

Architecting the Blockchain for Failure



Conor Svensson
@conors10



blk.io Founder
web3j Author



**Enterprise Technology
(Established)**



**Blockchain Technology
(Emergent)**

The Enterprise Ethereum Alliance

accenture



ANDLI安兑

BBVA



BlockApps



BNY MELLON

CME Group



CONSENSYS



CHRONICLED

CREDIT SUISSE



富邦金控 Fubon Financial



IC3 The Initiative For
CryptoCurrencies & Contracts

ING



The Institutes[®]
RISK & INSURANCE
KNOWLEDGE GROUP



J.P.Morgan



MONAX
INDUSTRIES



THOMSON REUTERS

Santander

string

telindus
powered by tongos

Tendermint

UBS



Agenda

Ethereum & web3j

Failure in Ethereum

Distributed Consensus

Consensus in Ethereum

- Public Network Consensus
- Consortium Network Consensus

Architecting the Blockchain for Failure

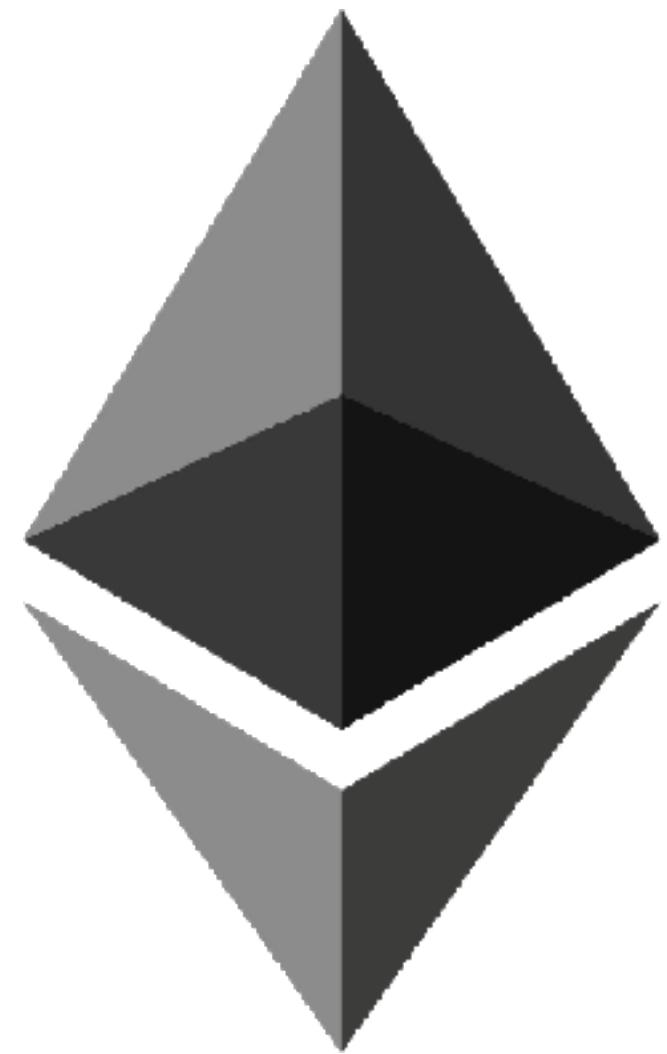
Ethereum & web3j

Failure in Ethereum

Distributed Consensus

Consensus in Ethereum

- Public Network Consensus
- Consortium Network Consensus



Ether the Cryptocurrency

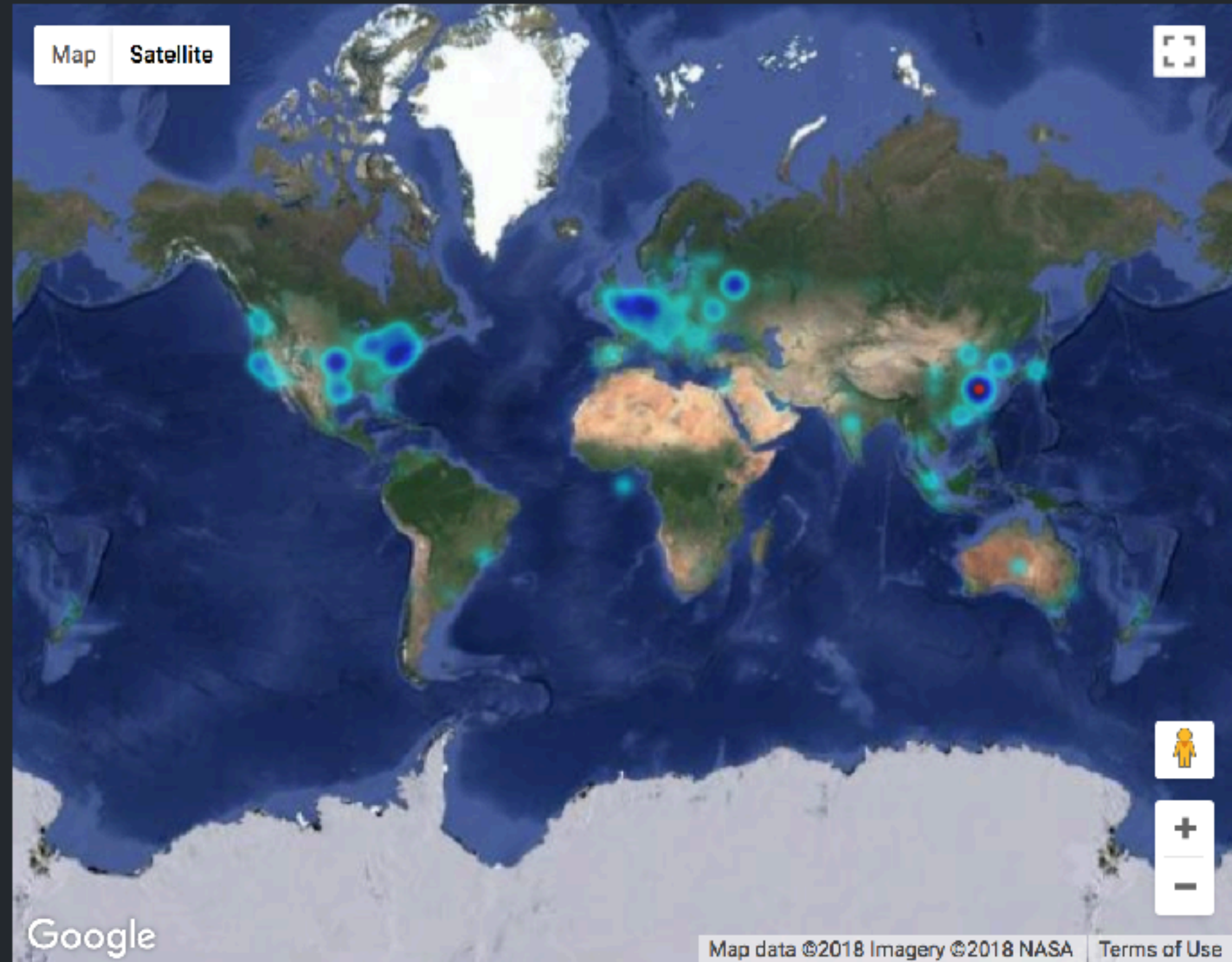


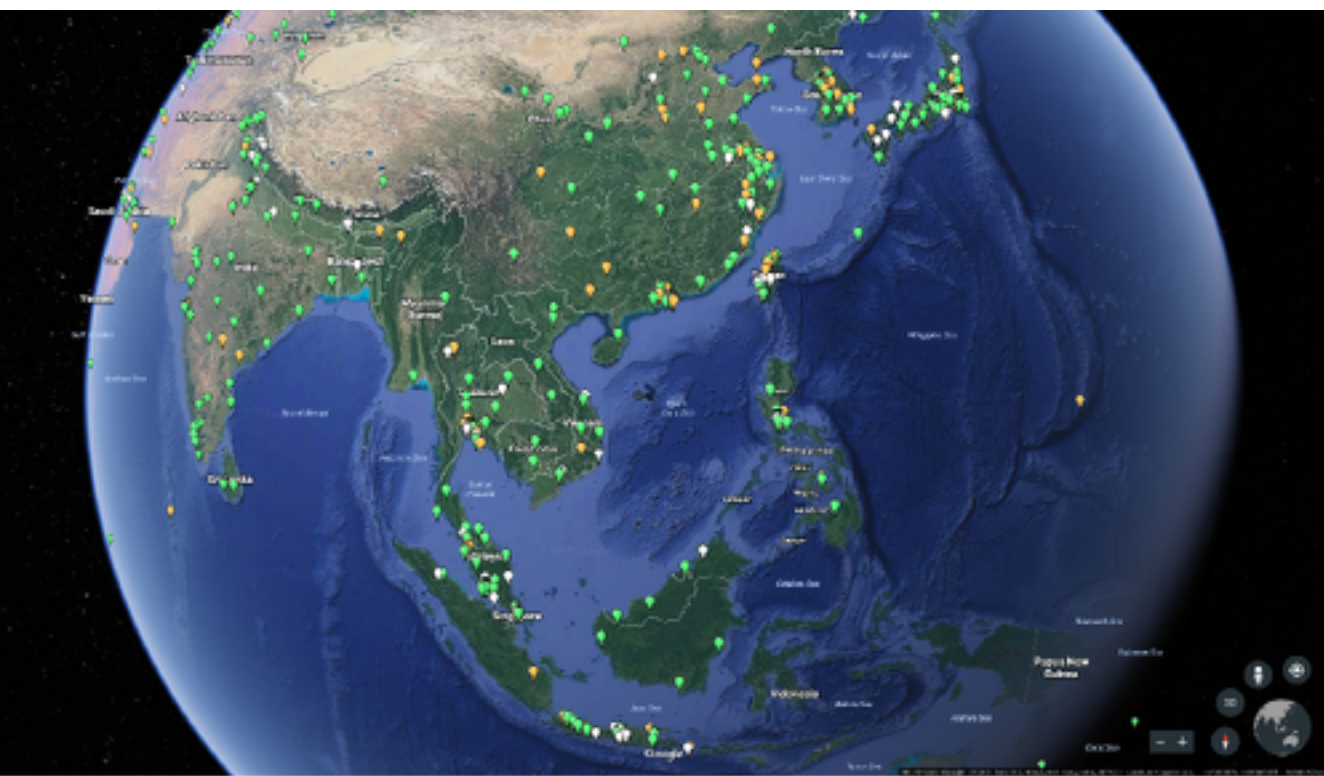
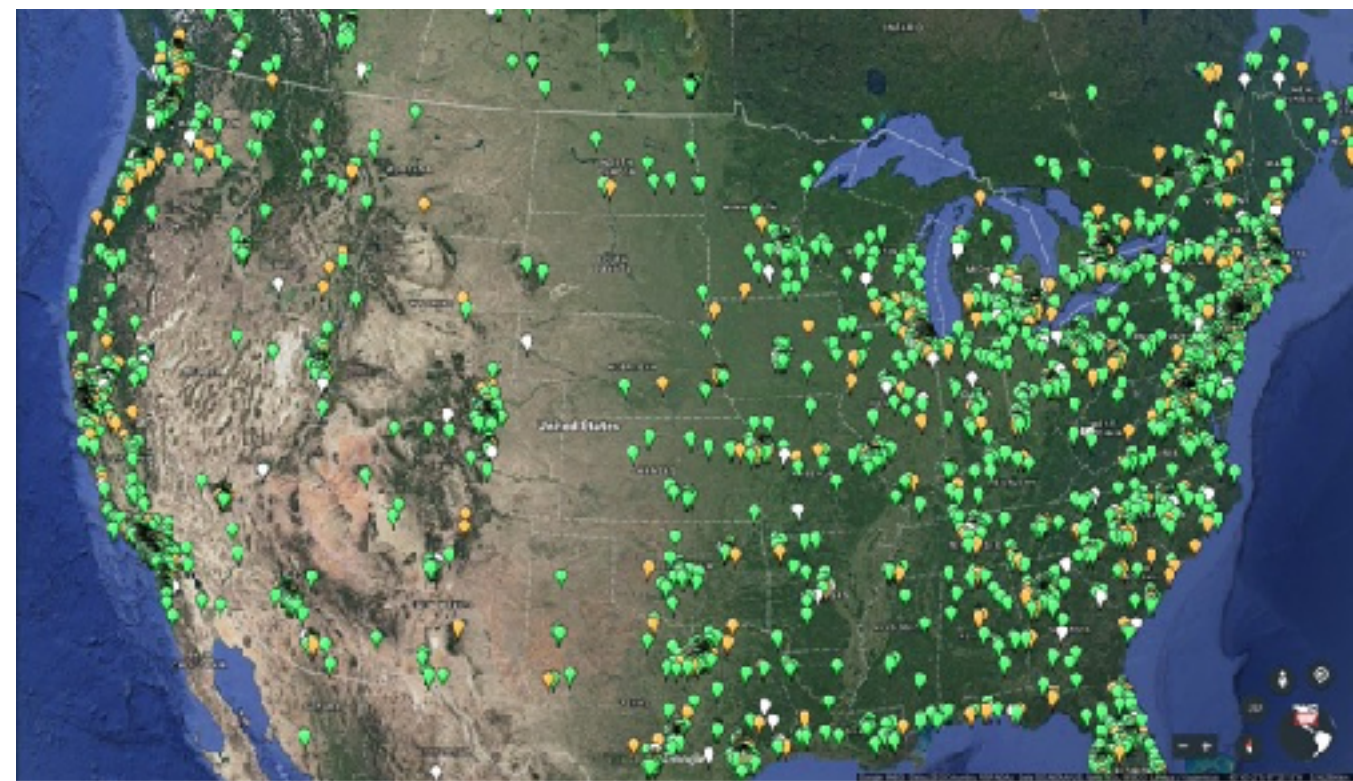
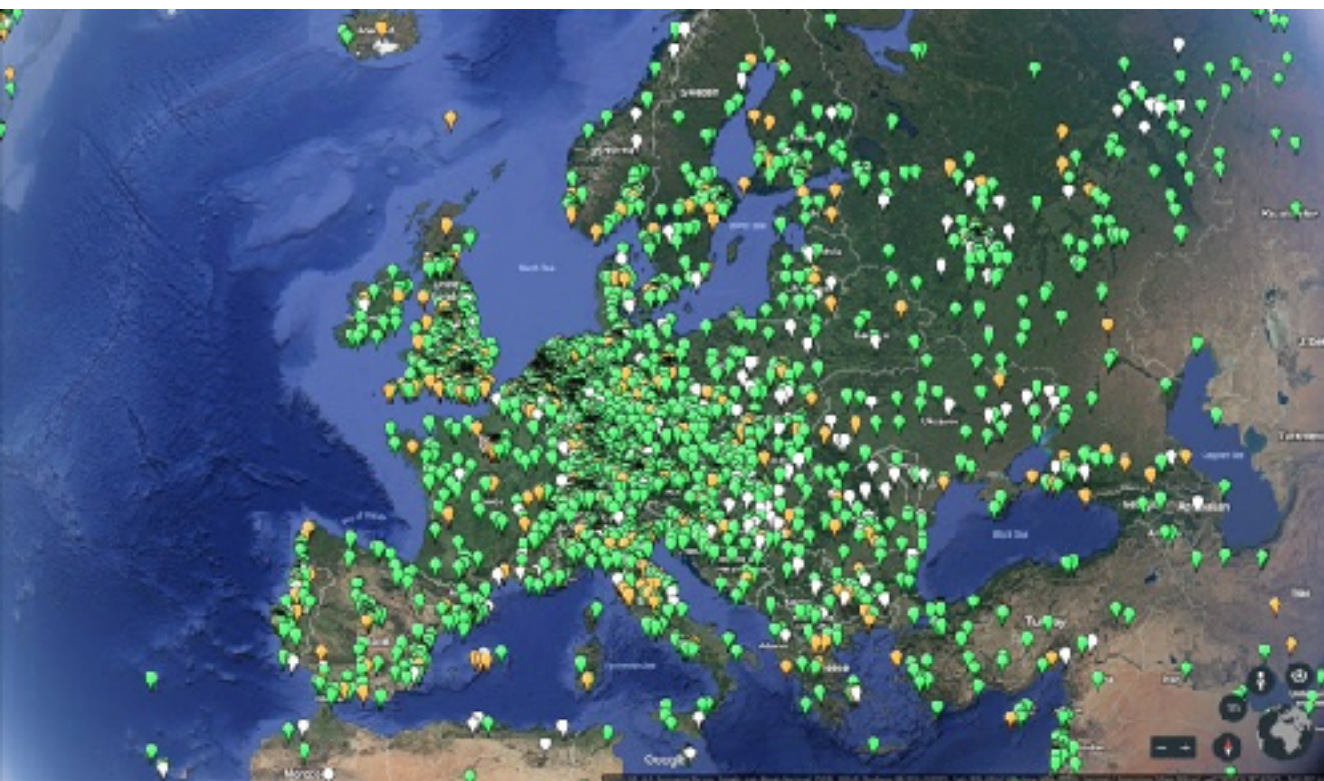
ETH pricing in effect

The World Computer

COUNTRIES

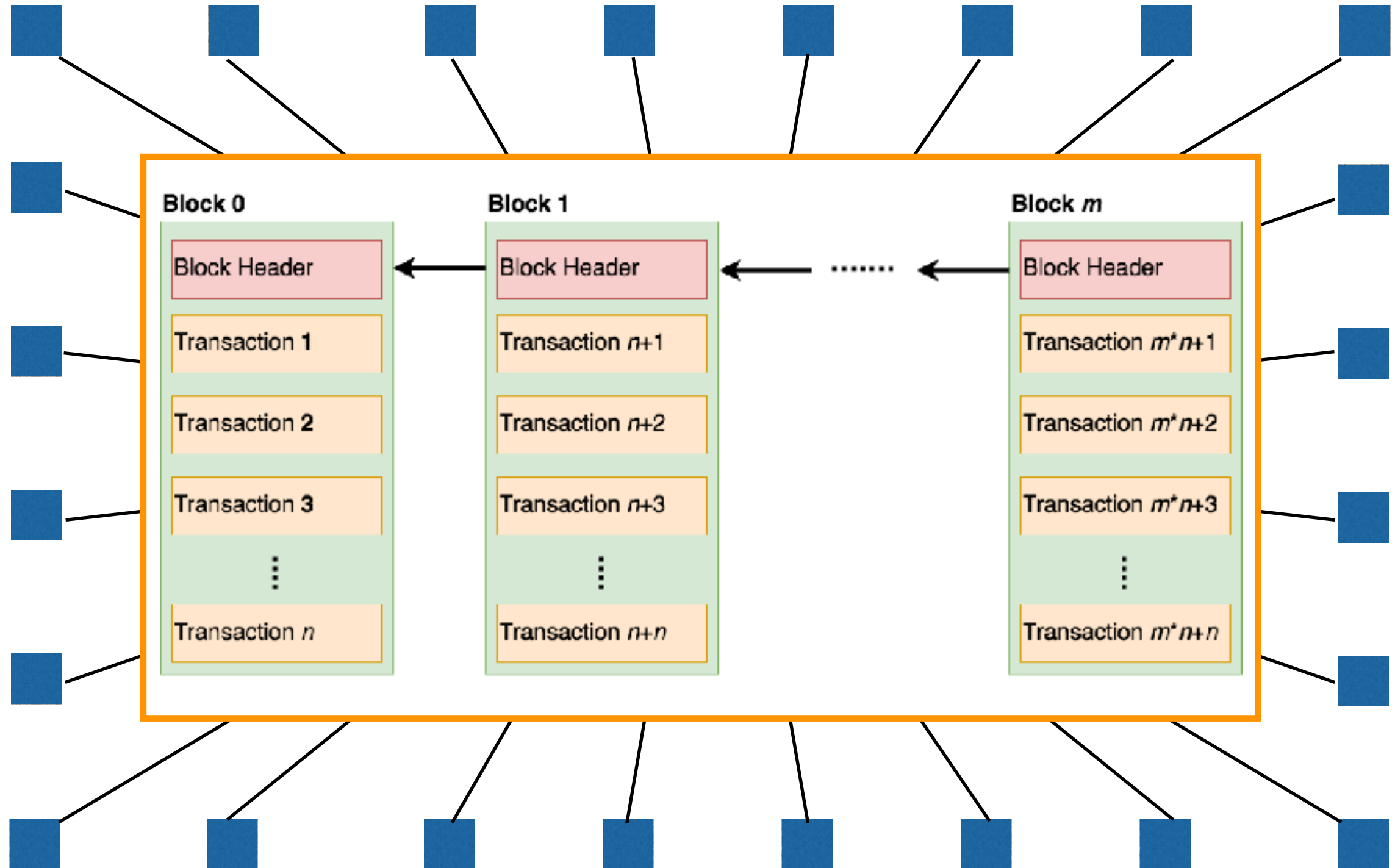
Total	22799 (100%)
United States	6747 (29.59%)
China	3348 (14.68%)
Germany	1388 (6.09%)
Russian Federation	1336 (5.86%)
Canada	1011 (4.43%)
United Kingdom	850 (3.73%)
Netherlands	576 (2.53%)
France	512 (2.25%)
Korea, Republic of	479 (2.10%)
Ukraine	439 (1.93%)



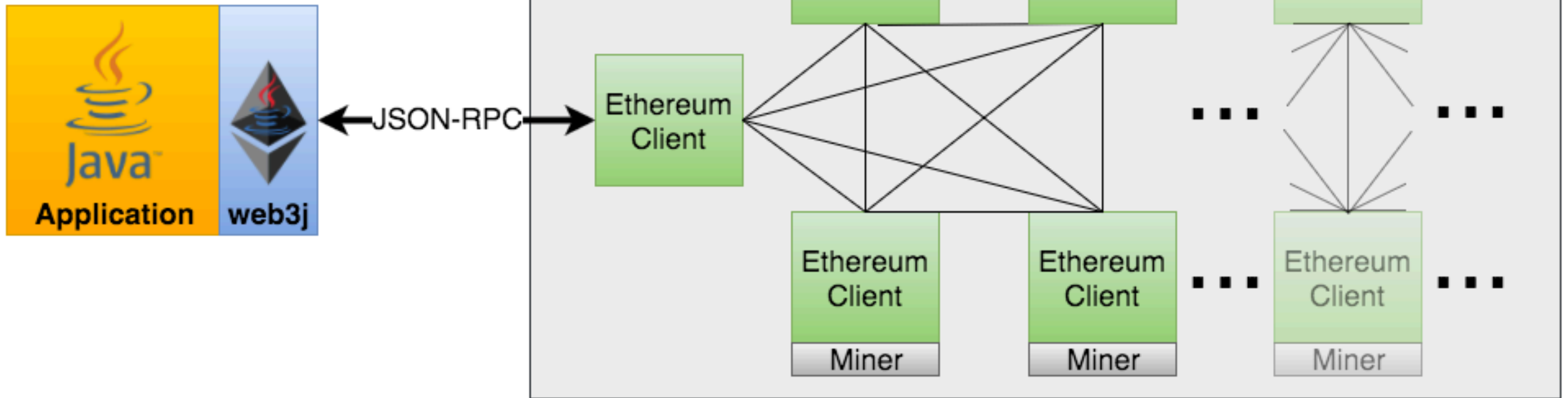


Source: https://twitter.com/peter_szilagyi/status/887272506914213888

The Blockchain

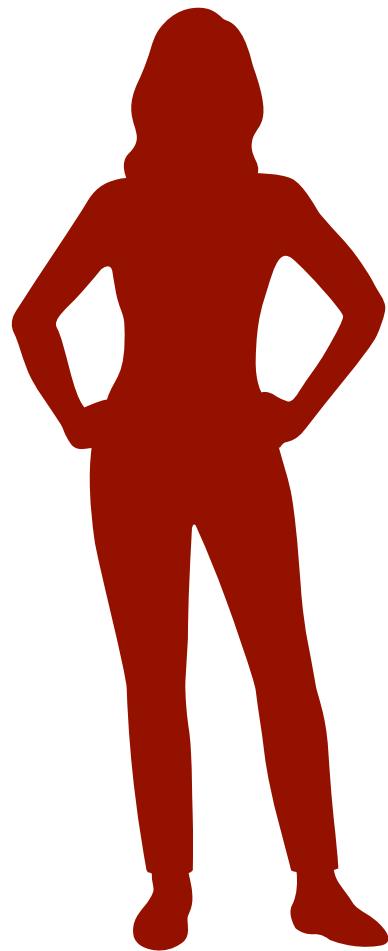


Integration



Sending Ether

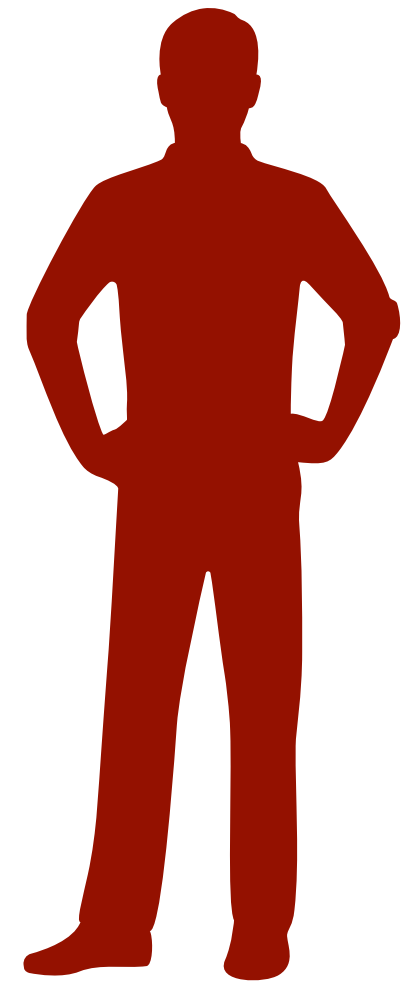
10 Ether



Alice



1 Ether



Bob

Wallet

0x19e03255f667bdfd50a32722df860b1eeaf4d635



Wallet file



Hardware wallet

Address Creation

EC DSA Private Key

0xa2d27ba84871112bb2ab87d849b8bce790667762fd7f30981ea775880c691e45



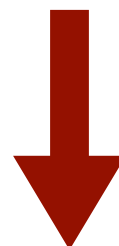
EC DSA Public Key

0x54c8cda130d3bfda86bd698cee738e5e502abc1fcb9e45709ee1fe38e855cda334ca
6f9288ab6d867f6baa2b2afeced0478e6a7225a5b1bb263ab21611817507



Keccak-256 Hash

0xbf58b3e74e951493fe64f409c98e381edc5fe1ac514935f3cc3edaa764cf004



Address

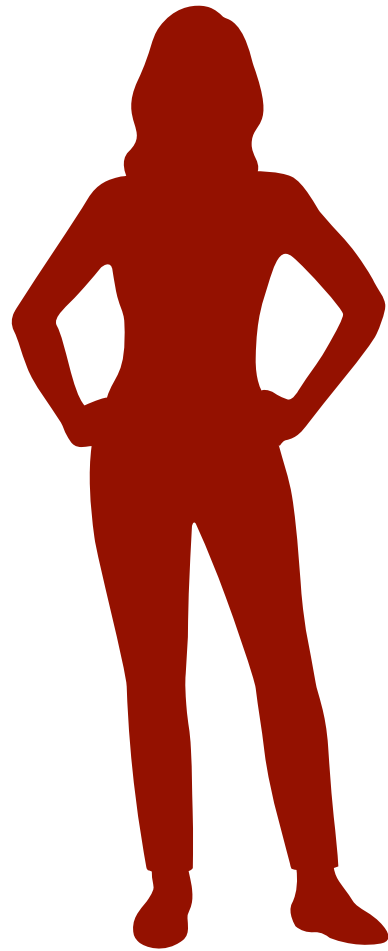
0x9c98e381edc5fe1ac514935f3cc3edaa764cf004

Wallet File

```
{  
  "address": "a929d0fe936c719c4e4d1194ae64e415c7e9e8fe",  
  "id": "c2fbffdd-f588-43a8-9b0c-facb6fd84dfe",  
  "version": 3,  
  "crypto": {  
    "cipher": "aes-128-ctr",  
  
"ciphertext": "27be0c93939fc8262977c4454a6b7c261c931dfd8c030b2d3e60ef76f99bfdc6",  
    "cipherparams": {  
      "iv": "5aa4fdc64eef6bd82621c6036a323c41"  
    },  
    "kdf": "scrypt",  
    "kdfparams": {  
      "dklen": 32,  
      "n": 262144,  
      "p": 1,  
      "r": 8,  
  
"salt": "6ebc76f30ee21c9a05f907a1ad1df7cca06dd594cf6c537c5e6c79fa88c9b9d1"  
    },  
    "mac": "178eace46da9acbf259e94141fbc7d3d43041e2ec546cd4fe24958e55a49446"  
  }  
}
```


Sending Ether

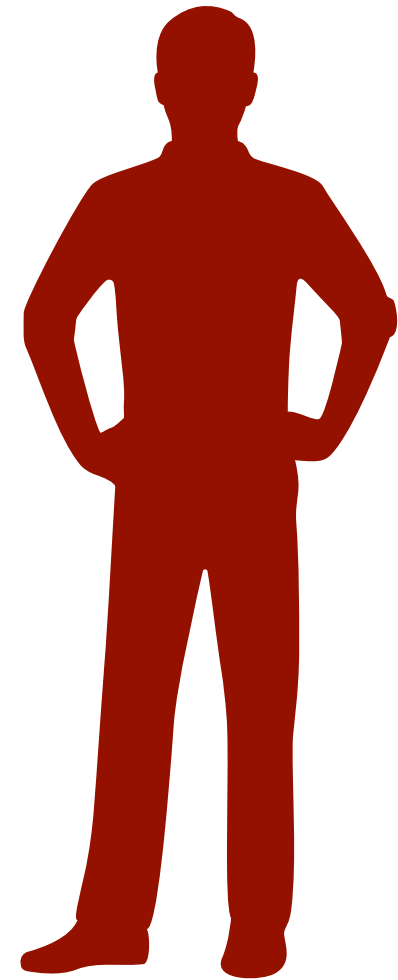
10 Ether



Alice



1 Ether



Bob

0x19e03255f667bdfd50a32722df860b1eeaf4d635

0x6869e289b2e0084888eb3c7dc80cd55a53602b9d

Sending Ether

Send 1 Ether from (0x19e0...) to (0x6869...)

Transaction

Recursive Length Prefix (RLP) Encoded Transaction

Cryptographically Signed Transaction



Private Key

Ethereum Node

Ethereum Virtual Machine

Transactions



Transaction

To address
Data (EVM bytecode)
Value (Ether)
Nonce
Gas price
Gas limit

Sign



Wallet
Private key

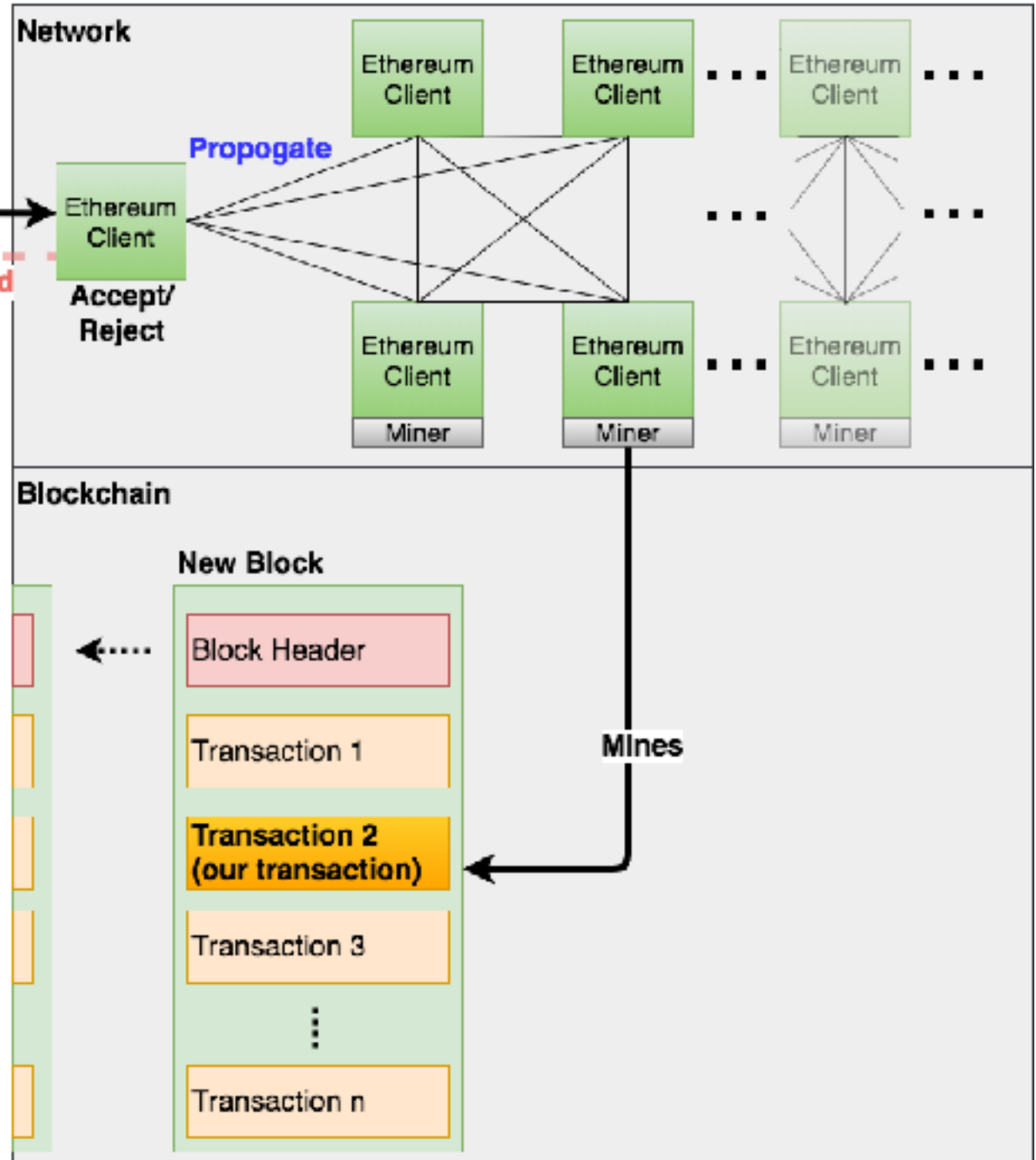
Signed Transaction

To address
Data (EVM bytecode)
Value (Ether)
Nonce
Gas price
Gas limit

ECDSA Signature
(Transaction Hash)

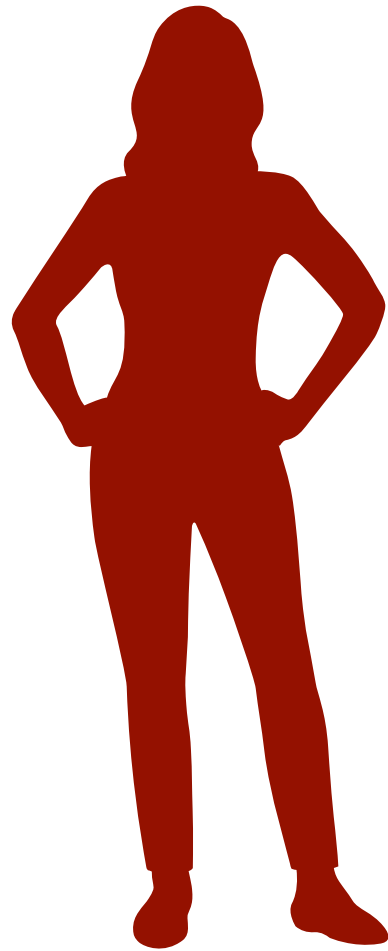
Send

Rejected



Transaction Complete

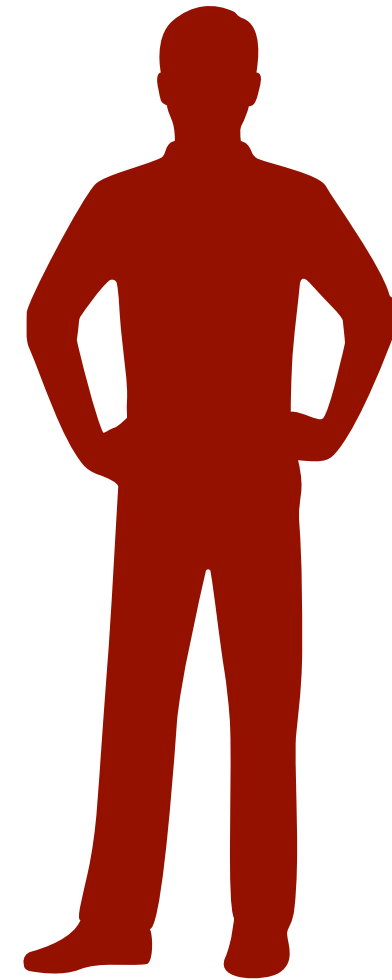
9 Ether



Alice

0x19e03255f667bdfd50a32722df860b1eeaf4d635

1 Ether



Bob

0x6869e289b2e0084888eb3c7dc80cd55a53602b9d

Transaction Types

Transfer Ether

- Send Ether somewhere

Push new code

- Deploy a smart contract

Call existing code

- Invoke a smart contract method

Query state

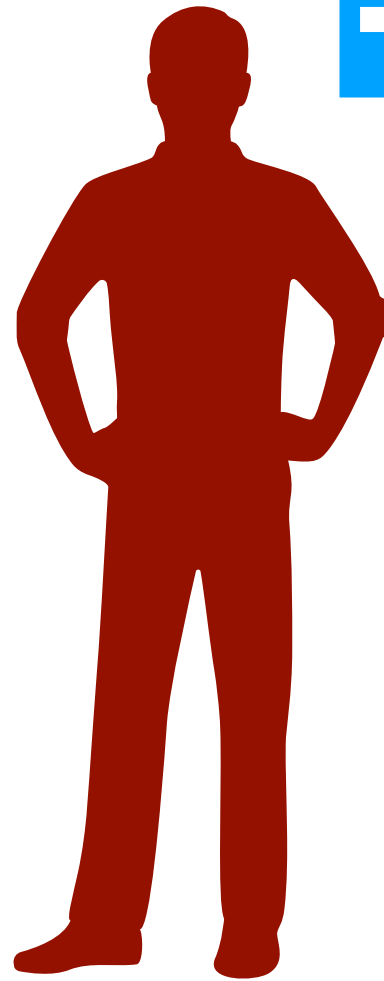
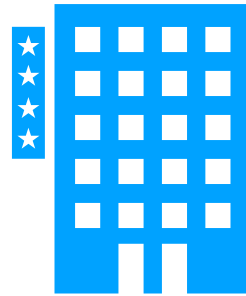
- Read a value(s) from a smart contract

Smart Contracts

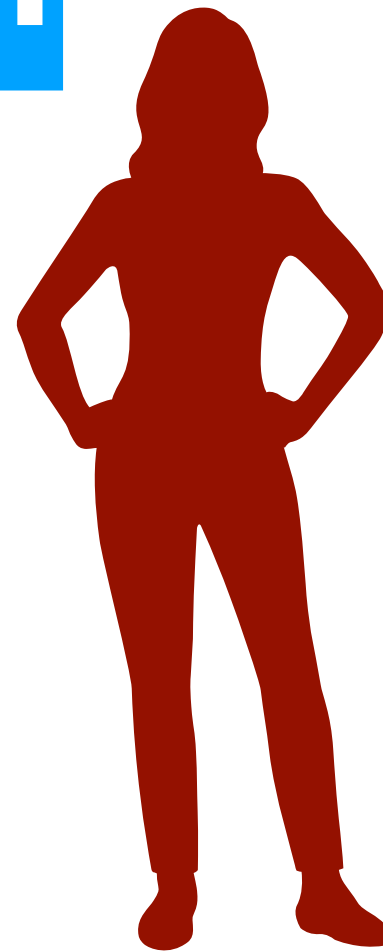
```
contract greeter {  
    string greeting;  
    function greeter(string _greeting) public {  
        greeting = _greeting;  
    }  
    function greet() constant returns (string) {  
        return greeting;  
    }  
}
```

A New Funding Model?

BC Inc.

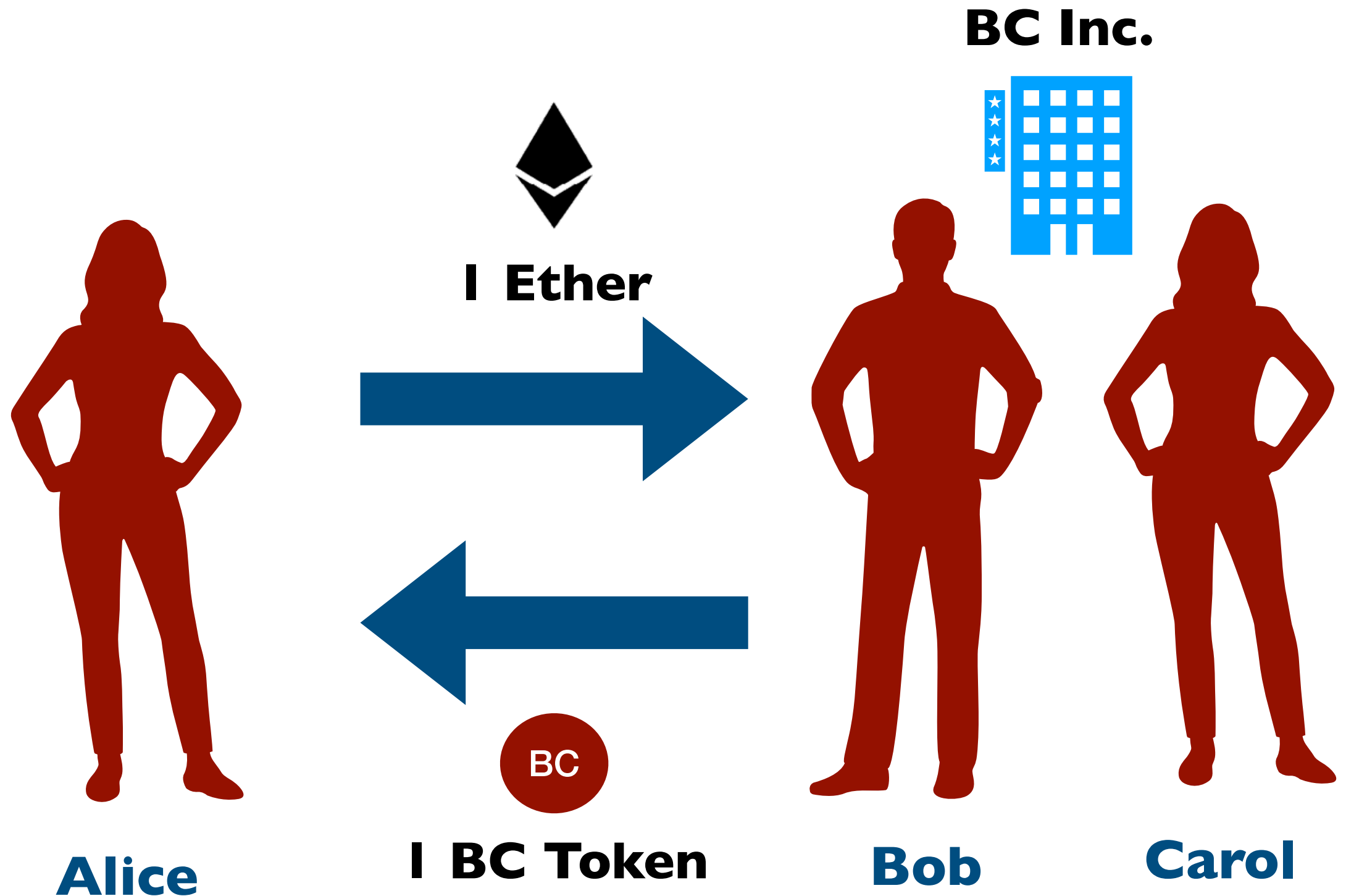


Bob

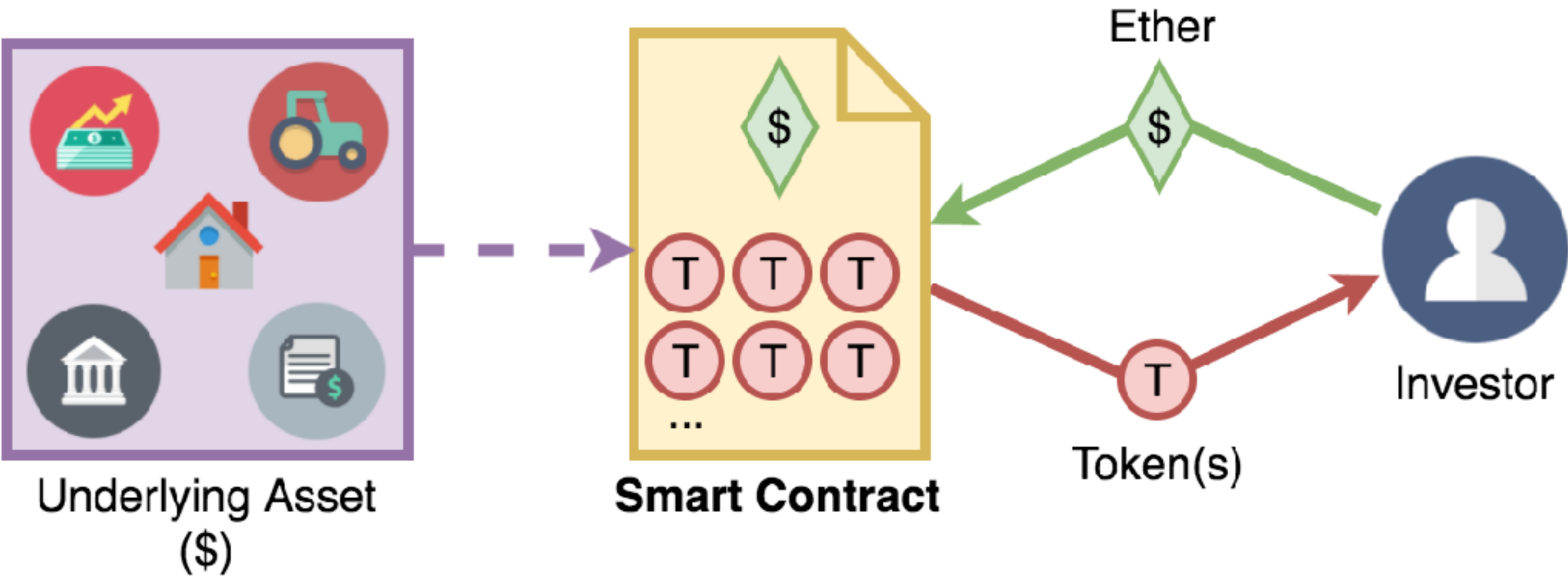


Carol








A New Funding Model?



The Initial Coin Offering (ICO)



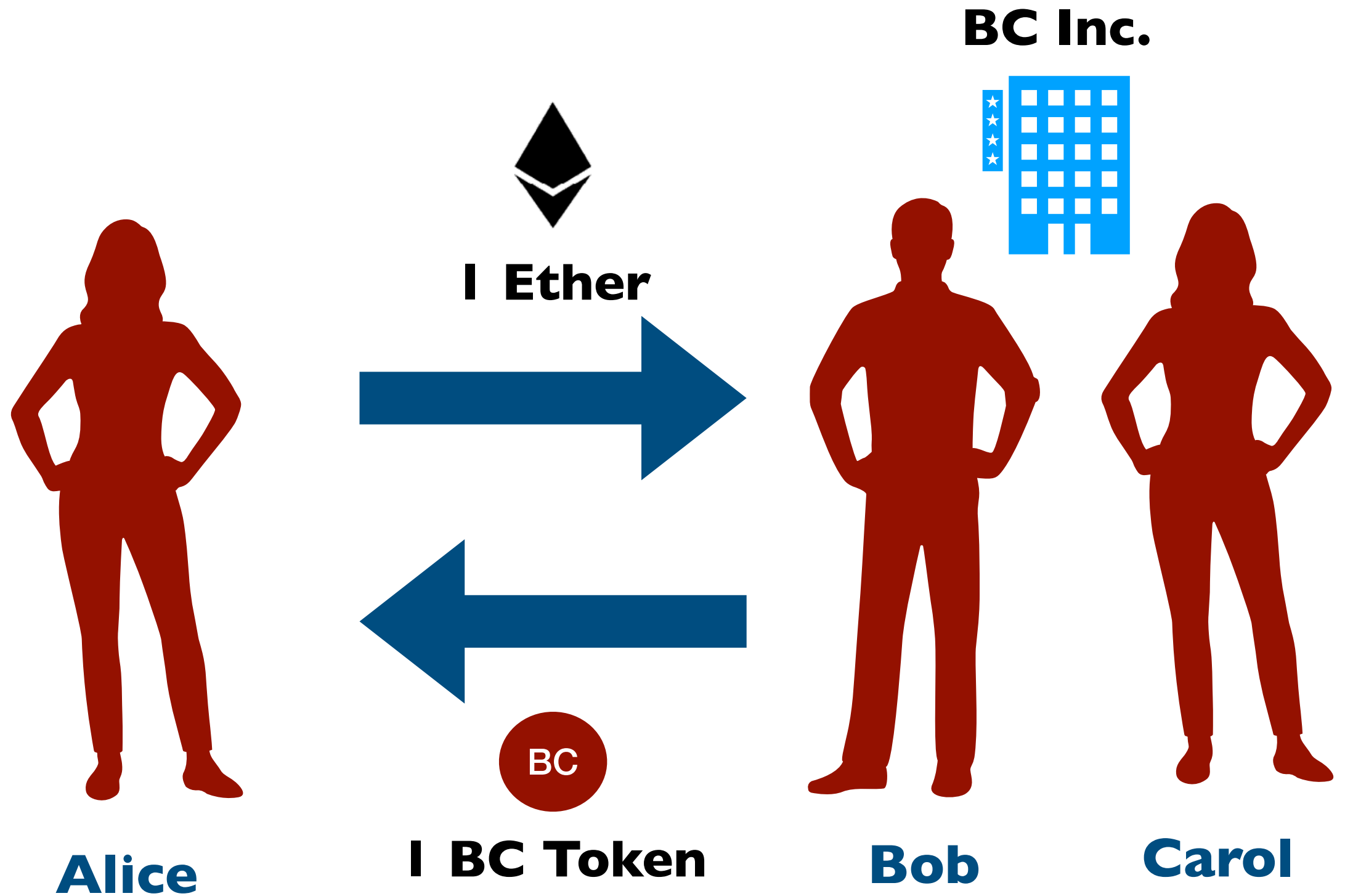
The ICO Machine

	Token	Price	%Change	MarketCap
1	 EOS (EOS) Infrastructure for Decentralized Applications	\$7.6698 0.00070097 Btc 0.009195 Eth	▼ -6.49%	\$5,450,351,745
2	 Tron (TRX) TRON is a blockchain-based decentralized protocol that aims to construct a worldwide free content entertainment system with the blockchain and distributed storage technology.	\$0.0449 0.00000411 Btc 0.000054 Eth	▼ -3.63%	\$2,954,460,777
3	 Qtum (QTM) Build Decentralized Applications that Simply Work Executable on mobile devices, compatible with major existing blockchain ecosystem	\$25.6415 0.00234345 Btc 0.030739 Eth	▼ -3.58%	\$1,895,642,556
4	 OmiseGO (OMG) OmiseGO (OMG) is a public Ethereum-based financial technology for use in mainstream digital wallet	\$16.2781 0.0014877 Btc 0.019514 Eth	▼ -7.20%	\$1,661,058,862
5	 ICON (ICX) The ICON Network is comprised of various institutions ranging from: financial institutions, insurance companies, hospitals, universities and more.	\$3.3808 0.00030898 Btc 0.004053 Eth	▼ -6.55%	\$1,304,882,787
6	 Digix Global (DGD) Every asset represents a unique bullion bar sitting in designated securitised custodial vaults.	\$502.4170 0.0459173 Btc 0.602296 Eth	▲ 1.30%	\$1,004,834,000
7	 Binance (BNB) Binance will build a world-class crypto exchange, powering the future of crypto finance.	\$9.6355 0.00088062 Btc 0.011551 Eth	▼ -6.66%	\$954,052,367

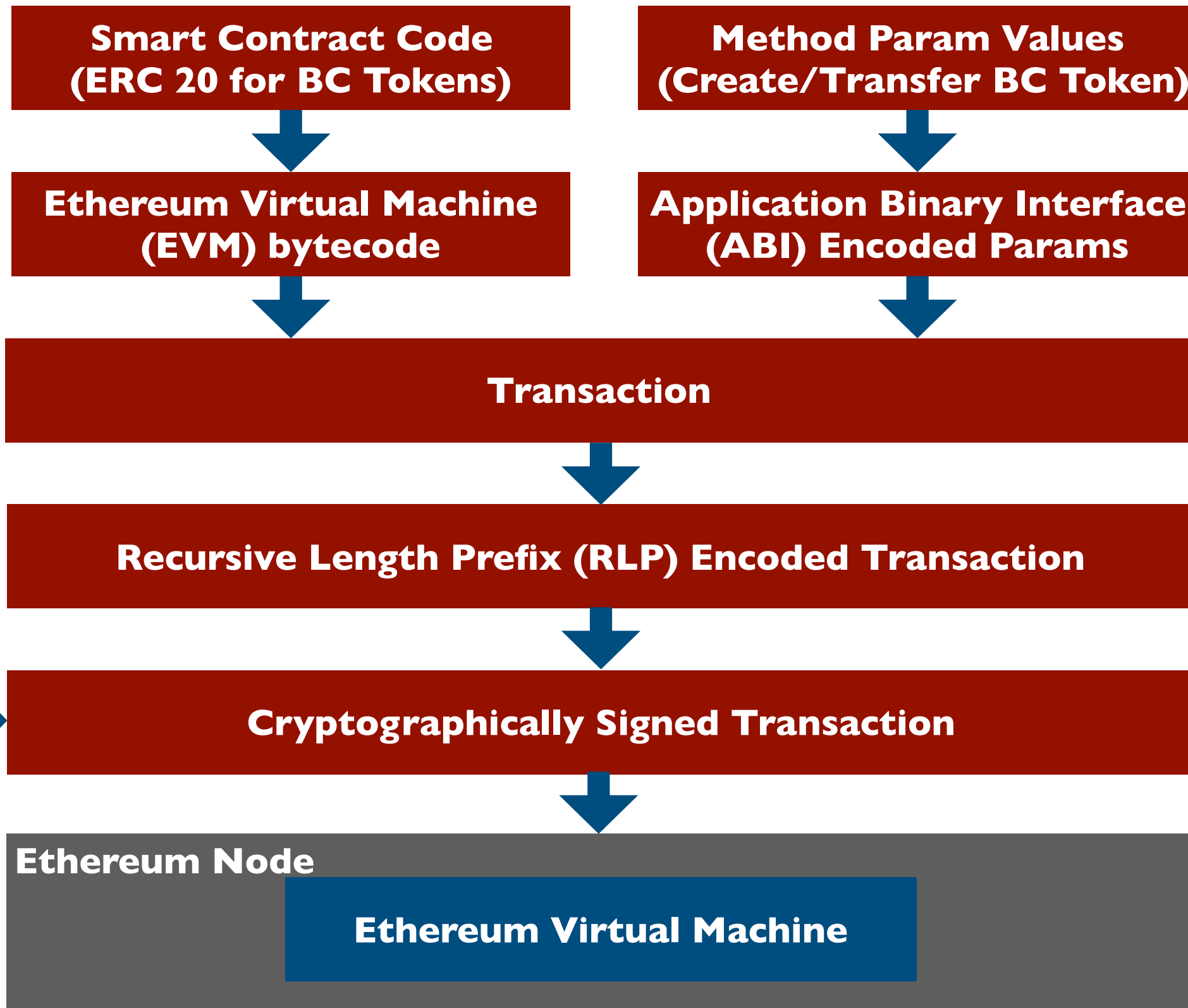
ERC-20

```
contract ERC20Interface {  
  
    function totalSupply() public constant returns  
(uint);  
  
    function balanceOf(address tokenOwner) public  
constant returns (uint balance);  
  
    function transfer(address to, uint tokens)  
public returns (bool success);  
  
    ...  
  
}
```

A New Funding Model?



Smart Contract Transactions



Transactions



Transaction

To address
Data (EVM bytecode)
Value (Ether)
Nonce
Gas price
Gas limit

Sign



Wallet
Private key

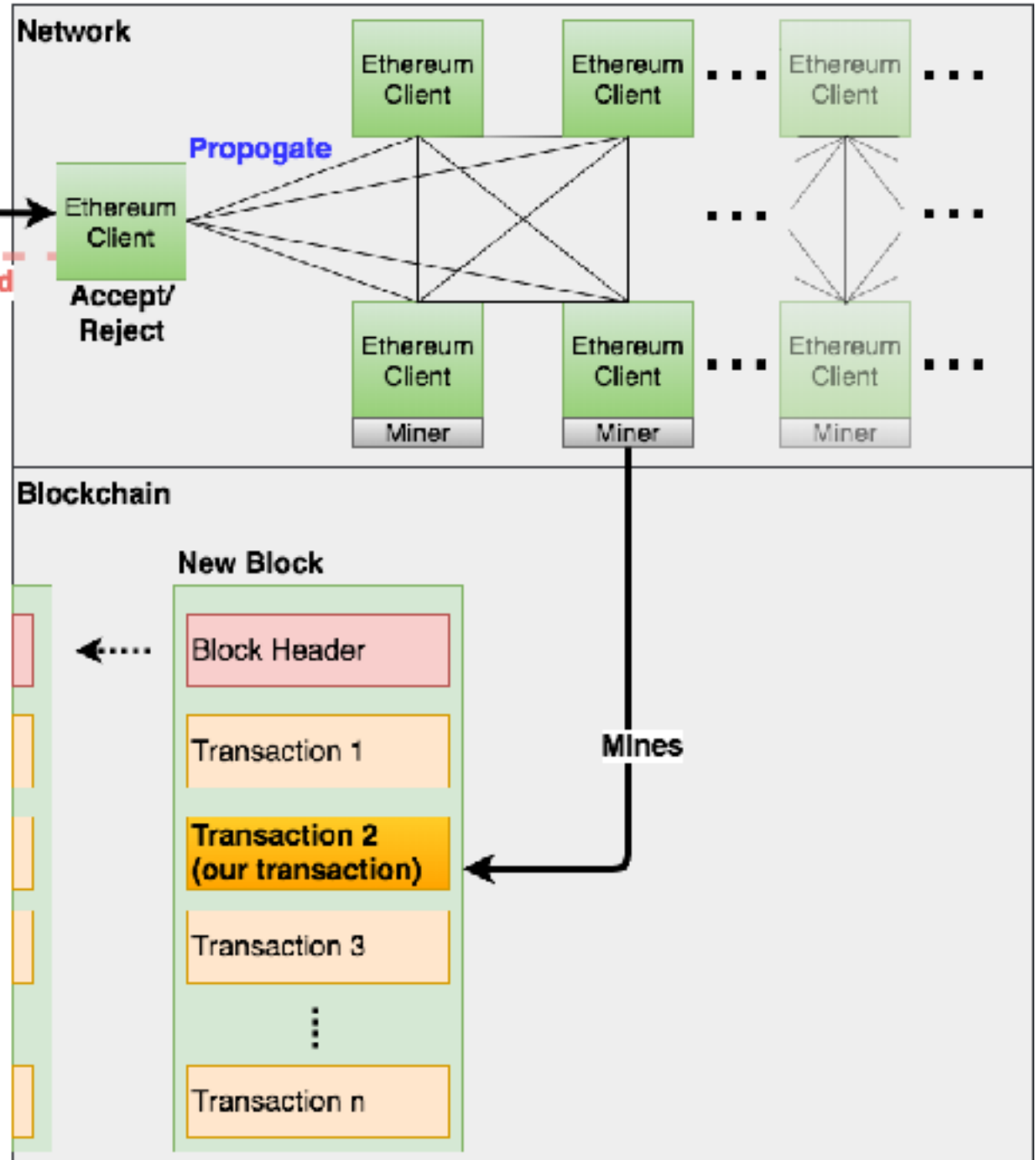
Signed Transaction

To address
Data (EVM bytecode)
Value (Ether)
Nonce
Gas price
Gas limit

ECDSA Signature
(Transaction Hash)

Send

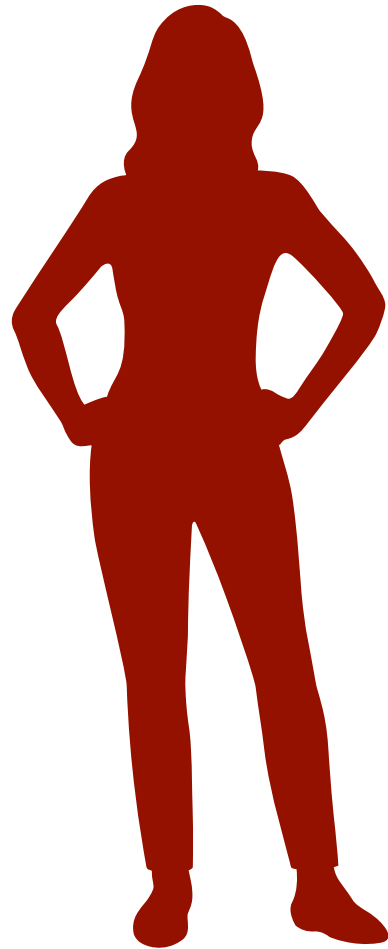
Rejected



Transaction Complete

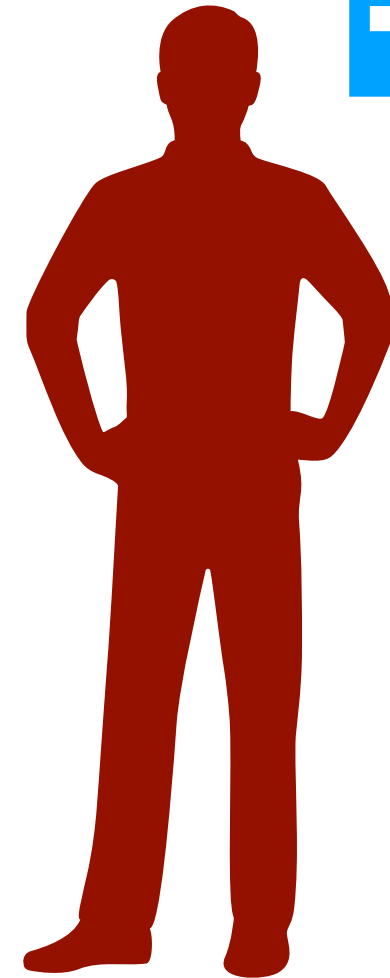
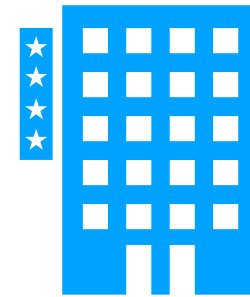


| BC Token



Alice

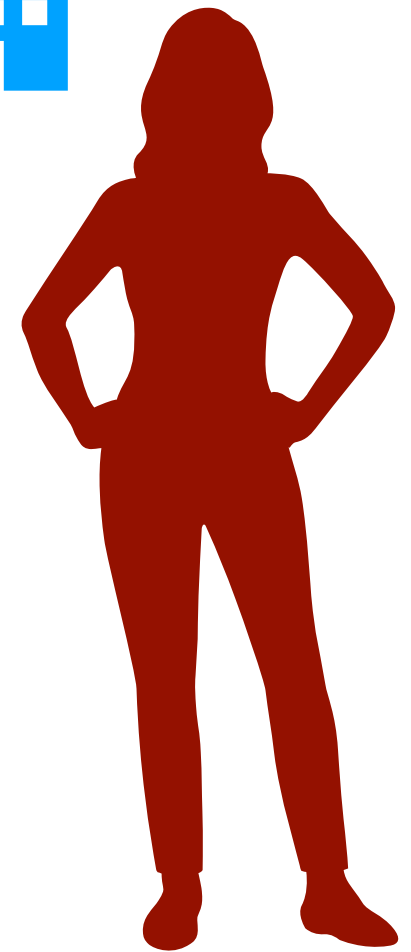
BC Inc.



Bob

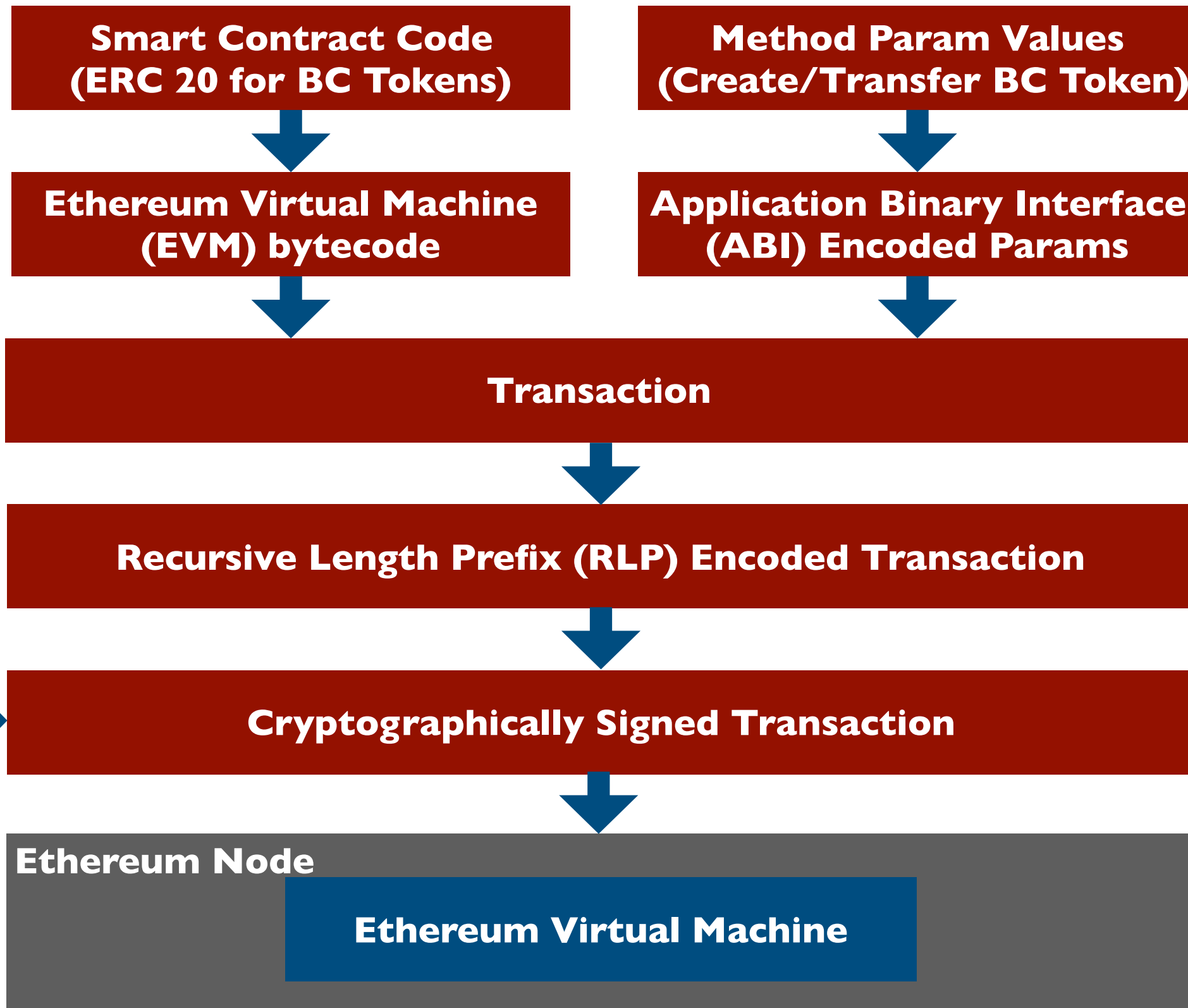


| Ether

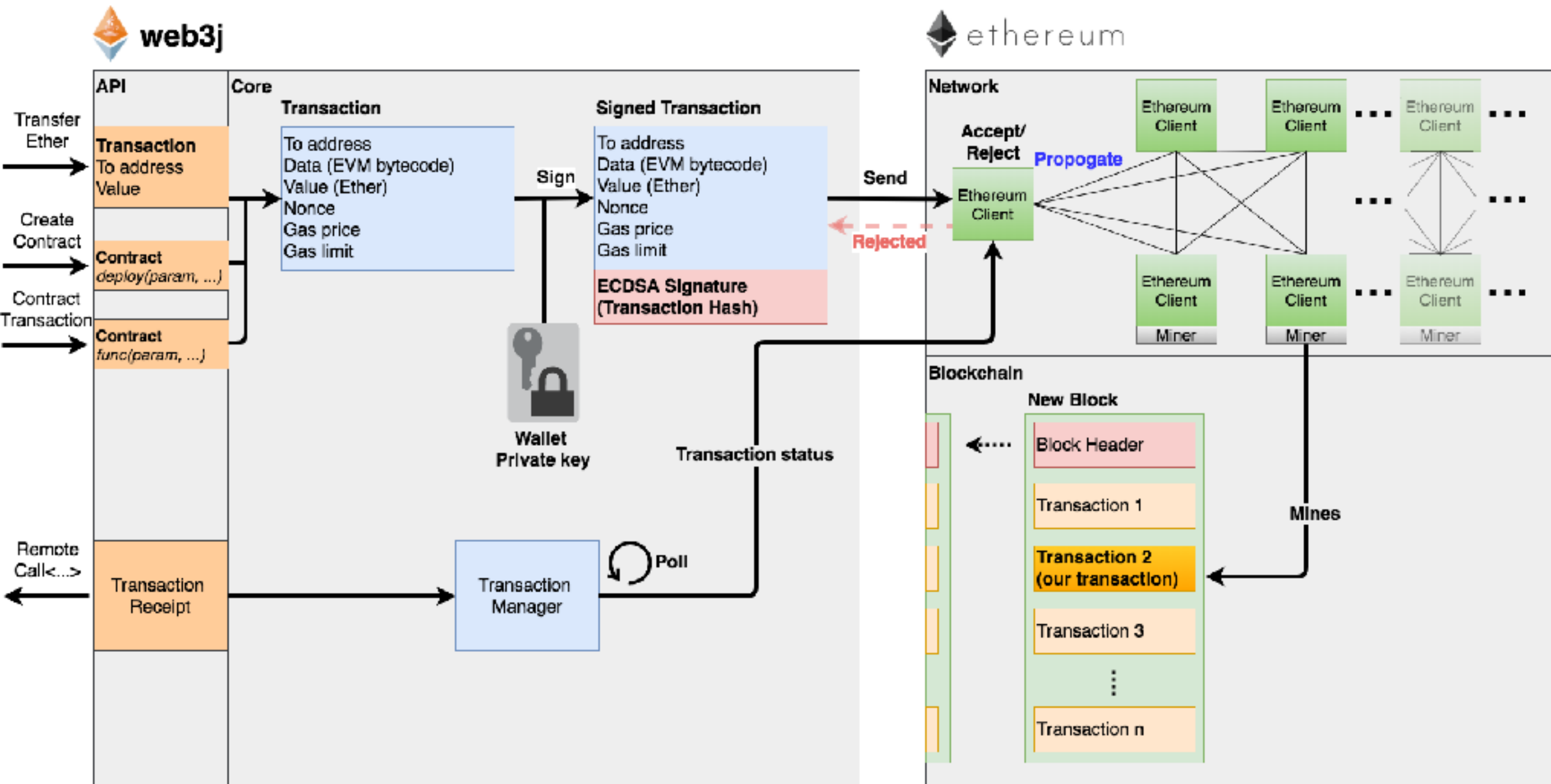


Carol

Smart Contract Transactions



Transaction Abstractions



Sending Ether in web3j

```
Web3j web3j = Web3j.build(new HttpService());
```

```
Credentials alice =  
WalletUtils.loadCredentials(  
    "alicesPassword", "/path/to/walletfile");
```

```
Transfer.sendFunds(  
    web3j, alice, 0x<bob's address>,  
    BigDecimal.valueOf(1.0),  
    Convert.Unit.ETHER).send();
```


Managing tokens in web3j

```
HumanStandardToken contract = deploy(web3j, bob,  
    GAS_PRICE, GAS_LIMIT,  
    BigInteger.valueOf(1_000_000),  
    "BC token",  
    BigInteger.valueOf(18), "BC").send();
```

```
contract.transfer(  
    0x<bob's address>, transferQuantity)  
    .send();
```

```
BigInteger balance = contract.balanceOf(  
    alice.getAddress()).send();
```

Ether, the fuel of Ethereum

Gas Price

Price per unit of computation

Gas Limit

Upper transaction cost bound

APPENDIX C. FEE SCHEDULE

The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero} .
G_{base}	2	Amount of gas to pay for operations of the set W_{base} .
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low} .
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid} .
G_{high}	10	Amount of gas to pay for operations of the set W_{high} .
$G_{extcode}$	700	Amount of gas to pay for operations of the set $W_{extcode}$.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{reset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{clear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{selfdestruct}$	24000	Refund given (added into refund counter) for self-destructing an account.
$G_{selfdestruct}$	5000	Amount of gas to pay for a SELFDESTRUCT operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{create2}$	20000	Paid for a CREATE2 operation.

Resilience in web3j

Open source

- Listen to your community

Documentation

- Including sample projects

Don't write your own Crypto

- Thanks to the Legion of the Bouncy Castle!

Code Quality

- Enforce standards
- Testing - Travis CI is free for OSS

Architecting the Blockchain for Failure

Ethereum & web3j

Failure in Ethereum

Distributed Consensus

Consensus in Ethereum

- Public Network Consensus
- Consortium Network Consensus





NEWS

Home

UK

World

Business

Politics

Tech

Science

Health

Family & Education

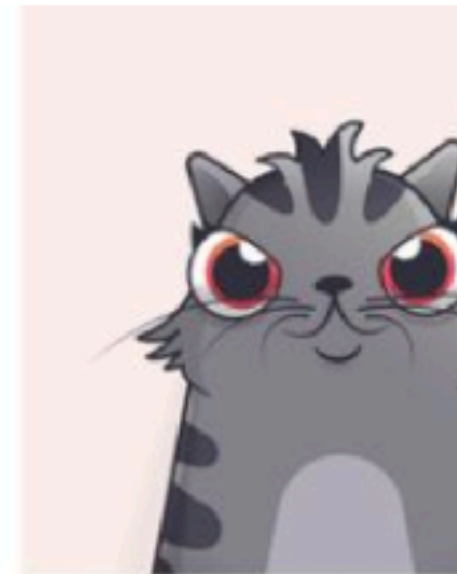
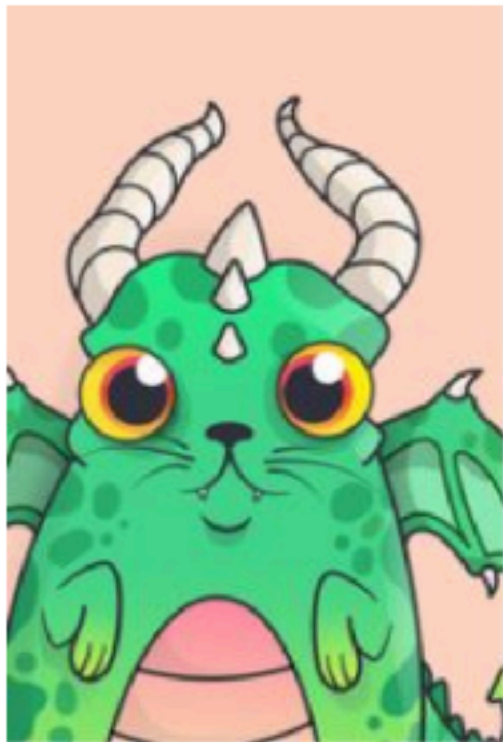
Technology

CryptoKitties craze slows down transactions on Ethereum

5 December 2017



Share





KLINT FINLEY BUSINESS 06.18.16 04:30 AM

A \$50 MILLION HACK JUST SHOWED THAT THE DAO WAS ALL TOO HUMAN

SHARE



SHARE
1461



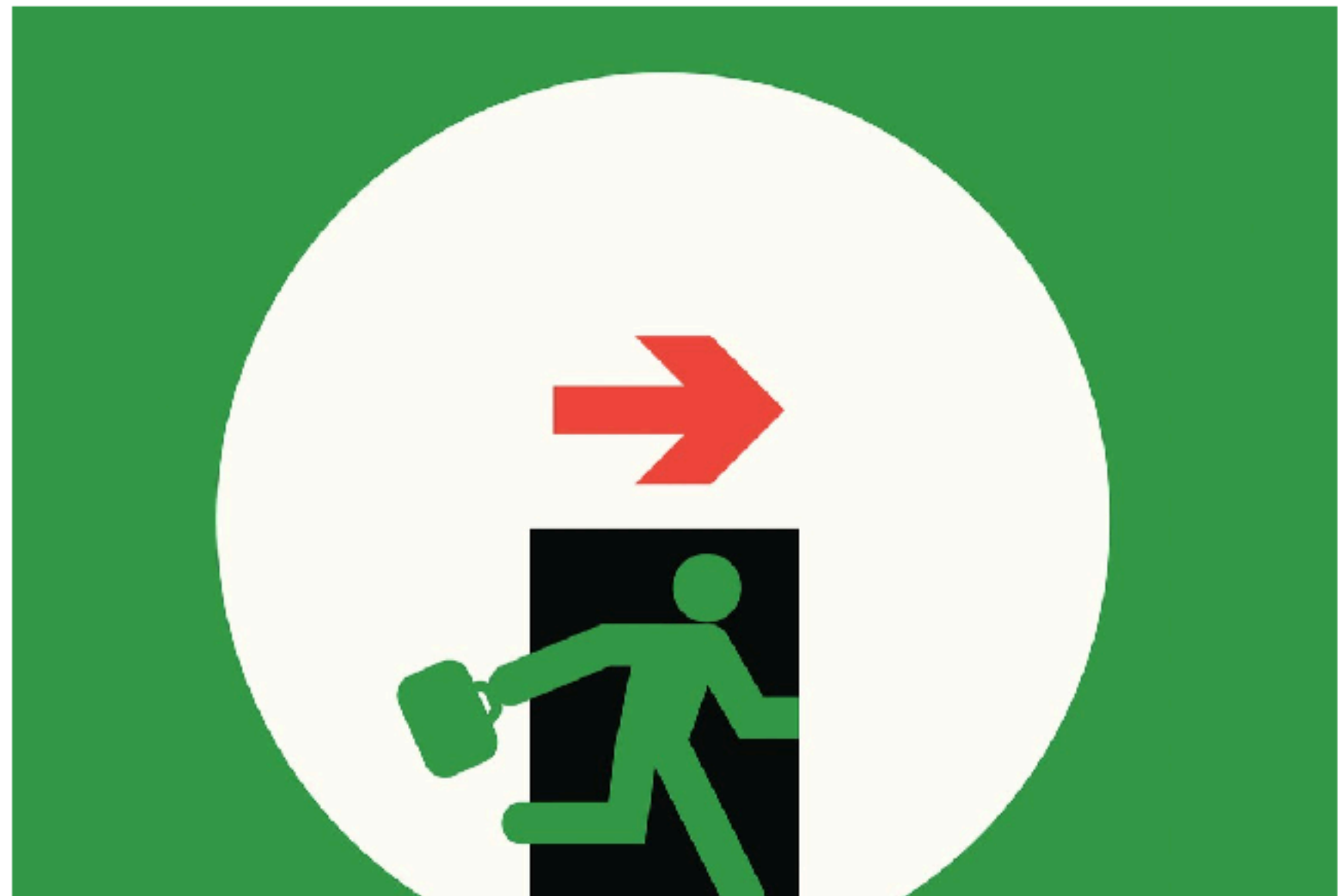
TWEET



COMMENT



EMAIL



Address Zero



LOGIN

Search by Address / Txhash / Block / Token / Ens

GO

HOME

BLOCKCHAIN

ACCOUNT

TOKEN

CHART

MISC

Address 0x00

Home / Normal Accounts / Address

Sponsored Link: **S SHPING** - \$3.4M RAISED IN PRESALE - ON TRACK TO BE LARGEST ICO IN AUSTRALIA - [JOIN NOW](#)

Overview



ETH Balance: 7,228.362688311567416148 Ether

ETH USD Value: \$6,026,285.97 (@ \$833.70/ETH)

Mined: 95 blocks 0.2 uncles

No Of Transactions: 756 txns

7,228 Ether
\$6,026,285.97

Misc



More Options

Address Watch

Add To Watch List

Token Balances

View (\$532,875,196.36)

>200

\$532,875,196.36

Transactions

Internal Transactions

Token Transfers

Mined Blocks

Mined Uncles

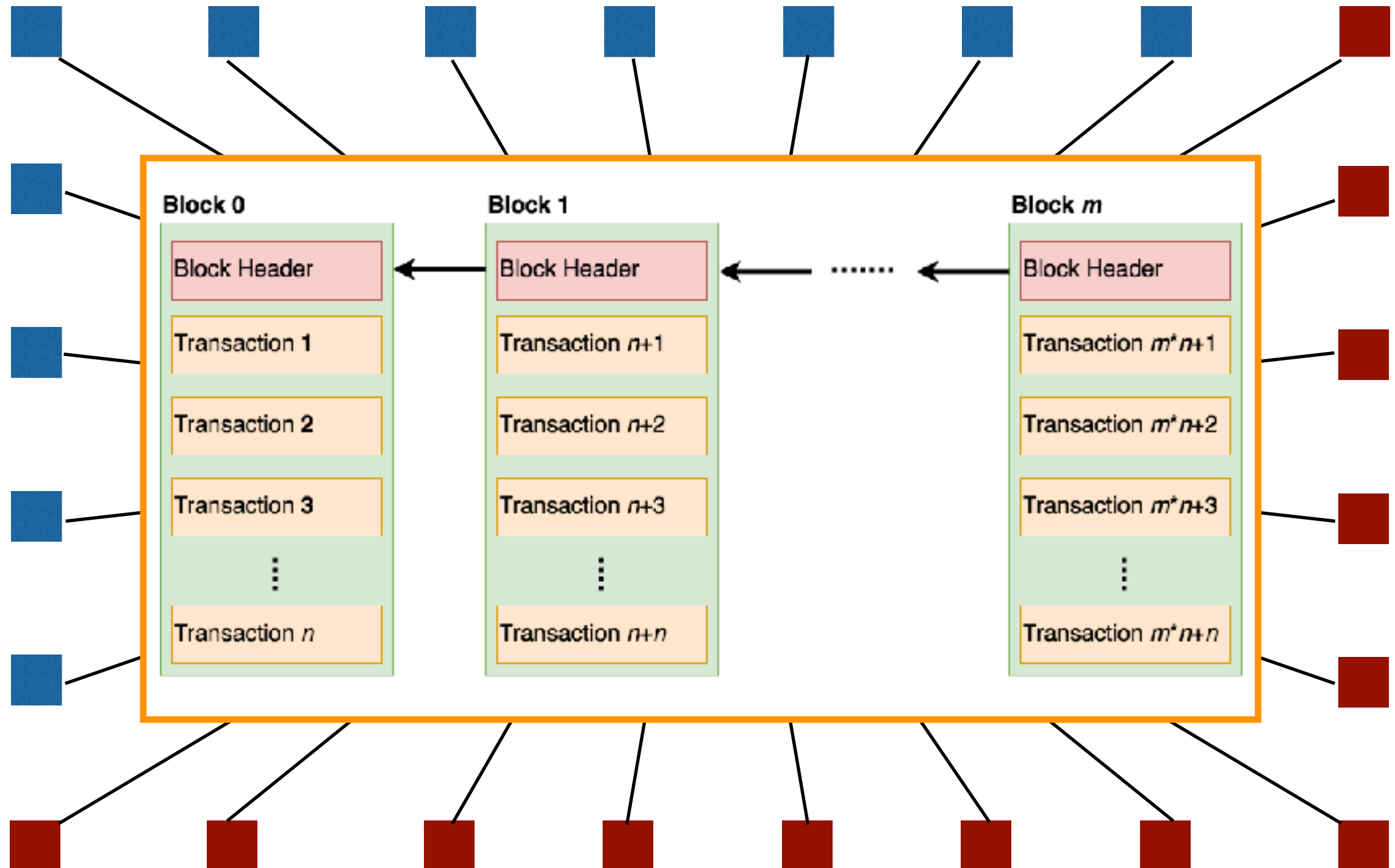
Comments

Latest 25 txns from a total Of 756 transactions

View All

TxHash	Block	Age	From	To	Value	[TxFee]
0x2b193e0d83a489...	5190326	2 days 17 hrs ago	0x1e162b2dfc58c6...	0x00000000000000...	0.0001 Ether	0.000021
0xb4653386223a66...	5186716	3 days 8 hrs ago	0x89a8f5f337304ea...	0x00000000000000...	0 Ether	0.001554624
0x170ab0468b2eae...	5186685	3 days 8 hrs ago	0x89a8f5f337304ea...	0x00000000000000...	0 Ether	0.001490528
0x2a91135bbf4ff6c...	5170431	6 days 2 hrs ago	0x1f46d26be97f4c0...	0x00000000000000...	0.005 Ether	0.00021042

Consensus Attacks



Architecting the Blockchain for Failure

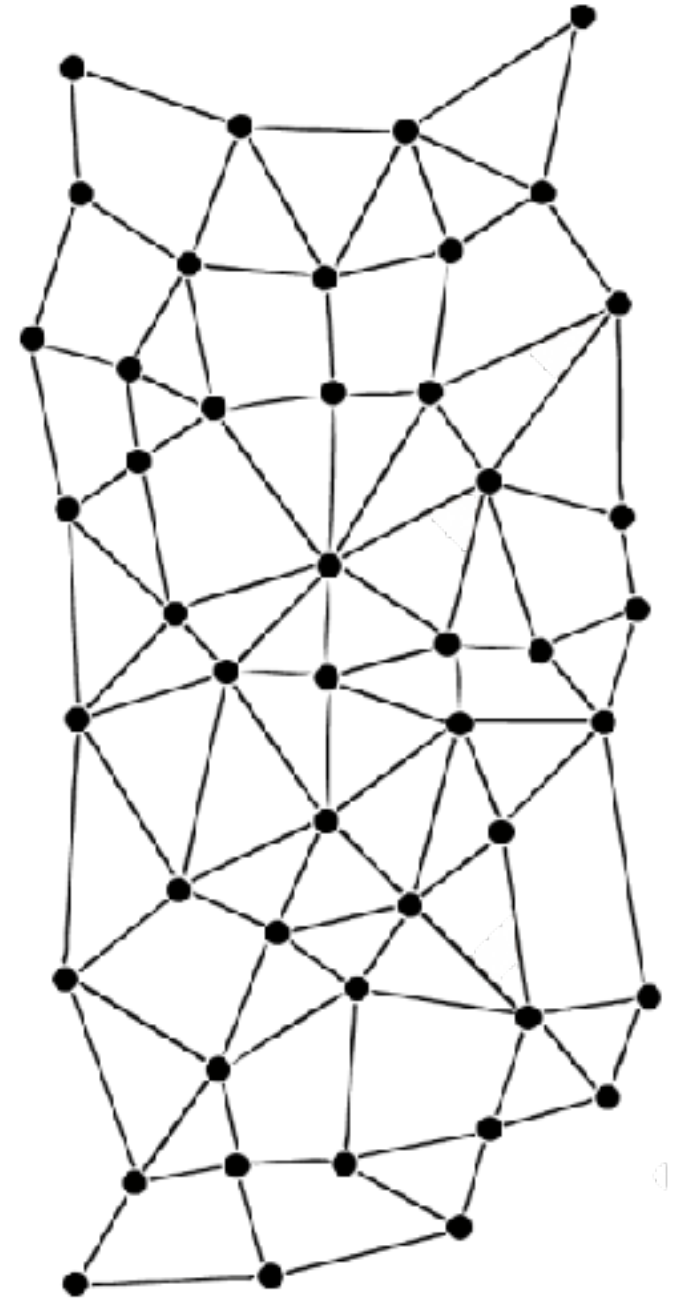
Ethereum & web3j

Failure in Ethereum

Distributed Consensus

Consensus in Ethereum

- Public Network Consensus
- Consortium Network Consensus



Distributed Consensus

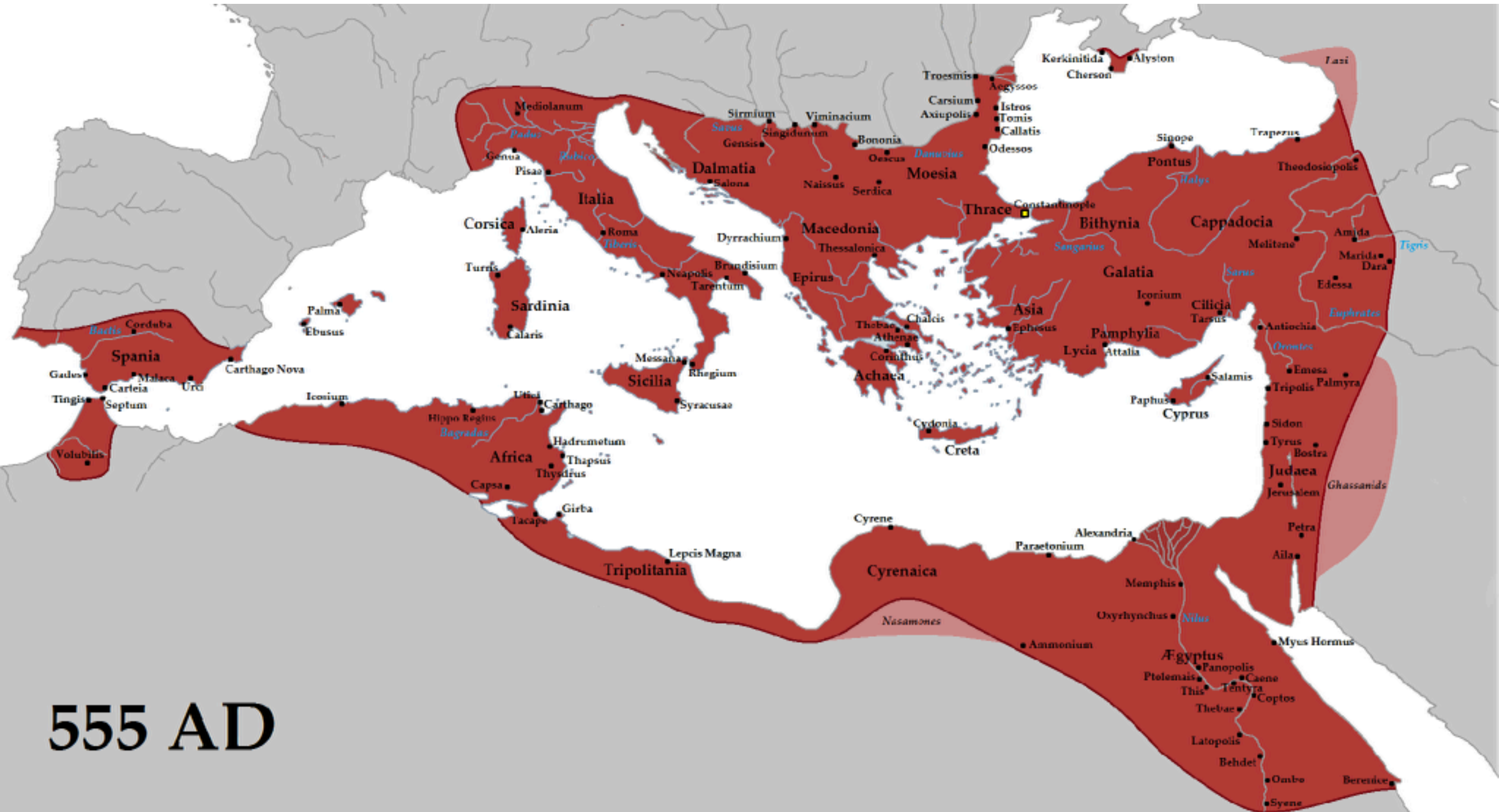
How to ensure a common worldview across nodes?

Quorums

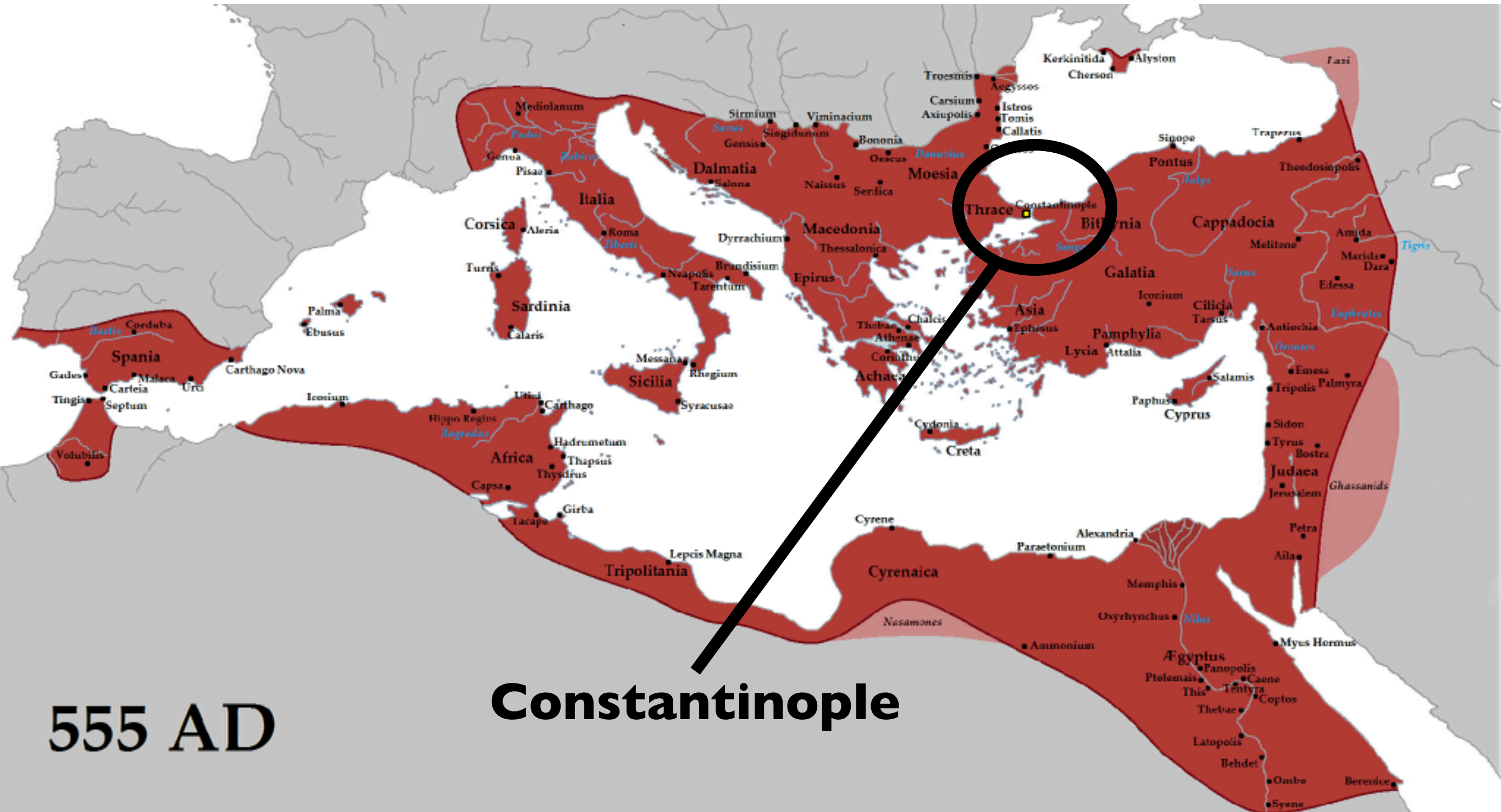
- Number of votes required to perform an operation across the system

Partial Asynchrony

- Timing assumptions are required



The Byzantine Empire



555 AD

Constantinople

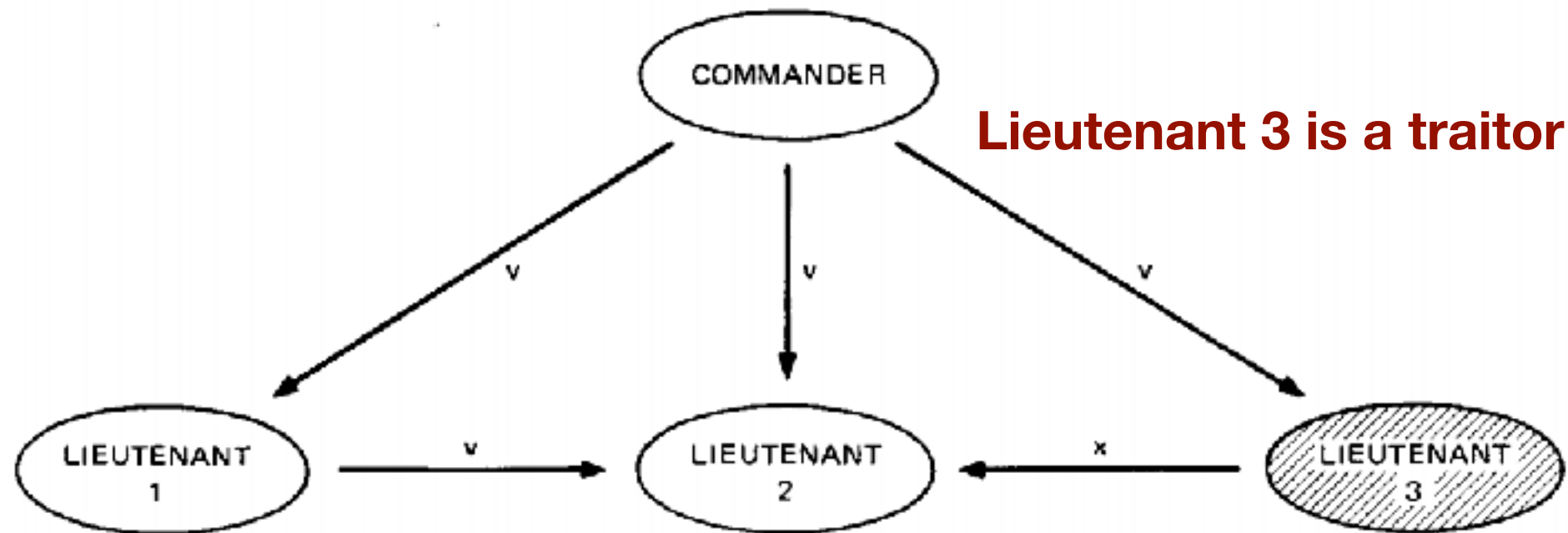
Byzantine Generals' Problem

- Multiple generals encircle city

- Should they?

- Attack

- Retreat



- Consensus required

- $3m + 1$ generals can cope with m traitors

Byzantine Fault Tolerance

Or just

Arbitrary Fault Tolerance

Architecting the Blockchain for Failure

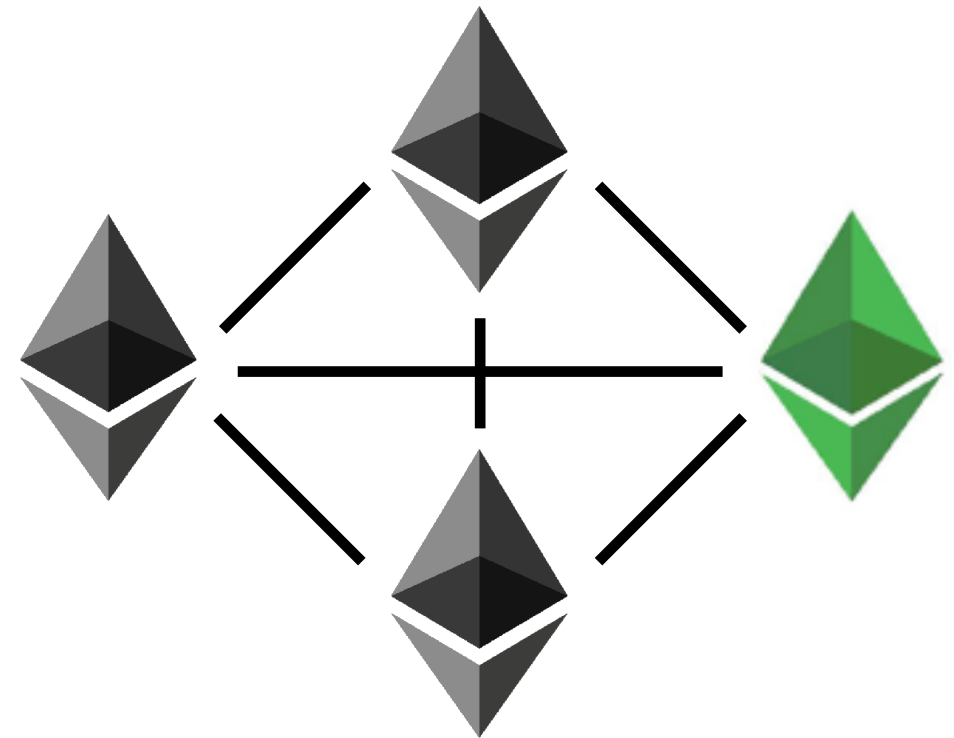
Ethereum & web3j

Failure in Ethereum

Distributed Consensus

Consensus in Ethereum

- **Public Network Consensus**
- Consortium Network Consensus



The Ethereum Network



Geth



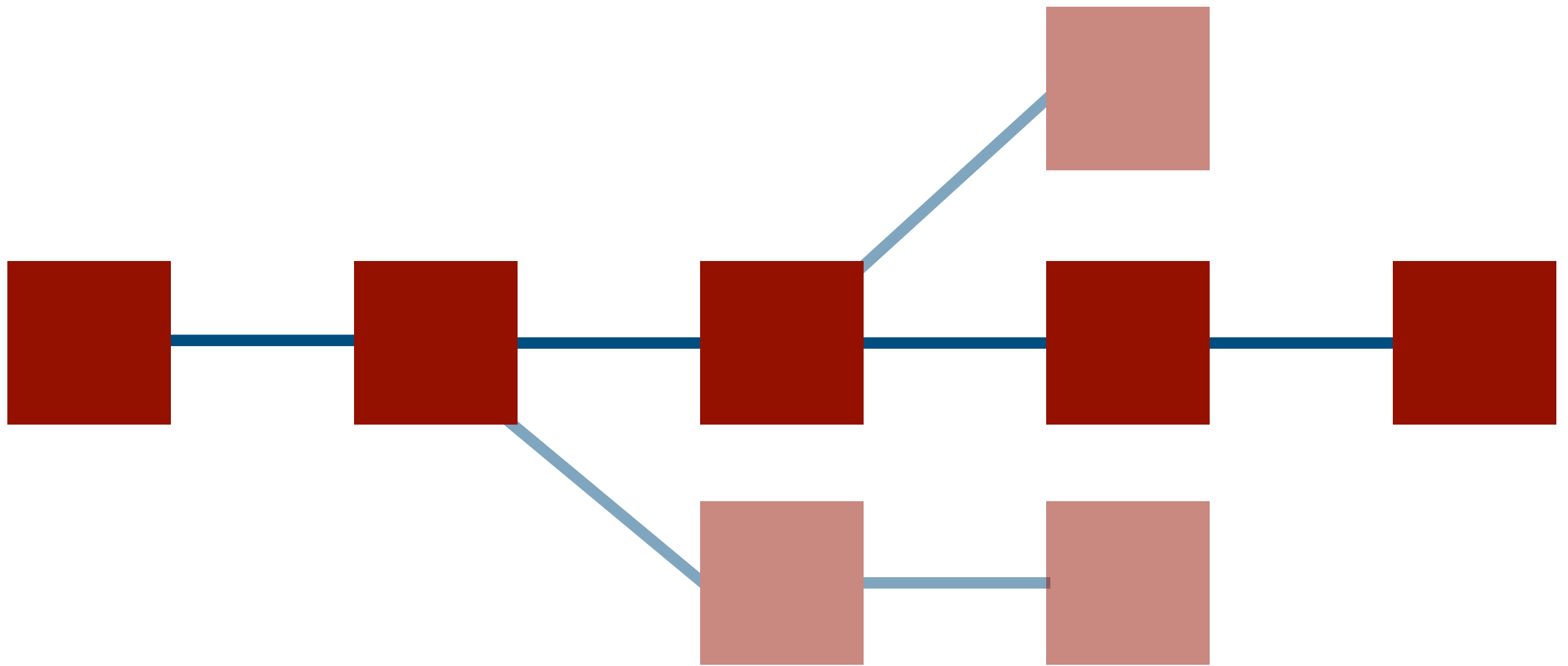
Parity

Other (C++, Java, Python, Ruby, Haskell)

Public Blockchain Networks

TRUST NO ONE

Proof of Work (PoW)



Longest Blockchain Wins



Proof of Work (PoW)

Miners continually compete to create blocks for the blockchain

- 5 ether reward for each solution

Based on Cryptographic hash function

```
hash(<block>) =>  
a7ffc6f8bf1ed76651c14756a061d662f580ff4de43b49fa82d80a4  
b80f8434a
```

Miners applying hash function millions (mega) of times/sec = MH/s

- Single GPU generates 5-30 MH/s
- CPU ~ 0.25 MH/s

Ethash Algorithm

Ethash Proof of Work algorithm (formerly Dagger Hashimoto)

- SHA3-256 variant Keccak hashing function
- Memory-hard computation
- Memory-easy validation
- Can't use ASICs (Application Specific Integrated Circuits)
- Uses 4GB directed acyclic graph file (DAG) regenerated every 30000 blocks by miner

Proof of Work

Simplified example:

```
nonce = random int
```

```
while hashimoto(block, nonce) > difficulty
```

```
    increment nonce
```

```
return nonce
```

Fetches bytes from DAG +
combine with block
Returns SHA3 Keccak hash

Solution

Proof of Work Difficulty

Hashing blocks

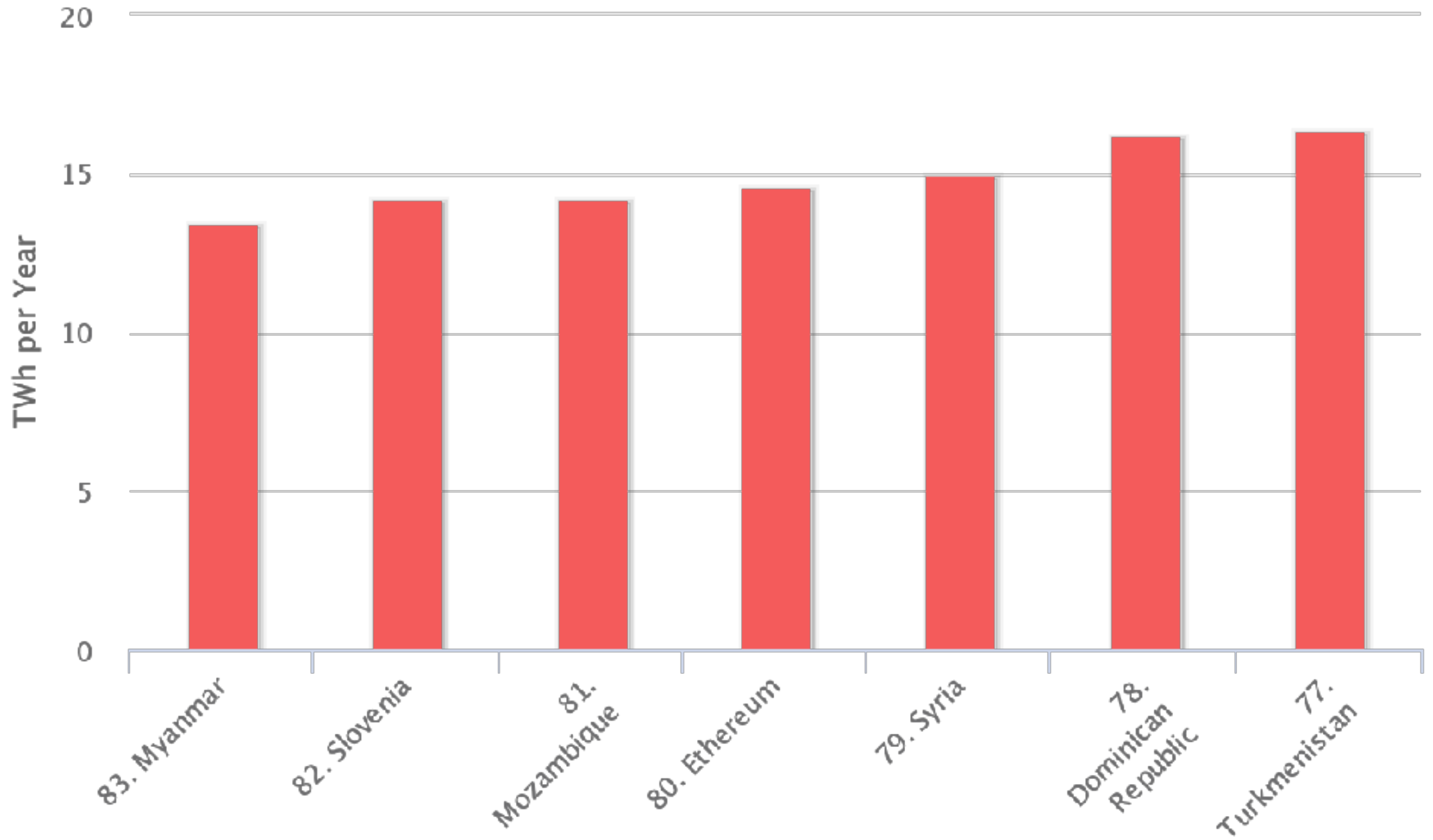
Difficulty - dynamically adjusts parameter defined originally in the first (genesis) block

- One block produced every ~14s
- Started at 0x400000000 (0.017 TH)

End of Feb 2018

- At 0xAC8166E4E448E (3035 TH)
- Network hash rate 210 TH/s

Energy Consumption by Country inc. Ethereum



Proof of Stake (PoS)

Validators lock Ether into a deposit

- Their **stake**

Validators rewarded for good behaviour

- Reward proportional to **stake**

Validators punished for bad behaviour

- Slash **stake**

PoS Benefits

No power hungry mining

Reduced need for crypto-currency issuance

Less centralisation

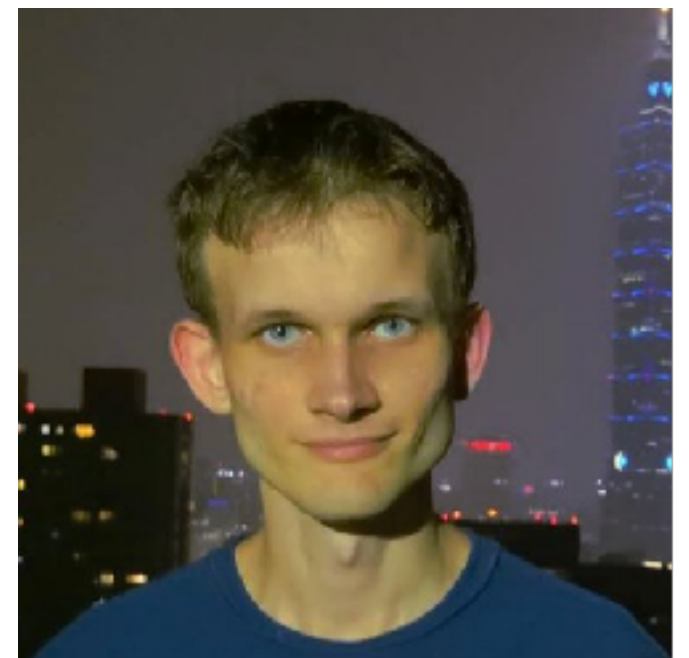
- Economies of scale do not apply

Casper the Friendly Finality Gadget

A.K.A Vitalik's Casper

Near term Ethereum Proof of Stake implementation:

- Hybrid PoW/PoS network
- Checkpoints every 100 blocks
- Introduces transaction finality



Casper the Friendly GHOST

A.K.A Vlad's Casper

Research based Ethereum Proof of Stake implementation:

- Correct by construction (CBC) approach
- Formally specified properties
- Derive protocol to satisfy properties
- Likely to heavily influence full PoS



When can we expect PoS?

How long is a piece of string?

- Originally slated for 2017

Alpha Testnet launched Jan 2018

- Vitalik's Casper
- Stand-alone network

Architecting the Blockchain for Failure

Ethereum & web3j

Failure in Ethereum

Distributed Consensus

Consensus in Ethereum

- Public Network Consensus
- **Consortium Network Consensus**



Private Blockchain Networks



Enterprise Ethereum Clients



ENTERPRISE
ETHEREUM
ALLIANCE

Fork of Geth

- Transaction privacy via secure enclave
- Additional consensus support

More clients in development

Proof of Authority

Set of authority nodes

Majority consensus required

Used in public Ethereum test networks

- Rinkeby (Geth)
- Kovan (Parity)

RAFT

Distributed log replication

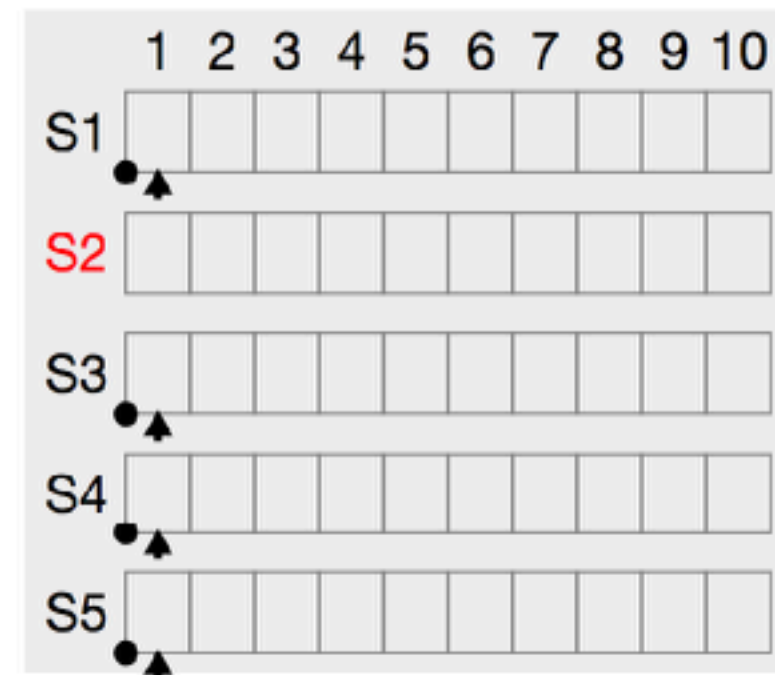
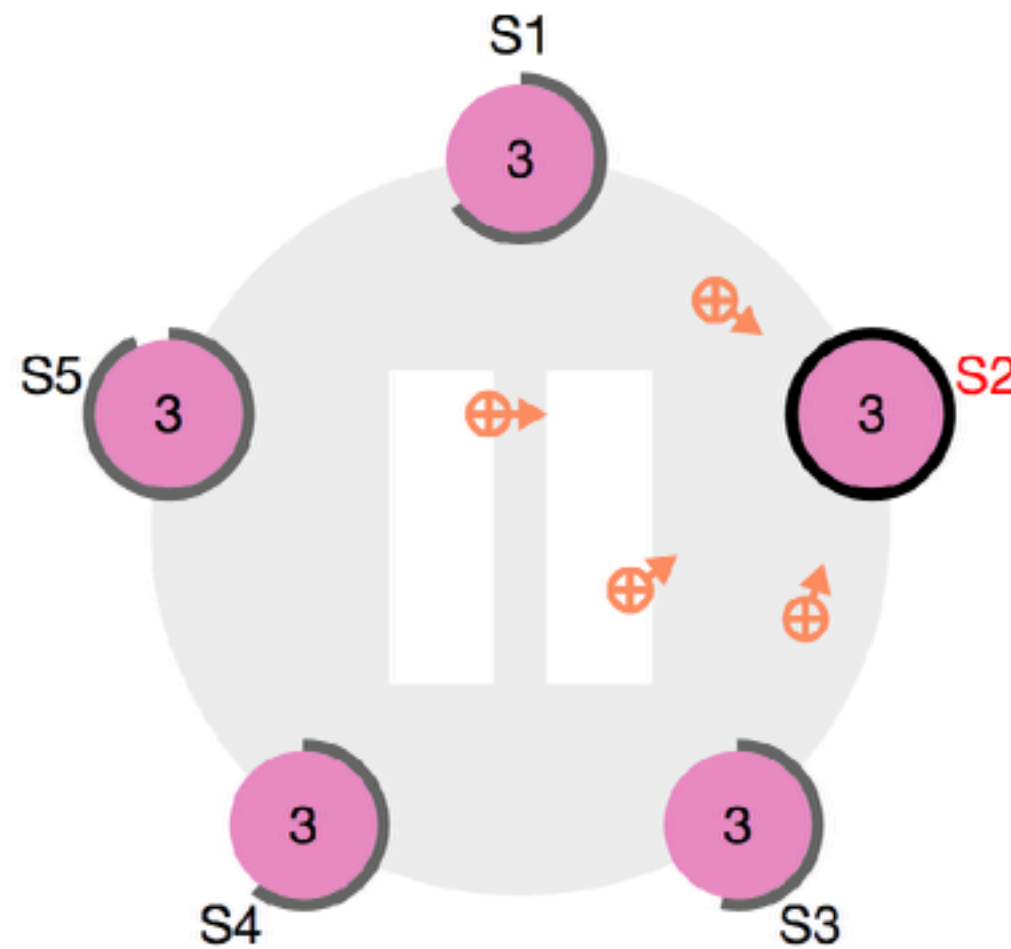
- All nodes start equal
- Leader election
 - Leaders elected by majority voting
- Uses majority consensus



Elected Leader

Node is either:

- Candidate
- Leader (S2)
- Follower



Log Replication

1. New block proposal sent via leader
2. Leader replicates block to followers
3. Majority notify leader of block written
4. Leader commits block
5. Leader notifies followers block is committed

RAFT is not BFT

Bad actor can:

- Ignore/confuse others with random requests
- Trigger a leader election
- Modify inbound requests
- Commit to log before recorded being recorded by Quorum

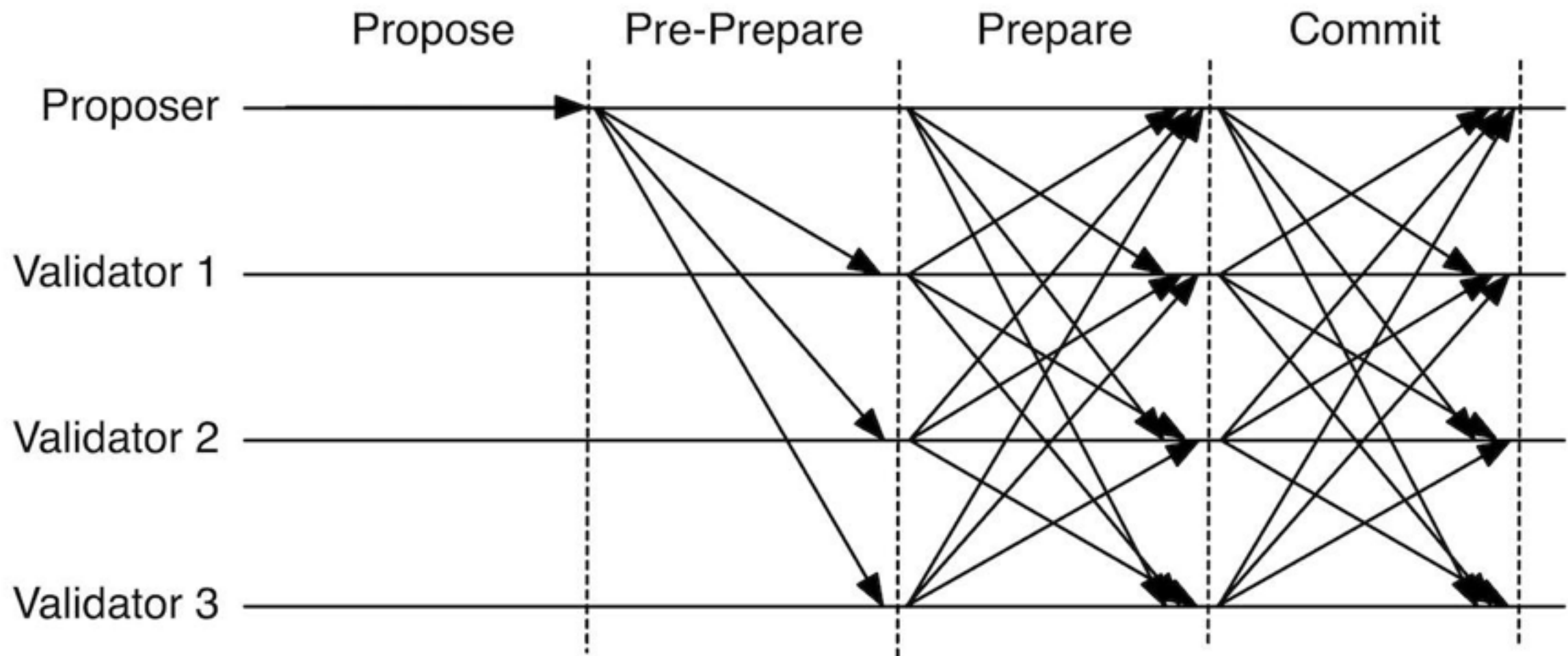
Practical BFT (PBFT)

- Miguel Castro and Barbara Liskov 1999 Paper
- Subset of nodes are validators
- 3-phase consensus
 - Pre-prepare
 - Prepare
 - Commit
- Tolerates f failures, where network validators = $3f + 1$

Istanbul BFT (IBFT) Consensus

1. Validator select new proposer (round-robin)
2. New block proposal broadcast + **PRE-PREPARE**
3. At least $2f + 1$ Validators broadcast **PREPARE**
=> Agreement on block
4. At least $2f + 1$ Validators broadcasts **COMMIT**
=> Agreement on commit
5. Transaction committed to validators

IBFT Consensus



Whirlwind Tour of Consensus

Public network consensus

- Proof of Work (PoW)
- Proof of Stake (PoS)

Private network consensus

- Proof of Authority (PoA)
- RAFT
- Practical Byzantine Fault Tolerance (PBFT)

Wrapping Up

Ethereum

- Ether the Cryptocurrency
- The World Computer
- Asset tokenisation
- web3j

Consensus

- Byzantine (arbitrary) failure
- Consensus in Ethereum networks

Thanks!



Conor Svensson
@conors10



blk.io Founder
web3j Author

