Post-Hype
Blockchain Design

Bulat Nasrulin
b.nasrulin@tudelft.nl

30 January 2020,
Delft
Blockchain Decade

- *December 2009* - First transactions on Bitcoin
- *July 2018* - Over 100,000 ERC20 tokens created
- *Dec 2018* - 90% of banks in EU and US claim to work on blockchain
- Japan accepts Bitcoins, Switzerland accepts crypto for taxes
CryptoKitties and Broken Dreams (Blockchain scalability limits)
State of the art does not scale!

- 128
- 256
- 512
- 1024

<table>
<thead>
<tr>
<th>Nodes participating in the consensus process</th>
<th>Max. transactions (tps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1024</td>
</tr>
<tr>
<td>4</td>
<td>512</td>
</tr>
<tr>
<td>8</td>
<td>256</td>
</tr>
<tr>
<td>16</td>
<td>128</td>
</tr>
<tr>
<td>32</td>
<td>64</td>
</tr>
<tr>
<td>64</td>
<td>32</td>
</tr>
</tbody>
</table>

Consensus Family
- Crash Fault Tolerant
- Delegated Proof-of-Stake
- Practical BFT
- Proof-of-Stake
- Federated BFT
Take a step back
Take a step back

Decentralisation

?  

Global Consensus

Scalability

≈libra

HYPERLEDGER
Take a step back

Decentralisation

? 

Scalability

Global Consensus

Hyperledger

Libra

Ethereum

High throughput
Low latency
Scales to many nodes
Take a step back

Decentralisation

Open membership
No single entity controls the validity of transactions

Scalability
High throughput
Low latency
Scales to many nodes

Global Consensus

Scalability
High throughput
Low latency
Scales to many nodes
Take a step back

Decentralisation

Open membership
No single entity controls the validity of transactions

Consensus
Every peer sees the same value at any time

Global Consensus

Scalability
High throughput
Low latency
Scales to many nodes

Scalability

Decentralisation
Consensus Revisited
Consensus Revisited

Every peer sees the same value at any time
Consensus Revisited

Every peer sees the same value at any time

• Every Peer? Limits scalability
Consensus Revisited

Every peer sees the same value at any time

• Every Peer? Limits scalability

• Same value? Many application allow marginal error and temporary inconsistencies
Every peer sees the same value at any time

- Every Peer? Limits scalability
- Same value? Many application allow marginal error and temporary inconsistencies
- At any time? Impractical with churn and heterogeneous network
Consensus Revisited

*Every peer sees the same value at any time*

- **Every Peer?** Limits scalability
- **Same value?** Many application allow marginal error and temporary inconsistencies
- **At any time?** Impractical with churn and heterogeneous network

*It depends on the application*
Clean-Slate Design

**Finality**
Two signatures are enough

**Tamper-proofness**
Linking transactions in a community

**Integrity Guarantees**
Random Audits and Witnesses
Our scalable solution

Consensus Family

Crash Fault Tolerant
Delegated Proof of Stake
Federated BFT
Practical BFT
Proof of Stake
XChain

Nodes participating in the consensus process

Max. throughput (tps)
Recommendations
Recommendations

• Explore design tradeoffs for your application

• Test and compare your system with others (We need common benchmarks for blockchains)
Recommendations

• Explore design tradeoffs for your application

• Test and compare your system with others (We need common benchmarks for blockchains)
References


- https://jochen-hoenicke.de/queue/#0,24h