The Swiss Blockchain Winter School 2019

Approaching blockchain scalability and governance with Polkadot and Parity Substrate

**Fabian Schulz**  
Technology Adoption @ Parity Technologies Ltd.  

fabian.s@parity.io | @kafabisch
One size doesn’t fit all
# The two sides of blockchain

<table>
<thead>
<tr>
<th>State transition function</th>
<th>Consensus</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Runtime’ / Business logic</td>
<td>Safety and liveness</td>
</tr>
<tr>
<td>What are the changes that are agreed upon?</td>
<td>How do we agree on what changes to include</td>
</tr>
<tr>
<td>Transactions, balances, contracts etc. all abstracted</td>
<td>Game-theoretically sound incentivization scheme</td>
</tr>
</tbody>
</table>
Specialization vs generalization

Current engineering bias

generalised  specialized
flexibility  optimization

Tension
Application-specific blockchains

- **Performance**  Single-app optimised state machine
- **Security**  Attack surface of VM is smaller
- **Sovereignty**  Not dependent on platform governance
- **Flexibility**  Not bound to platform limitations

- **Network effects**  Loss of access to data on other chains
- **Engineering effort**  Building a blockchain from scratch
Application-specific blockchains

- **Performance**  Single-app optimised state machine
- **Security**  Attack surface of VM is smaller
- **Sovereignty**  Not dependent on platform governance
- **Flexibility**  Not bound to platform limitations

- **Network effects**  Loss of access to data on other chains
- **Engineering effort**  Building a blockchain from scratch
Parachains

Relay Chain
Teams building on Polkadot

- **0x Protocol**  Decentralized exchange
- **Aragon**  Unstoppable organizations, DAOs
- **ChainX**  Developing a Bitcoin and Ethereum bridge
- **Ocean Protocol**  Ecosystem for sharing data
- **Edgeware**  Wasm-based smart contract platform

... and more
Nested Relay Chain Design
Implications on **security**
and governance
Pooled security

Traditional isolated security

Validators

Blockchains

65 %

35 %

Multichain pooled security

Validators

Blockchains

Consensus

100 %
<table>
<thead>
<tr>
<th>Name</th>
<th>Symbol</th>
<th>Market Cap</th>
<th>Algorithm</th>
<th>Hash Rate</th>
<th>1h Attack Cost</th>
<th>NiceHash-able</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>BTC</td>
<td>$60.71 B</td>
<td>SHA-256</td>
<td>41,485 PH/s</td>
<td>$252,749</td>
<td>0%</td>
</tr>
<tr>
<td>Ethereum</td>
<td>ETH</td>
<td>$11.28 B</td>
<td>Ethash</td>
<td>135 TH/s</td>
<td>$64,834</td>
<td>5%</td>
</tr>
<tr>
<td>Bitcoin Cash</td>
<td>BCH</td>
<td>$2.09 B</td>
<td>SHA-256</td>
<td>1,360 PH/s</td>
<td>$8,285</td>
<td>3%</td>
</tr>
<tr>
<td>Litecoin</td>
<td>LTC</td>
<td>$2.06 B</td>
<td>Scrypt</td>
<td>205 TH/s</td>
<td>$21,301</td>
<td>6%</td>
</tr>
<tr>
<td>Bitcoin SV</td>
<td>BSV</td>
<td>$1.09 B</td>
<td>SHA-256</td>
<td>1,190 PH/s</td>
<td>$7,253</td>
<td>3%</td>
</tr>
<tr>
<td>Monero</td>
<td>XMR</td>
<td>$726.91 M</td>
<td>CryptoNightV8</td>
<td>693 MH/s</td>
<td>$4,986</td>
<td>2%</td>
</tr>
<tr>
<td>Dash</td>
<td>DASH</td>
<td>$585.42 M</td>
<td>X11</td>
<td>2 PH/s</td>
<td>$5,030</td>
<td>28%</td>
</tr>
<tr>
<td>Ethereum Classic</td>
<td>ETC</td>
<td>$420.47 M</td>
<td>Ethash</td>
<td>8 TH/s</td>
<td>$3,828</td>
<td>85%</td>
</tr>
<tr>
<td>Zcash</td>
<td>ZEC</td>
<td>$281.30 M</td>
<td>Equihash</td>
<td>3 GH/s</td>
<td>$11,104</td>
<td>6%</td>
</tr>
<tr>
<td>Bitcoin Gold</td>
<td>BTG</td>
<td>$167.54 M</td>
<td>Zhash</td>
<td>3 MH/s</td>
<td>$704</td>
<td>13%</td>
</tr>
</tbody>
</table>

**PoW 51% attack cost**
The weakest link problem

Chain 1  Staked Finality with $3M security

Chain 2  Staked Finality with $10M security
The weakest link problem

Chain 1  Staked Finality with $3M security - validator set misbehaved

Chain 2  Staked Finality with $10M security
Pooled security

Traditional isolated security

Validators

Blockchains 65% 35%

Multichain pooled security

Consensus

100%
Implications on security and governance
Governance

- Referenda
- Adaptive quorum biasing
- Council
- Lock-voting  Hodler Bonus
- Delayed enactments
- Treasury
- Delegated voting  Planned
TURNOUT DEPENDS ON STAKES

<table>
<thead>
<tr>
<th>Governance Proposal</th>
<th>% Voter Turnout</th>
</tr>
</thead>
<tbody>
<tr>
<td>German Election</td>
<td>80</td>
</tr>
<tr>
<td>Brexit</td>
<td>76</td>
</tr>
<tr>
<td>US 2016 Elections</td>
<td>75</td>
</tr>
<tr>
<td>DASH Masternodes</td>
<td></td>
</tr>
<tr>
<td>Decred Politeia</td>
<td></td>
</tr>
<tr>
<td>EOS Block Producer</td>
<td></td>
</tr>
<tr>
<td>Ethereum Hard Fork (2016)</td>
<td></td>
</tr>
<tr>
<td>Aragon AGP-1</td>
<td></td>
</tr>
</tbody>
</table>

Sources: Tezos Foundation, TzScan.io, DASH website, StakingRewards.com, EOS Authority voting statistics, Decred website and dcrostats.com, Cryptoslate, NEO.edu, Coinmonks

Adaptive quorum biasing
Governance

- Referenda
- Adaptive quorum biasing
- Council
- Lock-voting Hodler Bonus
- Delayed enactments
- Treasury
- Delegated voting Planned

\[\text{aye} \times \sqrt{\text{turnout}} > \text{nay} \quad \text{Positive turnout bias}\]

<table>
<thead>
<tr>
<th>Turnout</th>
<th>Ayes to carry (Voting)</th>
<th>Ayes to carry (Electorate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1%</td>
<td>91%</td>
<td>0.9%</td>
</tr>
<tr>
<td>5%</td>
<td>82%</td>
<td>4%</td>
</tr>
<tr>
<td>20%</td>
<td>69%</td>
<td>14%</td>
</tr>
<tr>
<td>50%</td>
<td>59%</td>
<td>29%</td>
</tr>
</tbody>
</table>
Governance

- Referenda
- Adaptive quorum biasing
- Council
- **Lock-voting** ‘Hodler Bonus’ \( \text{Votes} = \text{Tokens} \times \text{Weeks} \) \( \text{Max. 12 weeks} \)
- Delayed enactments
- Treasury
- Delegated voting **Planned**
Forkless upgrades
Application-specific parachains

- **Performance**  Single-app optimised state machine
- **Security**  Attack surface of VM is smaller
- **Sovereignty**  Not dependent on platform governance
- **Flexibility**  Not bound to platform limitations

- **Network effects**  Loss of access to data on other chains
- **Engineering effort**  Building a blockchain from scratch
What is Parity Substrate?

Substrate is an open source, extensible framework for building blockchains.

It is modular.

It allows hot-upgrades of the internal runtime through WebAssembly.
ACCOUNTS & BALANCES
- Basic cryptocurrency
- Good for staking & tees

INDEXED ACCOUNTS
- Short account IDs
- 1-2 bytes

SESSIONS
- Key rotation for authorities

TIMESTAMP
- Have your chain know about time

STAKING
- Our POS logic

ASSETS
- Simple, secure additional on-chain fungible assets

TREASURY
- Decentralised grants

REFERENDA
- Basic coin-vote governance binding

CONTRACTS
- Turbo-charged Wasm-based smart contracts with robust Rust-based language

COUNCIL
- Approval-voted governance executive adjunct

Many more planned
libp2p

CONSENSUS

WEBASSEMBLY

RUNTIME
- governance
- dao
- staking
- slashing
- csprng
- parachains
- permissions
- smart contracts

Written in Rust
Built into both Wasm & native
Wasm stored on-chain

Written in Rust
Built into native

libp2p

Substrate building components
Forkless runtime upgrades

Native client environment

ENTRY APIs

Native runtime is same version as on-chain runtime?

✔

✗

WebAssembly interpreter

Wasm runtime (from chain)

Native runtime (from client)

Merklised storage database
**Polkadot:**
Web3 Foundation, protocol, token, many teams, implementations

**Substrate:**
Parity Technologies, software stack, Substrate chains, many tokens and chains
Parity updates and events

parity.io/newsletter
We’re hiring!

parity.io/jobs
THE STATE OF CHAINS

**Substrate**

**SOLO CHAIN**
- Consensus
- Needs economic incentivisation
- Completely Sovereign

**SOLO CHAIN + BRIDGE**
- Communication Possible
- Restricted state possible
- Own consensus possible
- Completely sovereign

**PARACHAIN**
- Uses Polkadot Relay Consensus
- Uses Polkadot Relay Validation
- Open for all to verify/validate
- No economic incentivisation needed
- Sovereign over state transitions
Compound Your Crypto

Staked helps institutional investors reliably and securely compound their crypto by 5% - 100% annually through staking and lending.

Proof of Stake is replacing Proof of Work

~25% of the total cryptocurrency market (~$25 billion today) will use proof-of-stake (PoS) as a security model by the end of 2019. Investors of...
The largest true staking services provider.

We’ve developed the leading crypto infrastructure to earn and share staking rewards with coin holders.

Grow your coins

Join our Private Beta  
Apply