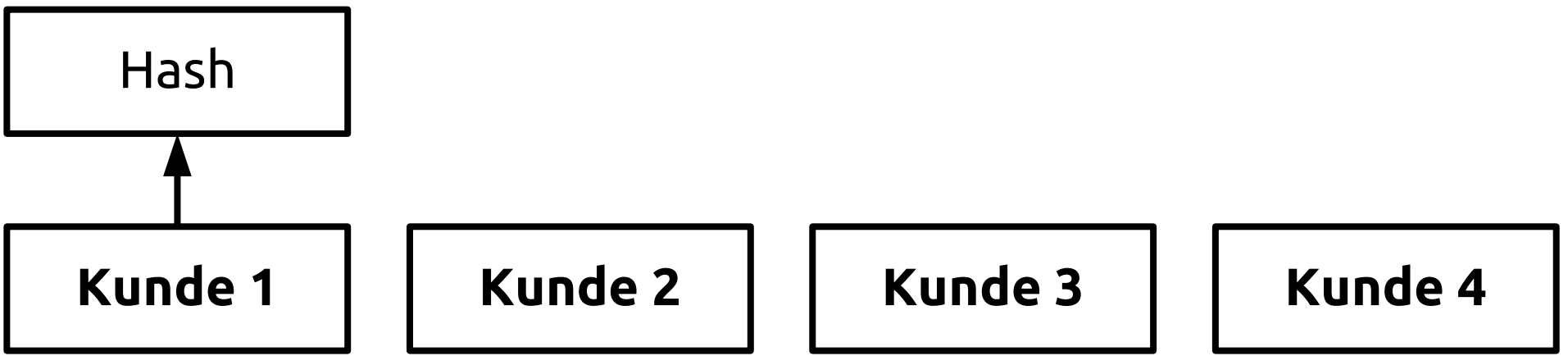


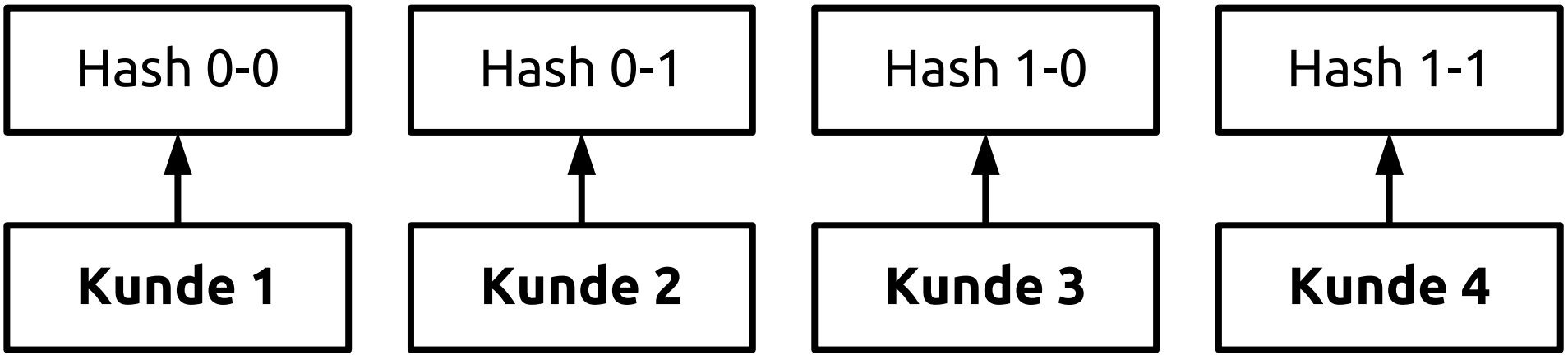
Datenschutz

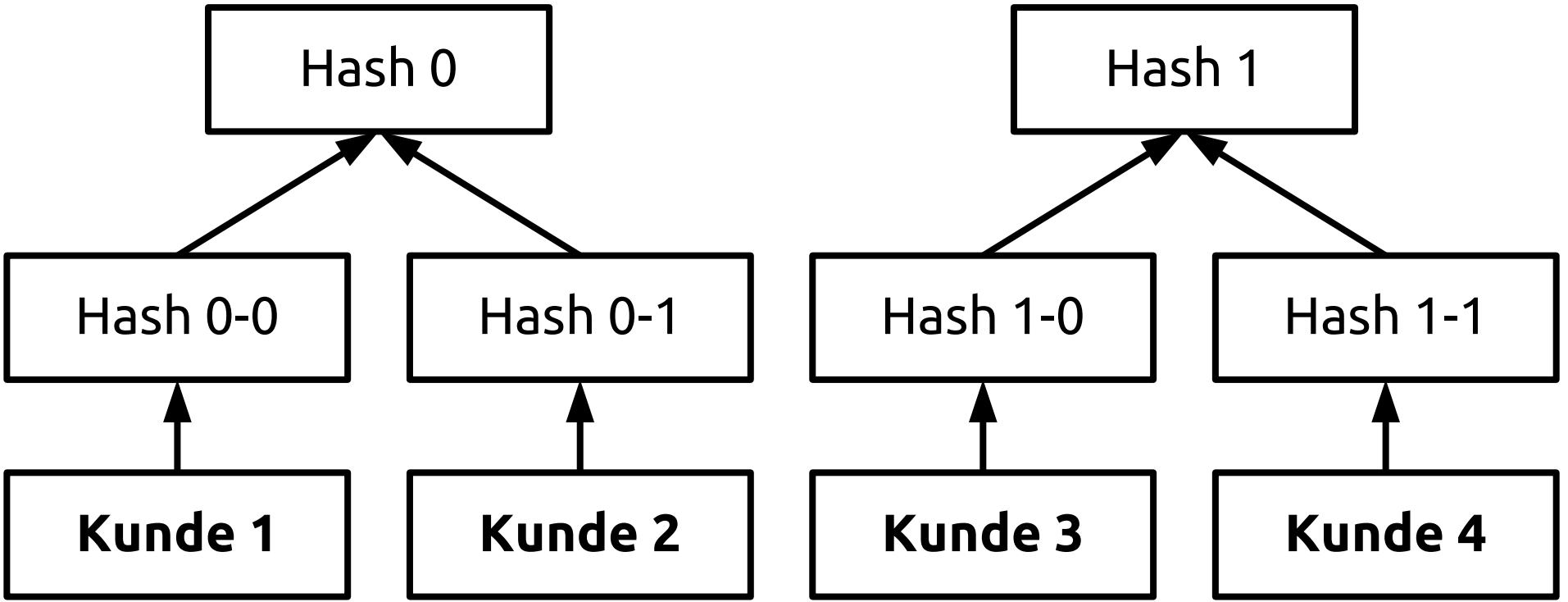
Daten veröffentlichen?

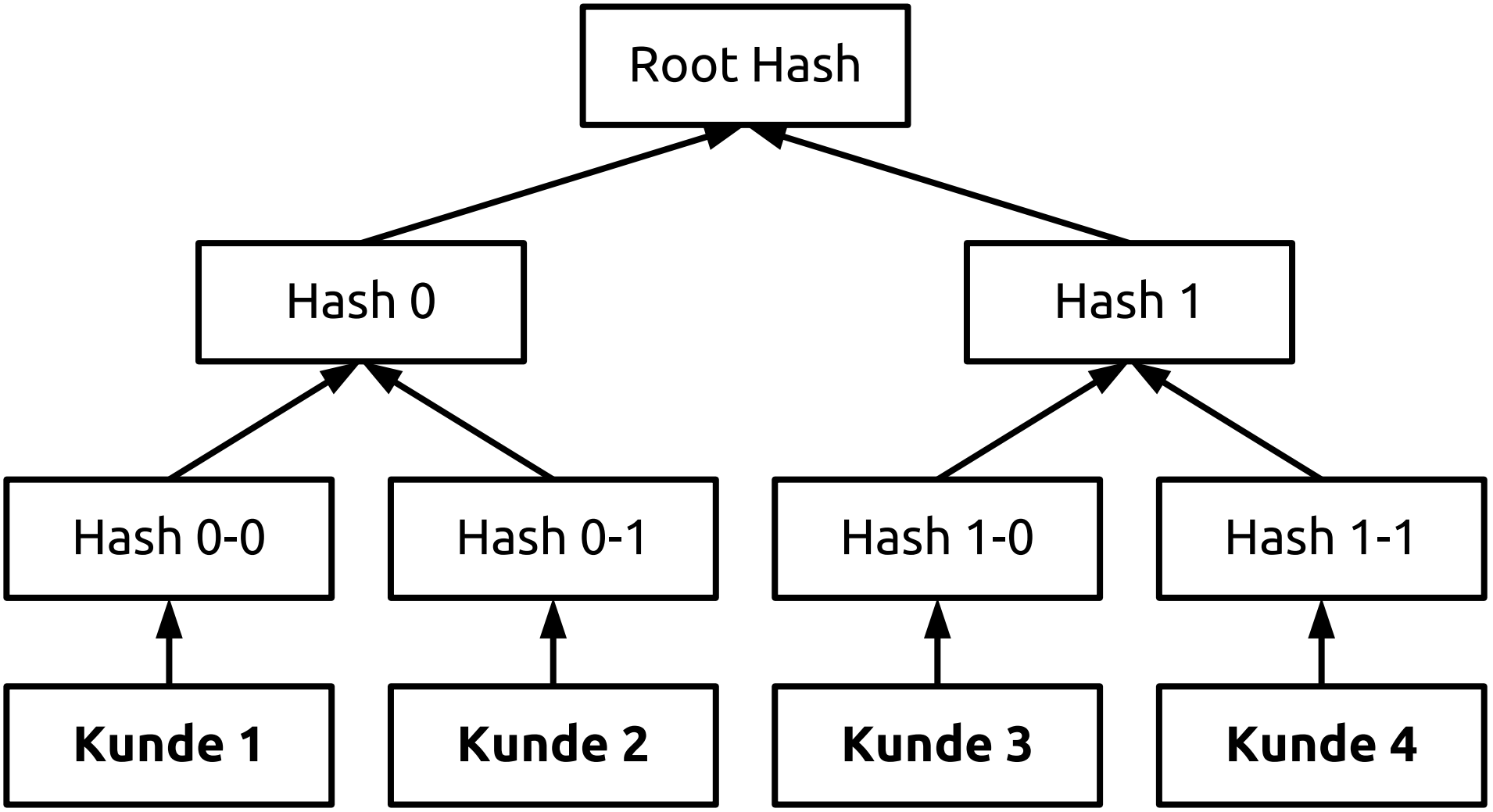
Hash-Baum

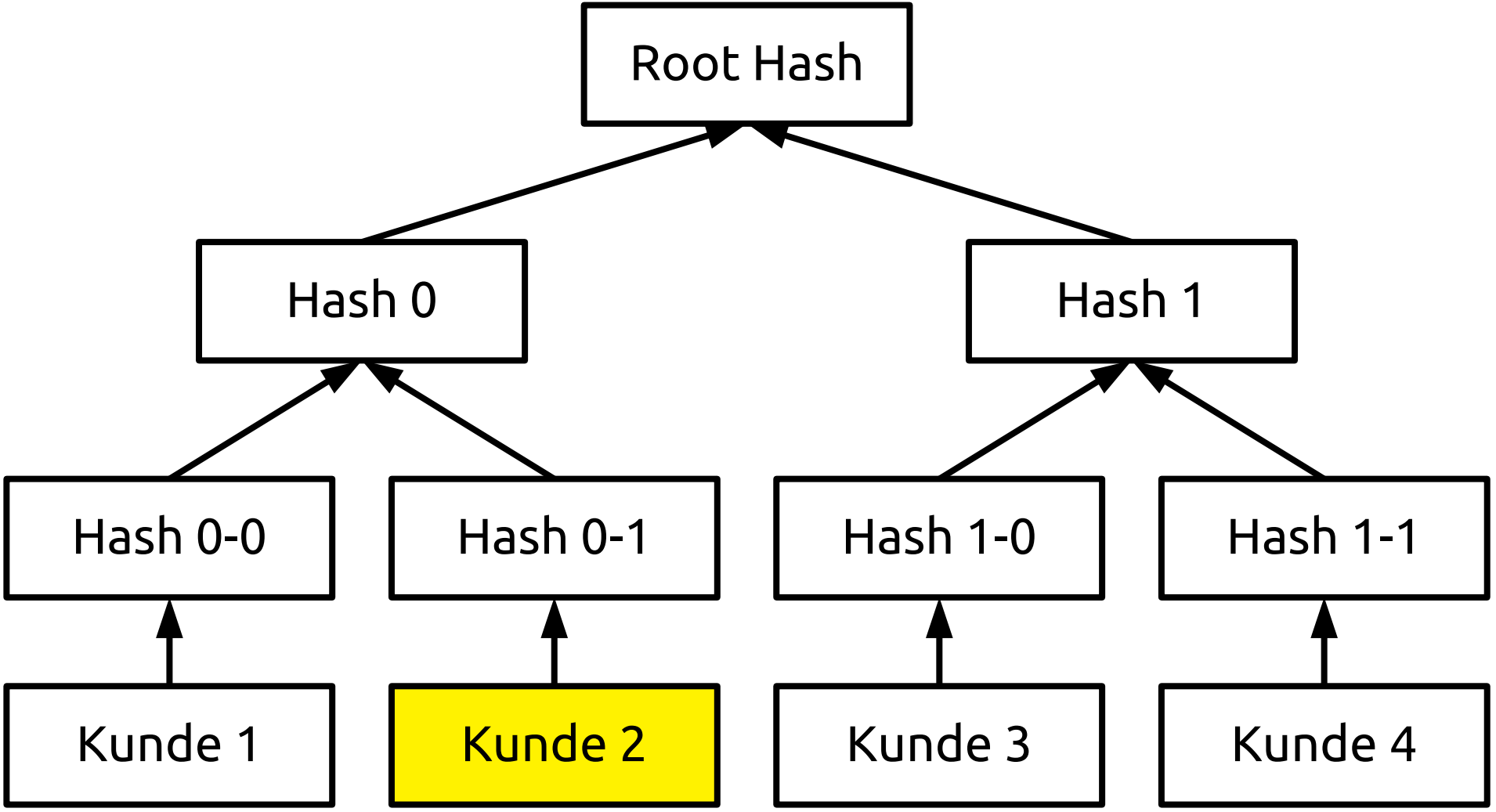
Merkle-Tree

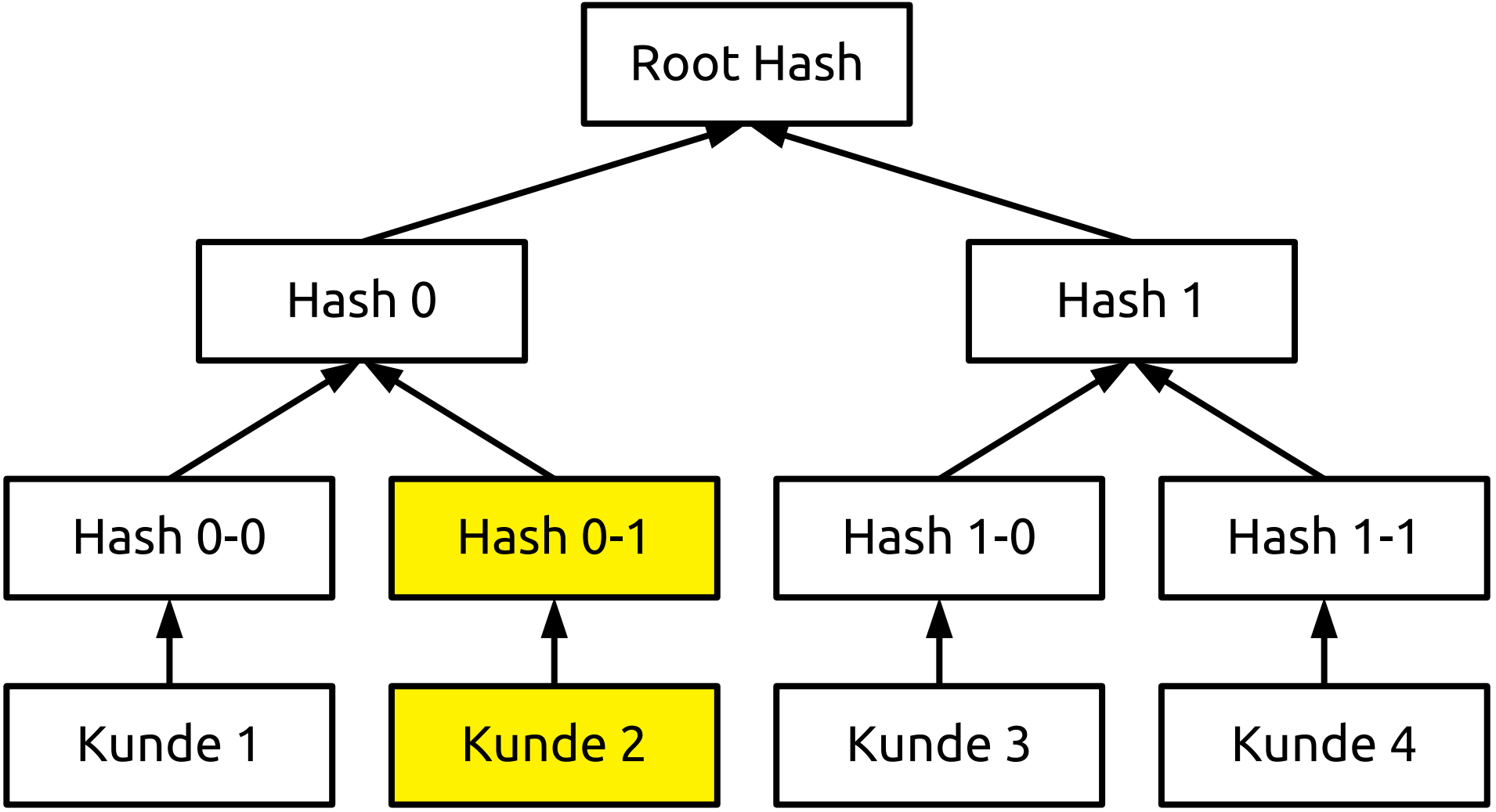

Hash
Kunde 1
Kunde 2
Kunde 3
Kunde 4

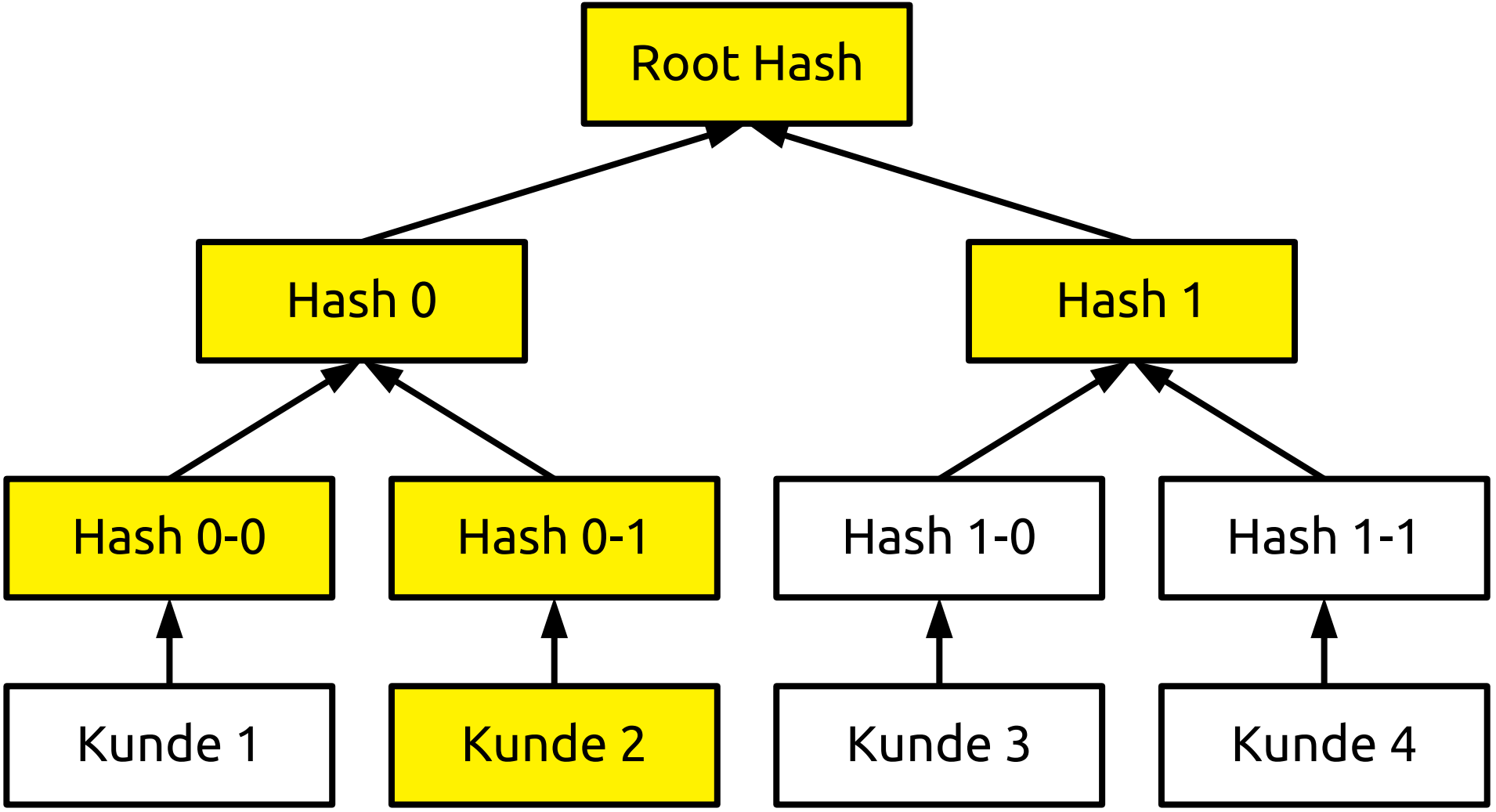

Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde 3
Kunde 4


Hash 0
Hash 1
Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde 3
Kunde 4

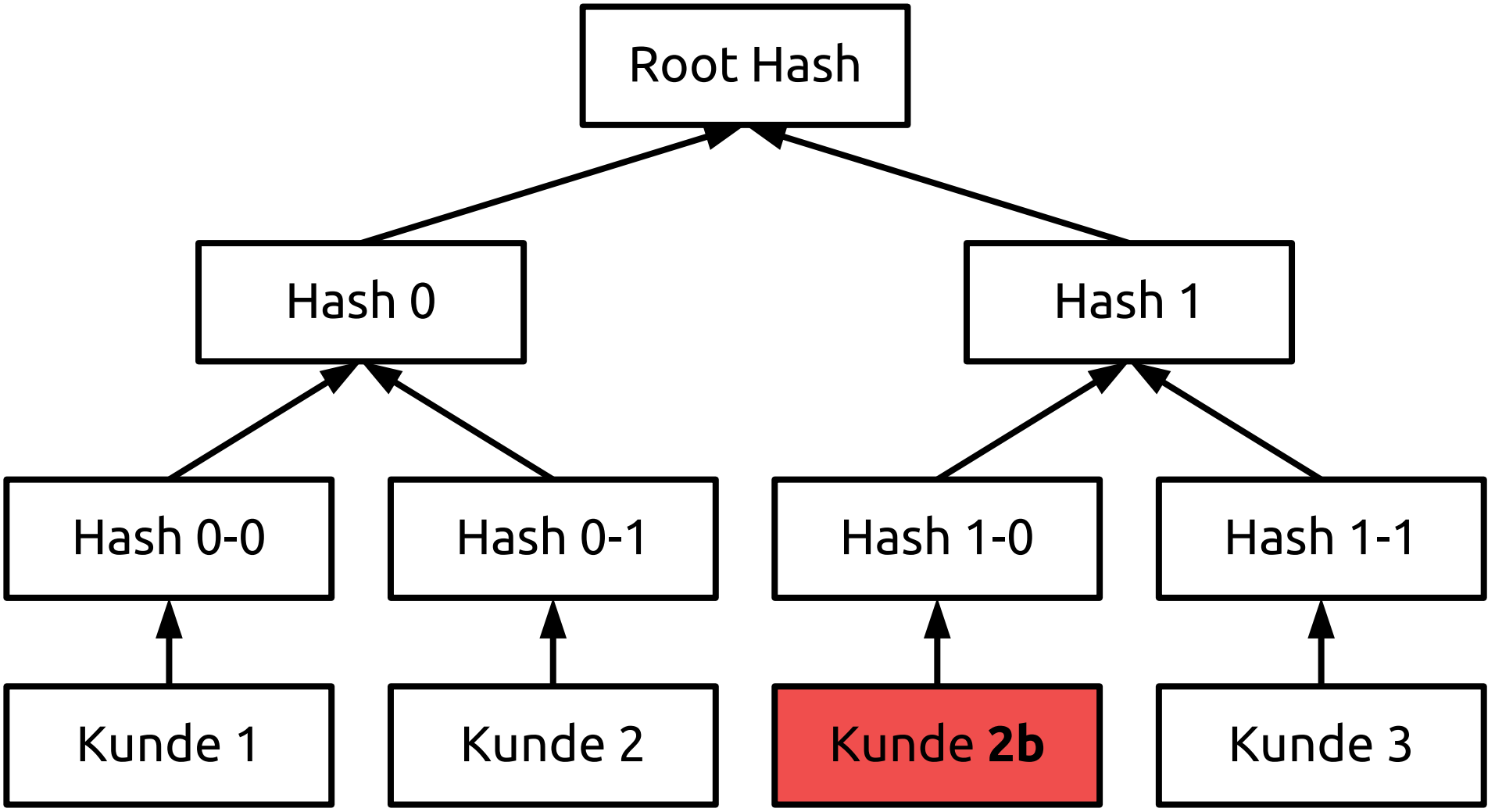

Root Hash
Hash 0
Hash 1
Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde 3
Kunde 4

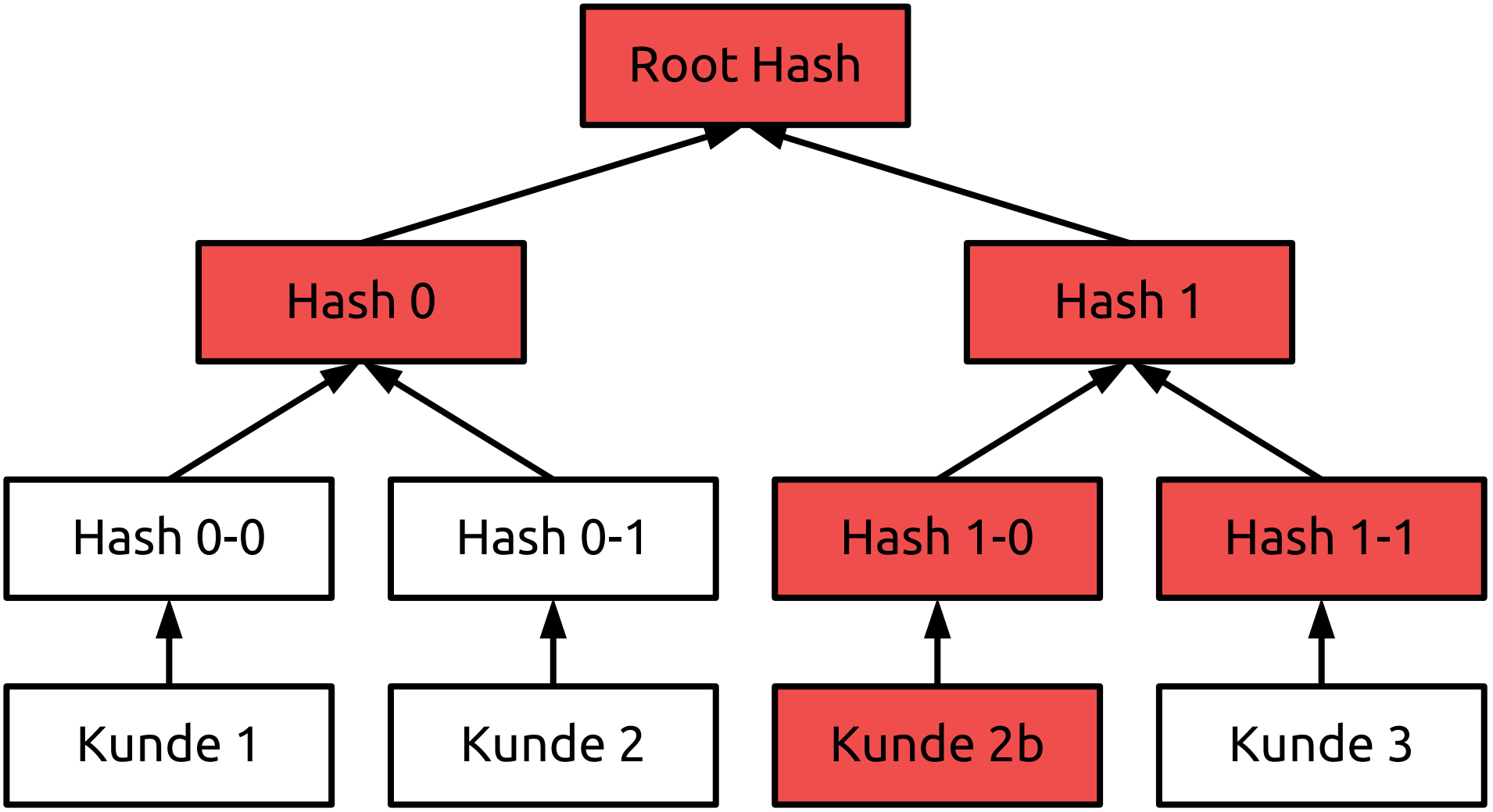

Root Hash
Hash 0
Hash 1
Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde 3
Kunde 4

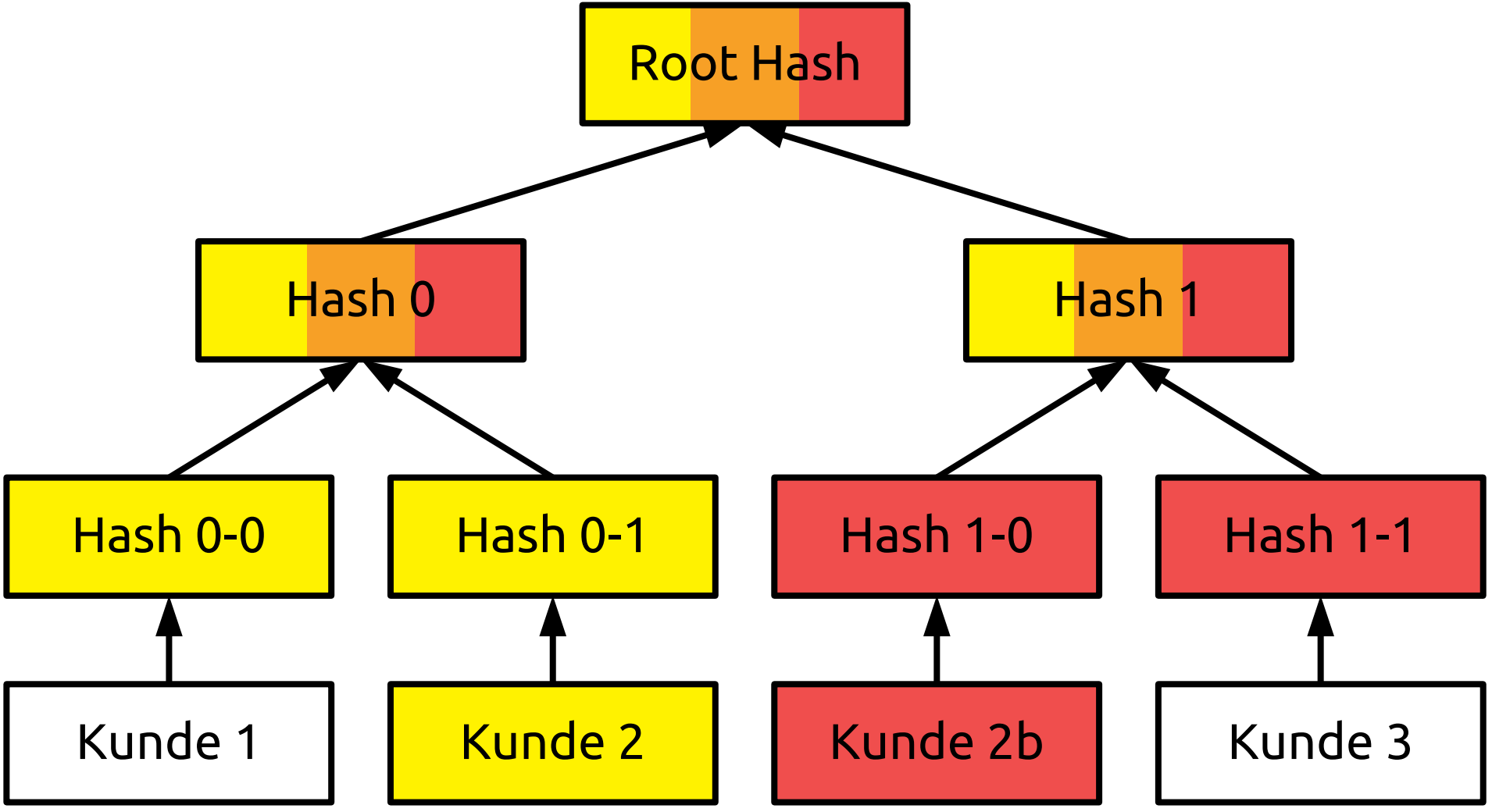

Root Hash
Hash 0
Hash 1
Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde 3
Kunde 4

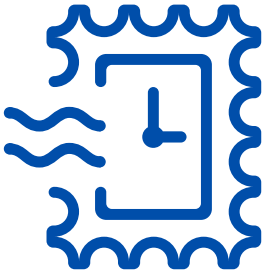

Root Hash
Hash 0
Hash 1
Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde 3
Kunde 4

Datenschutz


Root Hash
Hash 0
Hash 1
Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde **2b**
Kunde 3


Root Hash
Hash 0
Hash 1
Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde 2b
Kunde 3


Root Hash
Hash 0
Hash 1
Hash 0-0
Hash 0-1
Hash 1-0
Hash 1-1
Kunde 1
Kunde 2
Kunde 2b
Kunde 3



Existenzbeweis

Kein Beweis der Nicht-Existenz

Ein Ort
für die gesamte Wahrheit


ethereum

Smart Contracts

“Smart Contracts”

World Computer

browser
ballot.sol

config

```solidity
pragma solidity ^0.4.0;
contract Ballot {

    struct Voter {
        uint weight;
        bool voted;
        uint8 vote;
        address delegate;
    }
    struct Proposal {
        uint voteCount;
    }

    address chairperson;
    mapping(address => Voter) voters;
    Proposal[] proposals;

    /// Create a new ballot with $(_numProposals) different proposals.
    constructor(uint8 _numProposals) public {
        chairperson = msg.sender;
        voters[chairperson].weight = 1;
        proposals.length = _numProposals;
    }

    /// Give $(voter) the right to vote on this ballot.
    /// May only be called by $(chairperson).
    function giveRightToVote(address voter) public {
        if (msg.sender != chairperson || voters[voter].voted) return;
        voters[voter].weight = 1;
    }

    /// Delegate your vote to the voter $(to).
    function delegate(address to) public {
        Voter storage sender = voters[msg.sender]; // assigns reference
        if (sender.voted) return;
        while (voters[to].delegate != address(0) && voters[to].delegate != msg.sender)
            to = voters[to].delegate;
        if (to == msg.sender) return;
        sender.voted = true;
        sender.delegate = to;
        Voter storage delegateTo = voters[to];
        if (delegateTo.voted)
            proposals[delegateTo.vote].voteCount += sender.weight;
        else
            delegateTo.weight += sender.weight;
```

Environment: JavaScript VM

Account: 0xca3...a733c (99.999999999

Gas limit: 3000000

Value: 0

Ballot

uint8 _numProposals | Create

Load contract from Add | At Address

0 pending transactions

Ballot at 0x692...77b3a (memory)

delegate	address to
giveRightToVote	address voter
vote	uint8 proposal
winningProposal	

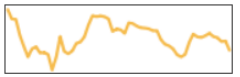
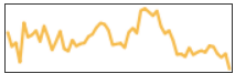
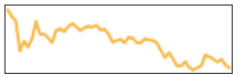
[2] only remix transactions, script | Search transactions | Listen on network

ERC20 Token Standard

```
contract ERC20 {
    function totalSupply() constant returns (uint totalSupply);
    function balanceOf(address _owner) constant returns (uint balance);
    function transfer(address _to, uint _value) returns (bool success);
    function transferFrom(address _from, address _to, uint _value) returns (bool success);
    function approve(address _spender, uint _value) returns (bool success);
    function allowance(address _owner, address _spender) constant returns (uint remaining);
    event Transfer(address indexed _from, address indexed _to, uint _value);
    event Approval(address indexed _owner, address indexed _spender, uint _value);
}
```

Top 100 Tokens by Market Capitalization

Cryptocurrencies Watchlist USD Next 100 → View All

#	Name	Platform	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	EOS	Ethereum	$11,042,096,037	$12.80	$1,565,480,000	862,697,452	3.52%	
2	TRON	Ethereum	$4,445,361,325	$0.067612	$303,589,000	65,748,111,645	-4.21%	
3	Tether	Omni	$2,306,743,985	$0.999828	$2,837,440,000	2,307,140,814	-0.21%	
4	VeChain	Ethereum	$2,204,447,352	$4.19	$88,208,100	526,019,398	-8.30%	
5	Binance Coin	Ethereum	$1,437,365,016	$12.60	$47,274,600	114,041,290	3.58%	
6	ICON	Ethereum	$1,405,301,287	$3.63	$33,572,200	387,231,348	-4.83%	
7	OmiseGO	Ethereum	$1,298,828,212	$12.73	$34,854,500	102,042,552	-1.50%	
8	Zilliqa	Ethereum	$1,010,985,814	$0.138739	$72,441,800	7,286,961,952	0.34%	
9	Aeternity	Ethereum	$904,527,218	$3.88	$23,716,600	233,020,472	0.08%	

Smart Contracts

Oracles

Photo by Jamie Street on Unsplash

Ein Ort
für die gesamte Wahrheit

```
contract HashStore is owned {
    mapping(uint256 => bytes32) public storedHashes;

    function storeHash(uint256 stakeholderId, bytes32 hash)
        ownerOnly external
    {
        storedHashes[stakeholderId] = hash;
    }
}
```

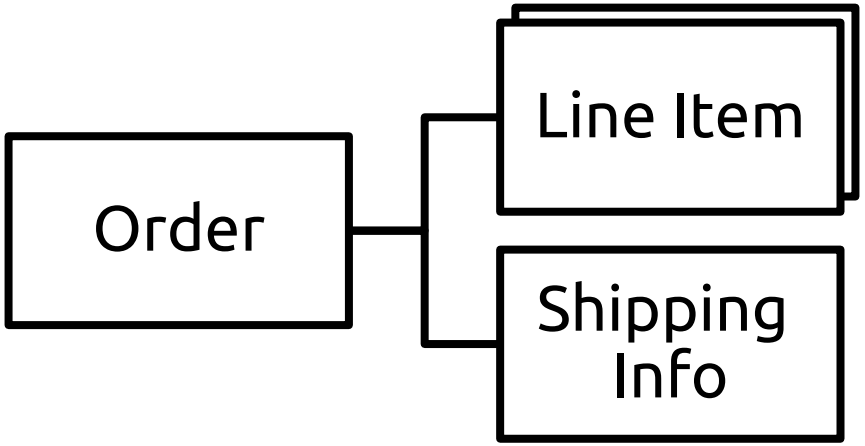
Beweis der Nicht-Existenz

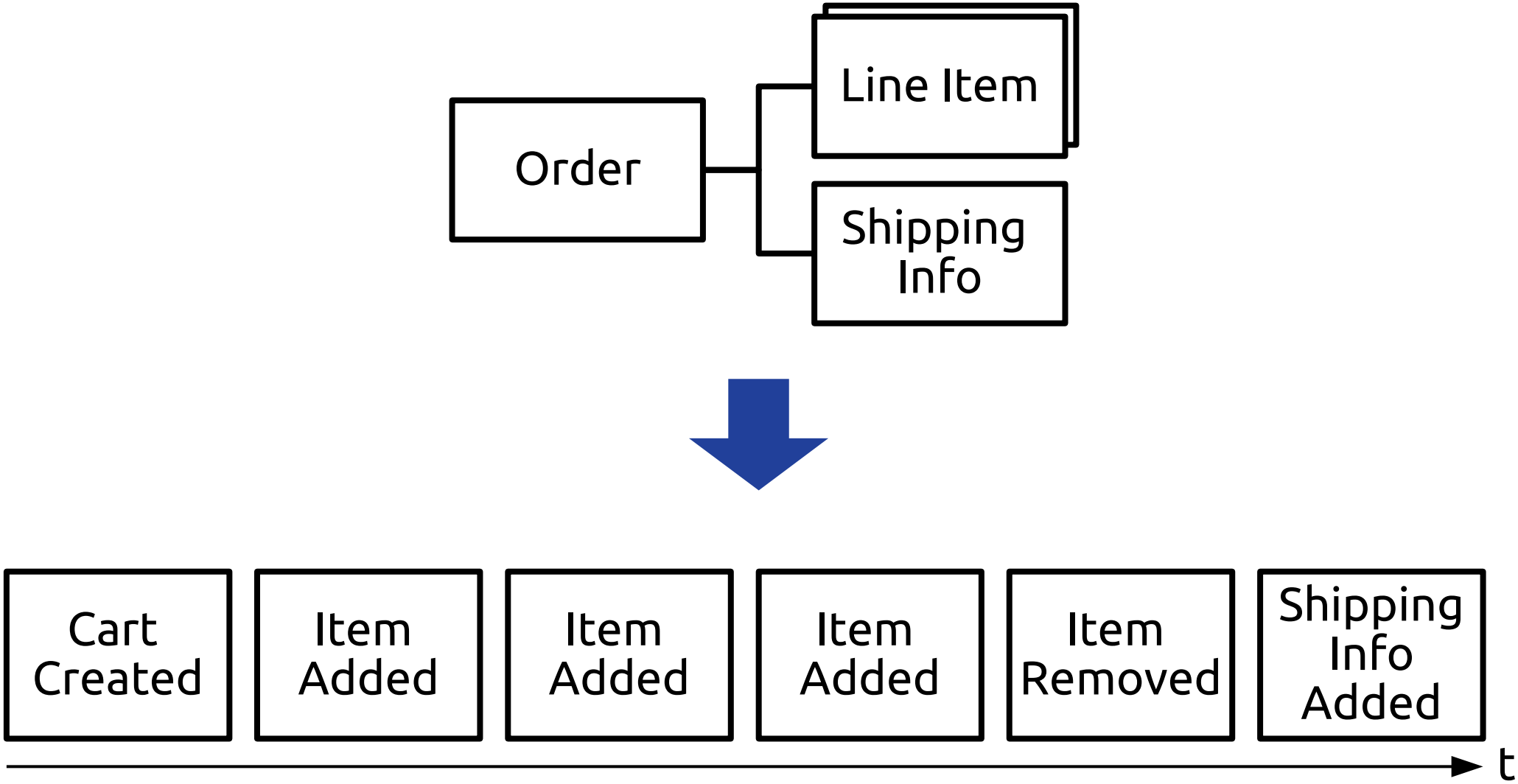
Jeder Zustand des Systems

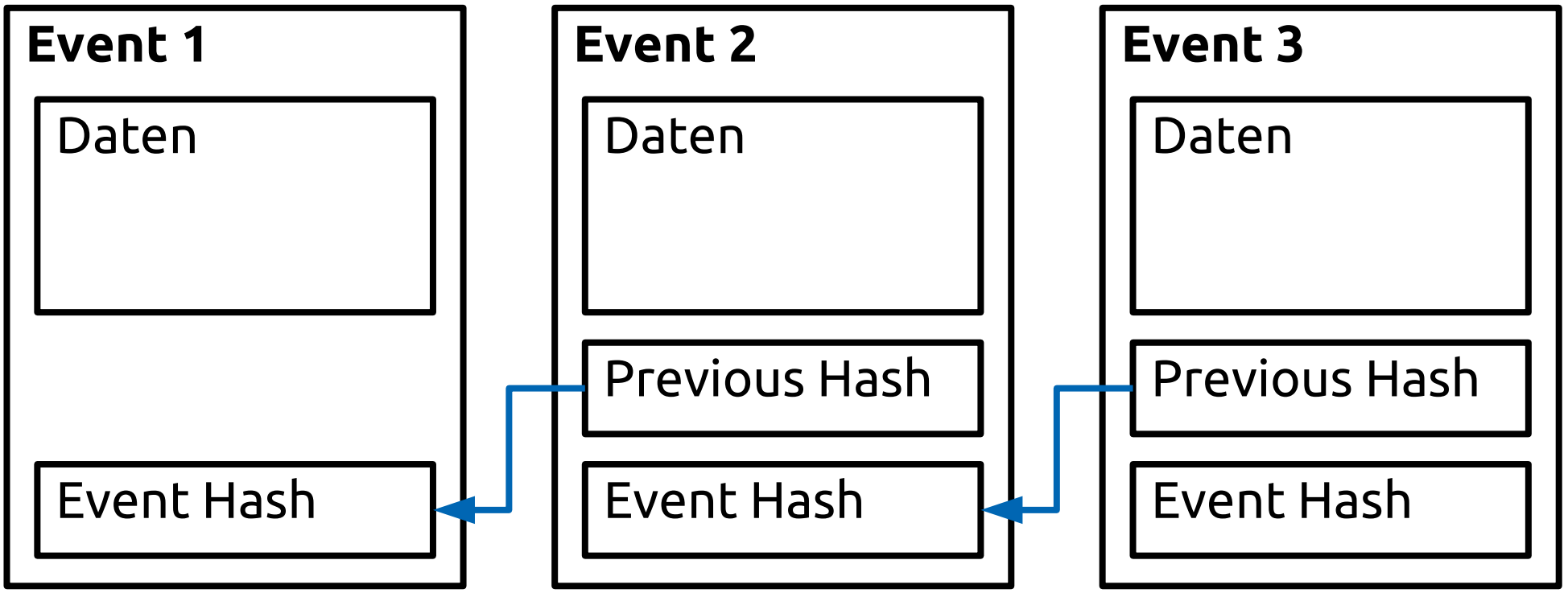
Versionierung

Append-Only

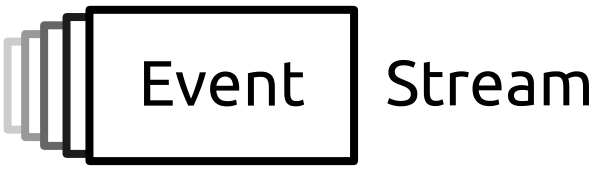
Event Sourcing

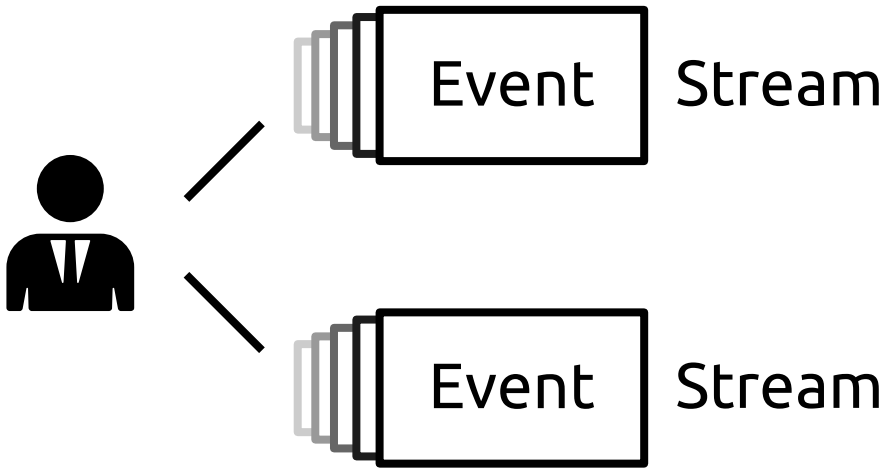

Order
Line Item
Shipping Info

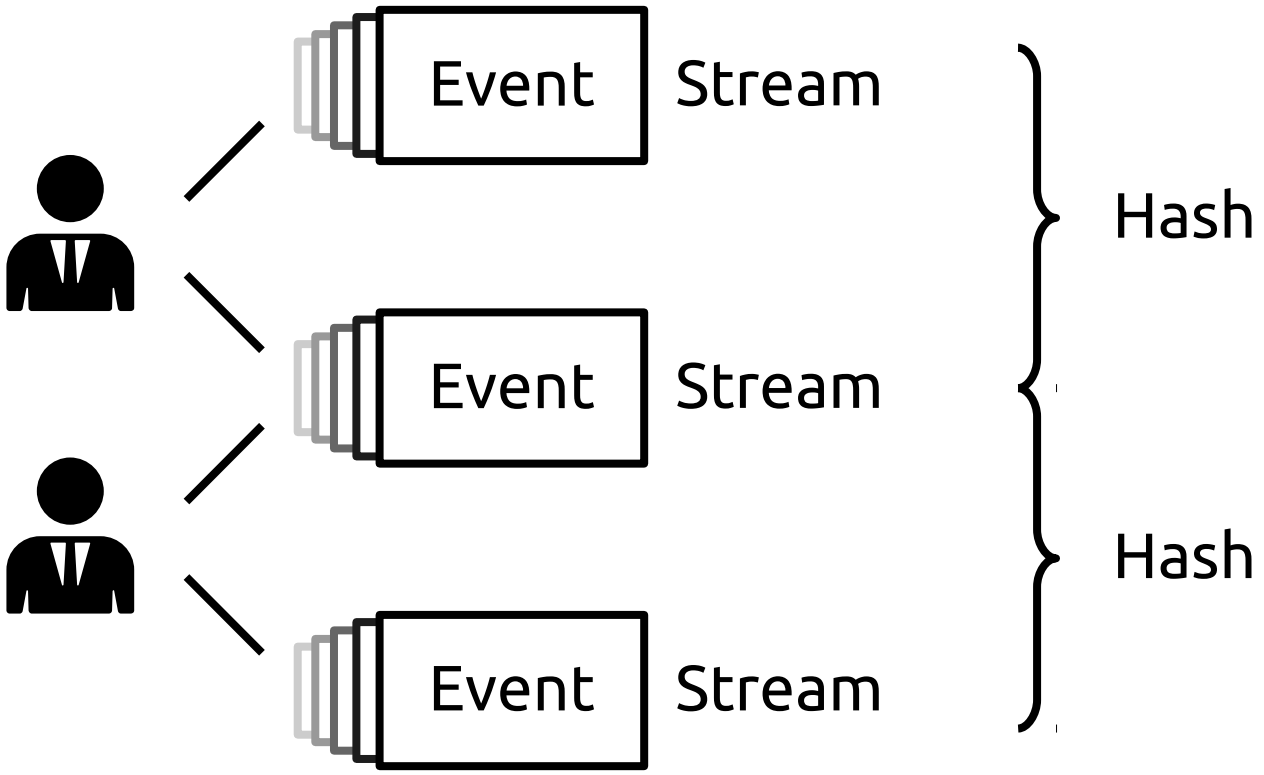

Order
Line Item
Shipping Info
Cart Created
Item Added
Item Added
Item Added
Item Removed
Shipping Info Added
t

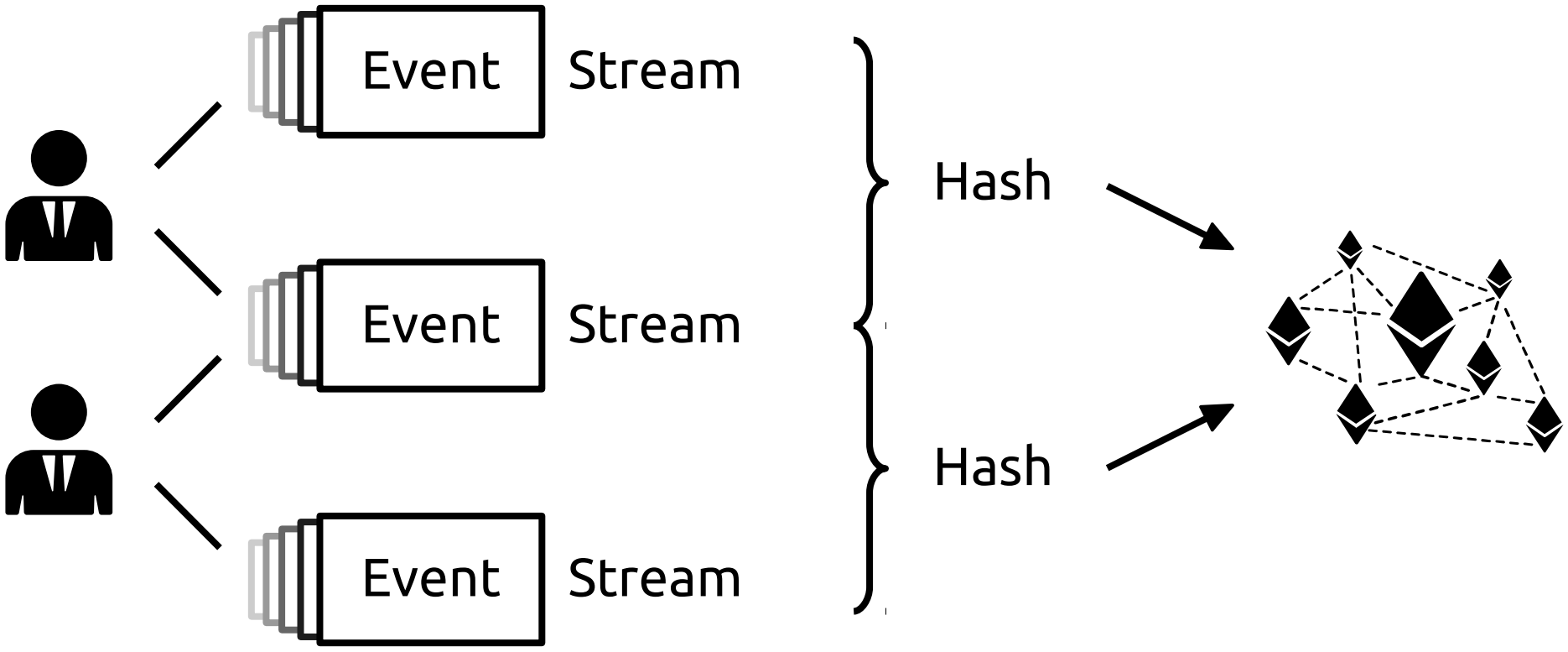

Event 1
Daten
Event Hash
Event 2
Daten
Previous Hash
Event Hash
Event 3
Daten
Previous Hash
Event Hash

Jeder Zustand des Systems


Event
Stream


Event
Stream
Event
Stream


Event
Stream
Event
Stream
Event
Stream
Hash
Hash


Event
Stream
Event
Stream
Event
Stream
Hash
Hash

Encoding

Signaturen

GDPR