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

parity

One size doesn’t fit all

parity

The two sides of blockchain

State transition function

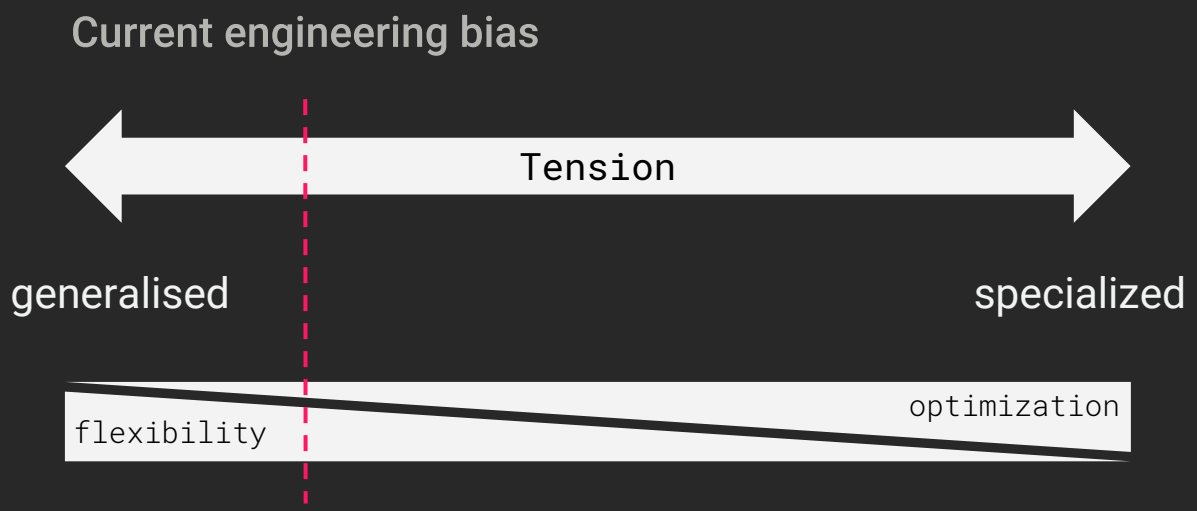
- ‘Runtime’ / Business logic
- What are the changes that are agreed upon?
- Transactions, balances, contracts etc. all abstracted

Consensus

- Safety and liveness
- How do we agree on what changes to include
- Game-theoretically sound incentivization scheme

parity

Specialization vs generalization



parity

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

parity

Application-specific blockchains

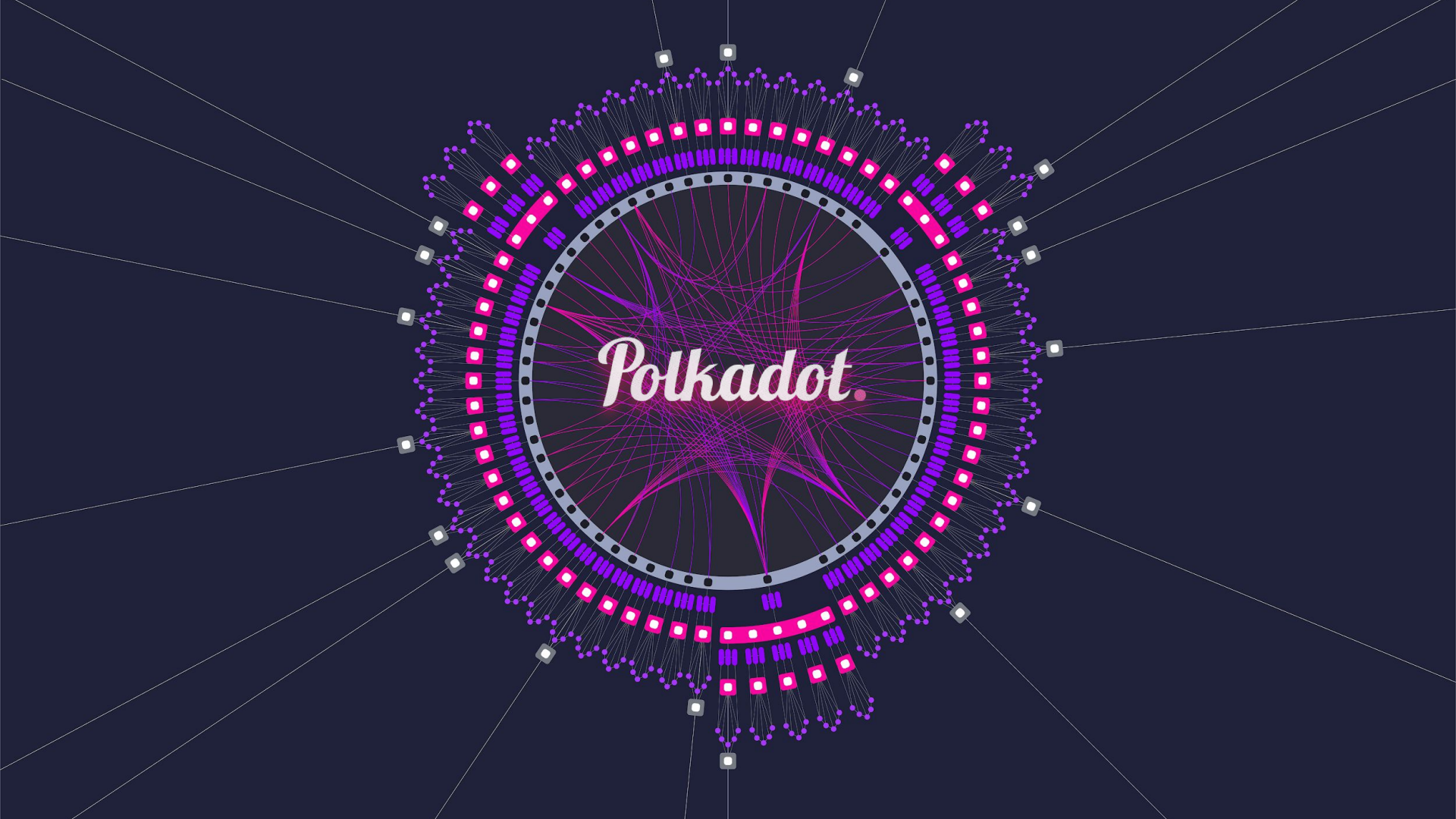
+

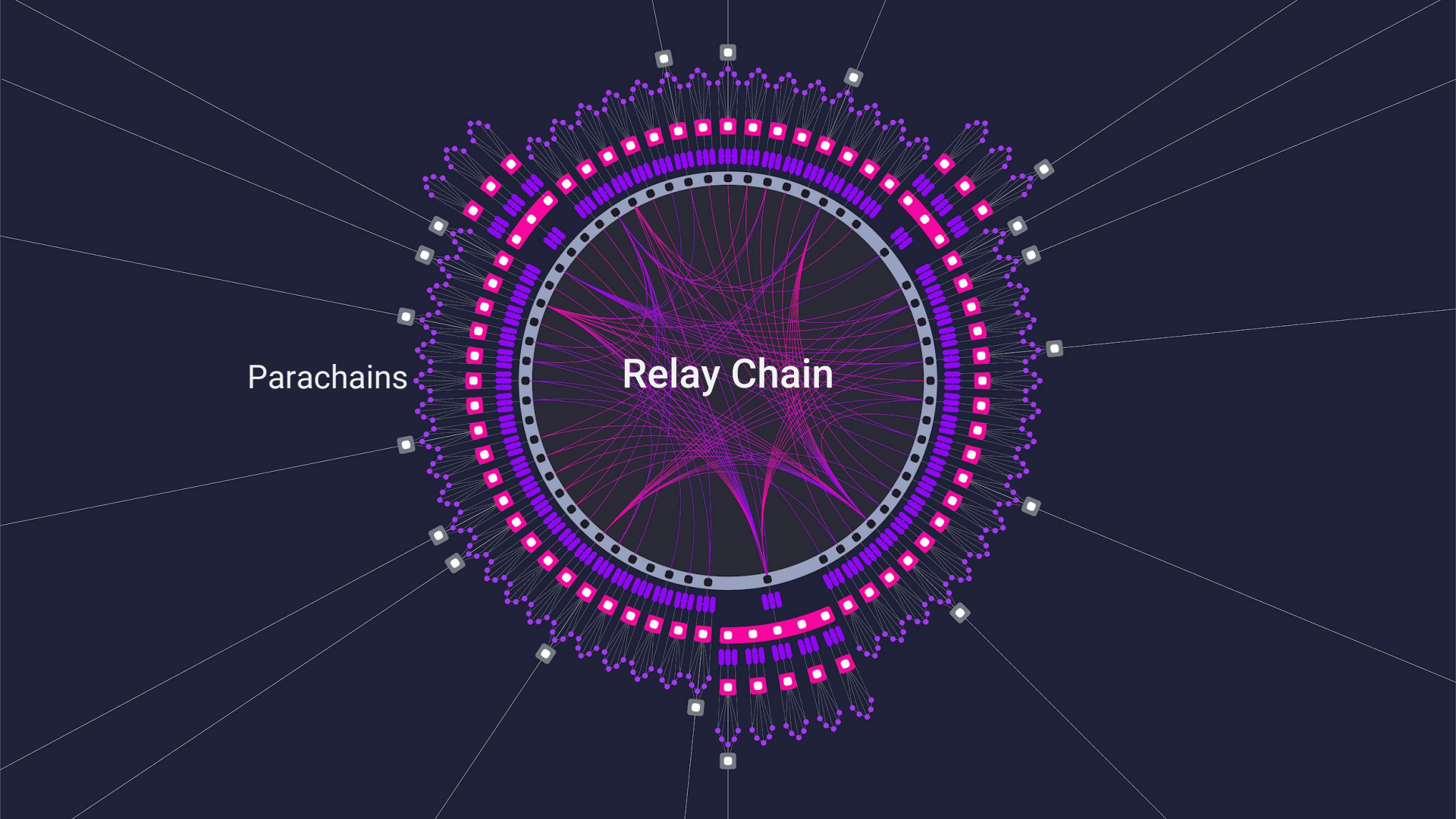
- **Performance** Single-app optimised state machine
- **Security** Attack surface of VM is smaller
- **Sovereignty** Not dependent on platform governance
- **Flexibility** Not bound to platform limitations

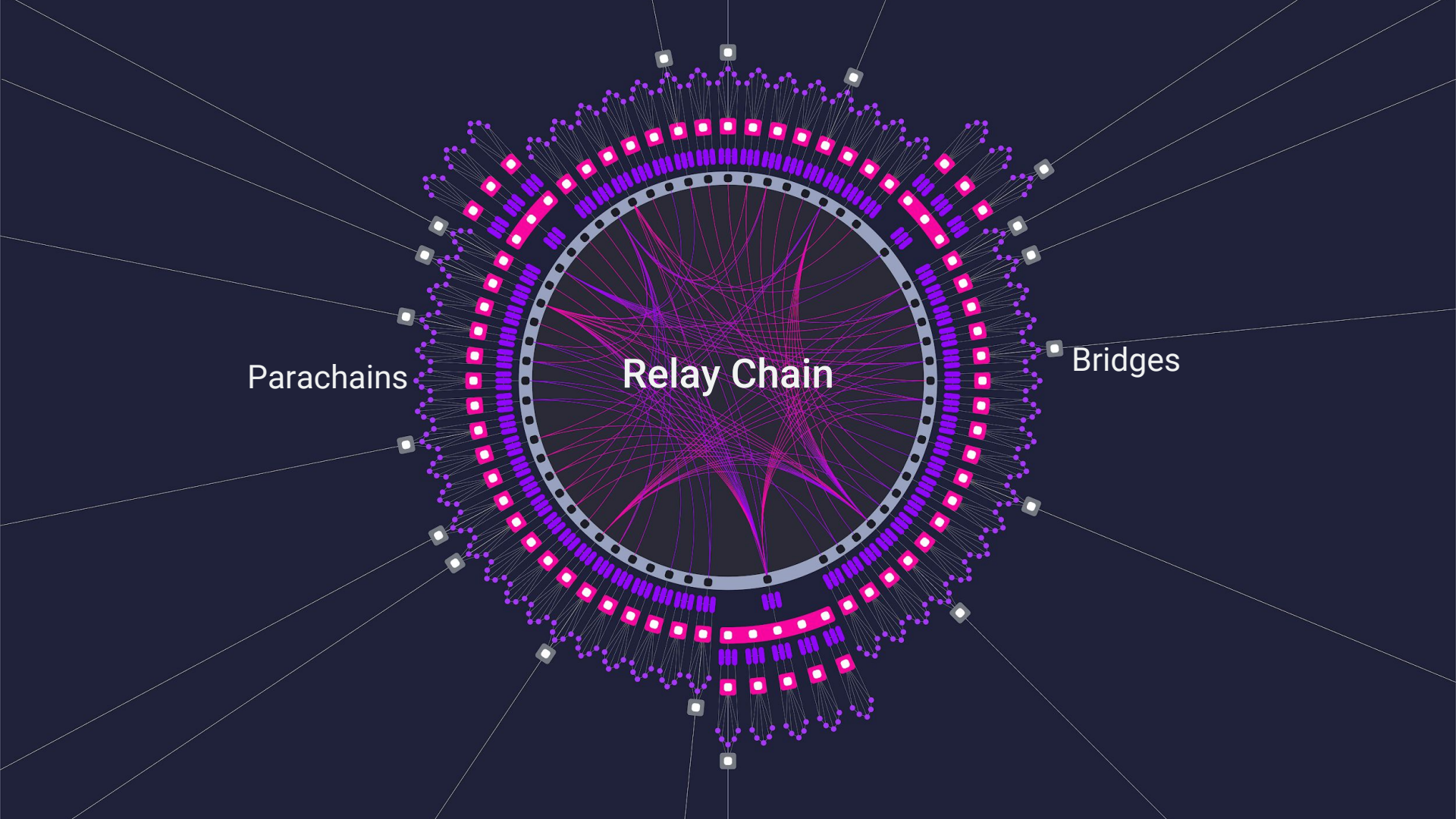
—

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

parity


Polkadot.


Parachains
Relay Chain

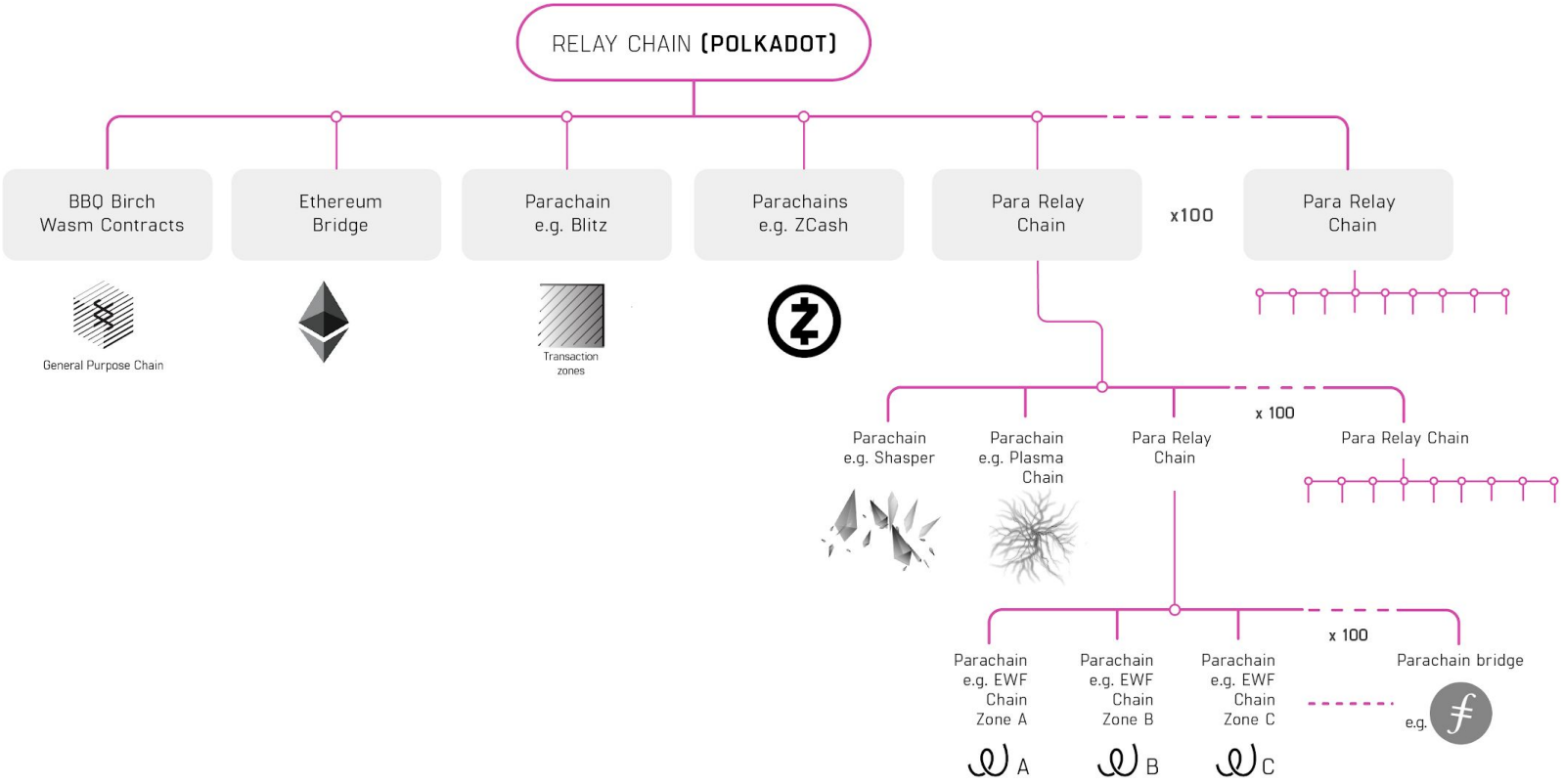

Parachains
Relay Chain
Bridges

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

parity



Nested Relay Chain Design

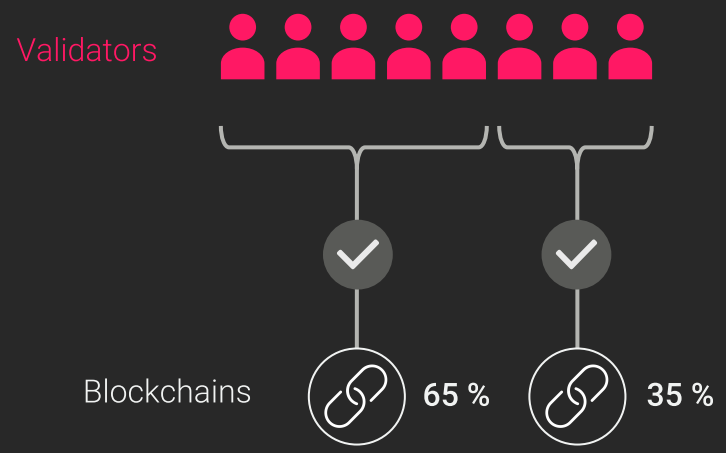
Polkadot.

Implications on security and governance

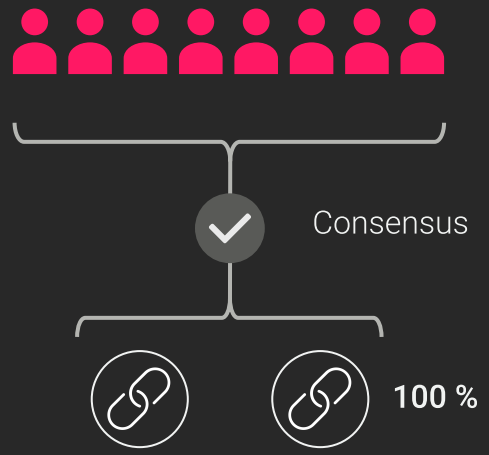
parity

Pooled security

Traditional isolated security



Multichain pooled security



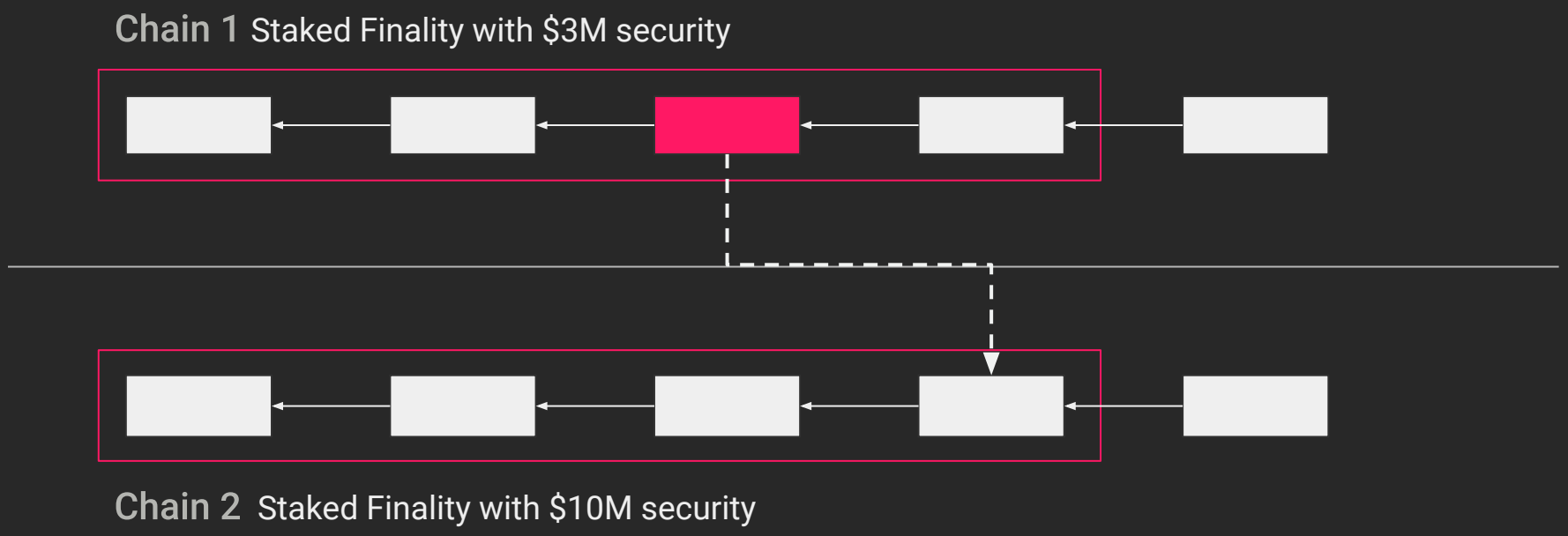
parity

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

PoW 51% attack cost

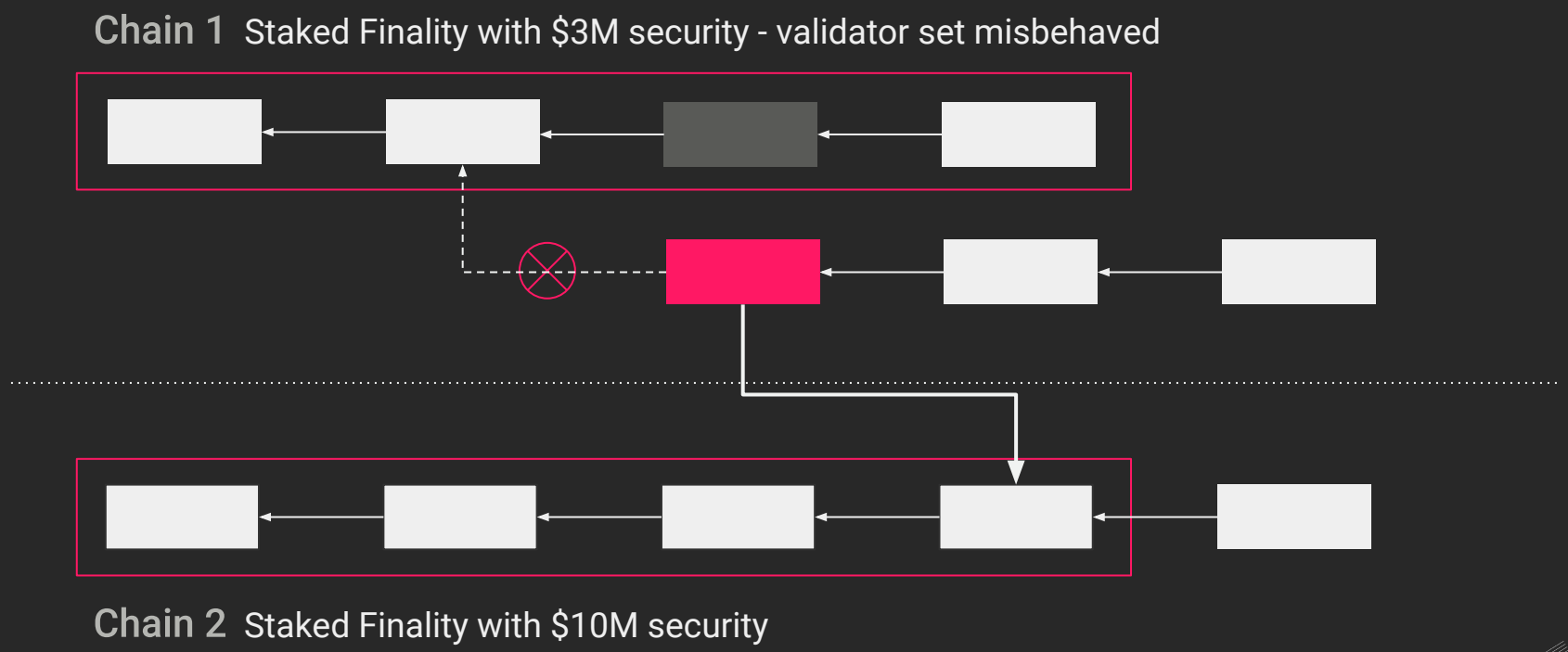
crypto51.app

The weakest link problem



parity

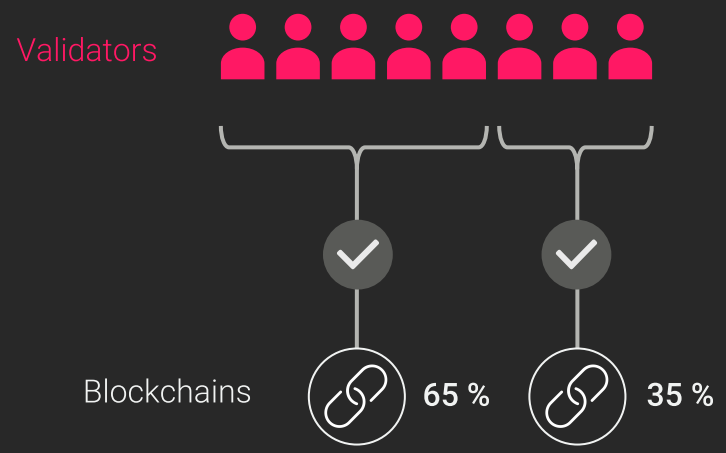
The weakest link problem



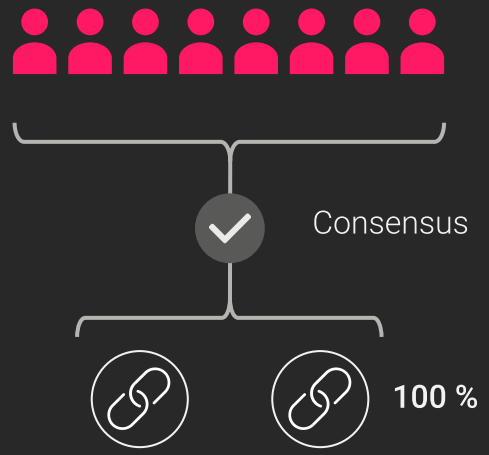
parity

Pooled security

Traditional isolated security



Multichain pooled security



parity

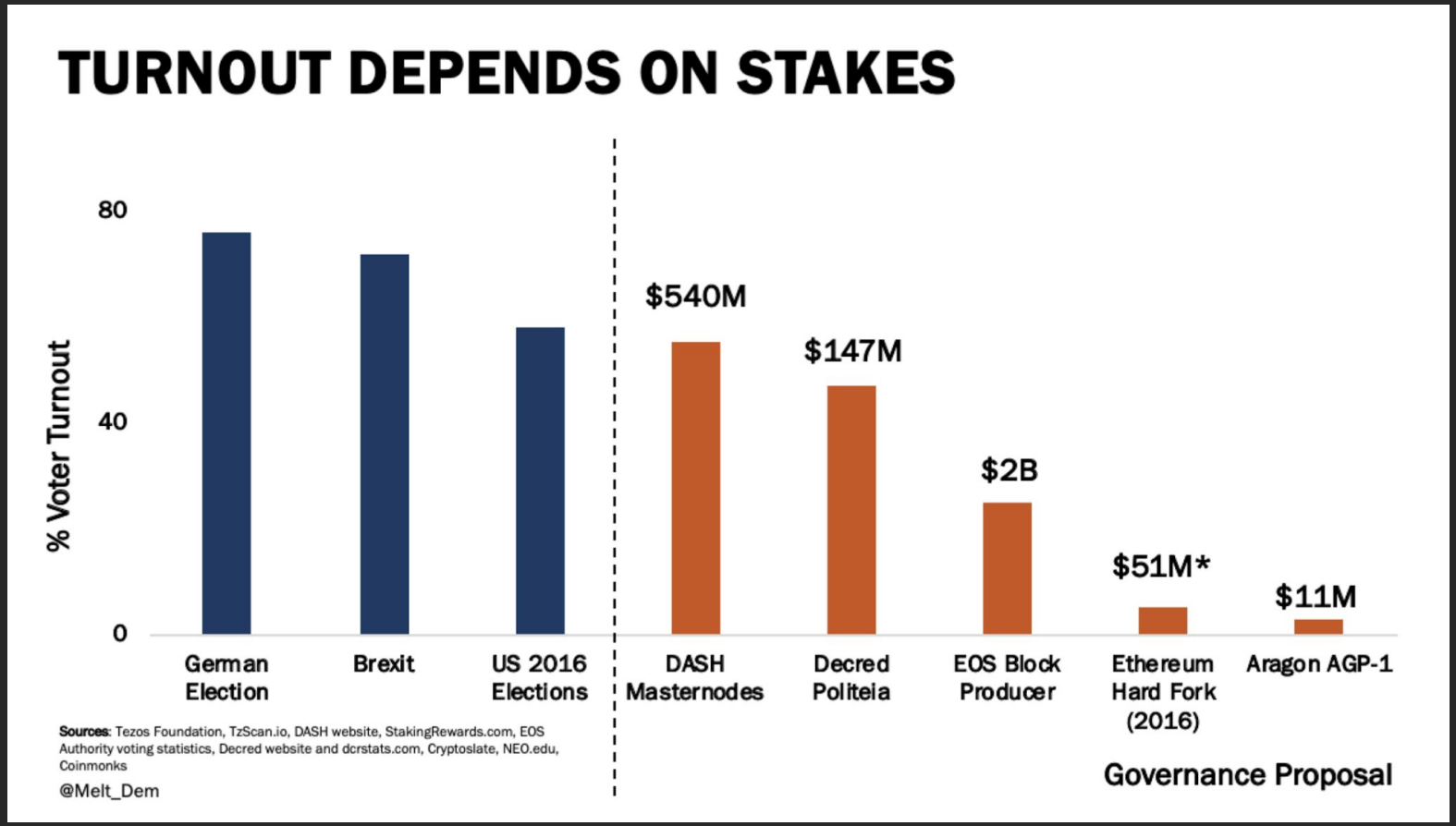
Implications on security and governance

parity

Governance

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

parity



Adaptive quorum biasing

Governance

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

aye * √turnout > nay Positive turnout bias

Turnout	Ayes to carry (Voting)	Ayes to carry (Electorate)
1%	91%	0.9%
5%	82%	4%
20%	69%	14%
50%	59%	29%

parity

Governance

- Referenda
- Adaptive quorum biasing
- Council
- Lock-voting ‘Hodler Bonus’ Votes = Tokens * Weeks Max. 12 weeks
- Delayed enactments
- Treasury
- Delegated voting Planned

parity

Forkless upgrades

parity

Application-specific parachains

+

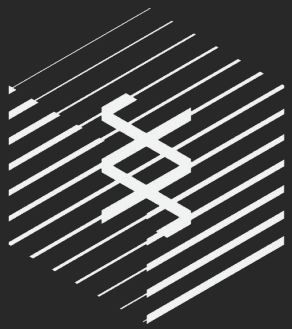
- **Performance** Single-app optimised state machine
- **Security** Attack surface of VM is smaller
- **Sovereignty** Not dependent on platform governance
- **Flexibility** Not bound to platform limitations

—

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

parity

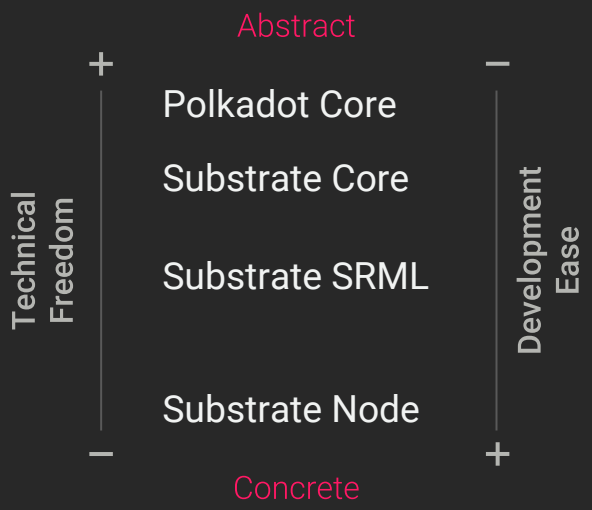
What is Parity Substrate?



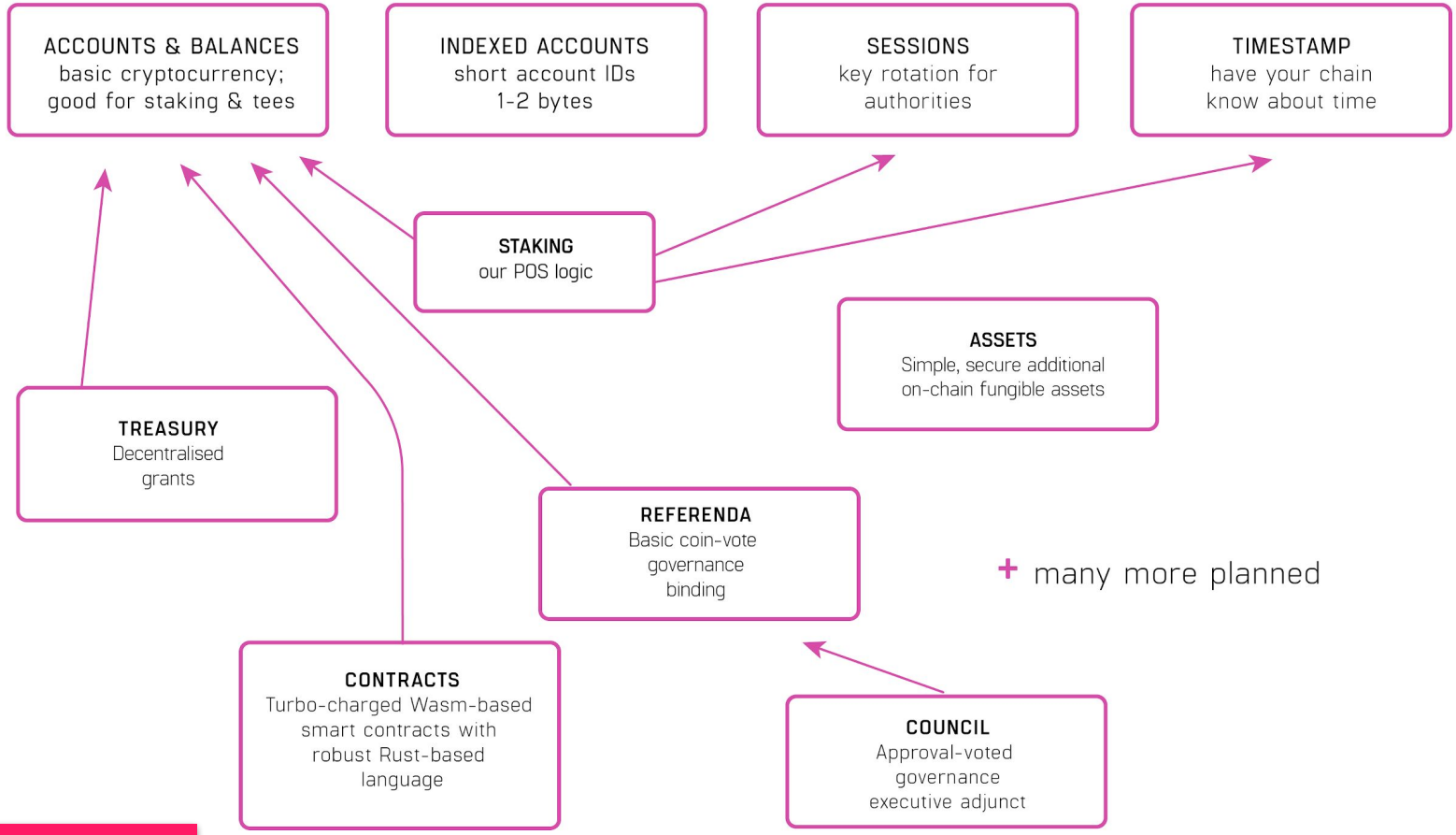
Substrate is an open source, extensible framework for building blockchains.

It is modular.

It allows hot-upgrades of the internal runtime through WebAssembly.



parity



Advantages of SRML

Written in Rust

Built into both Wasm & native

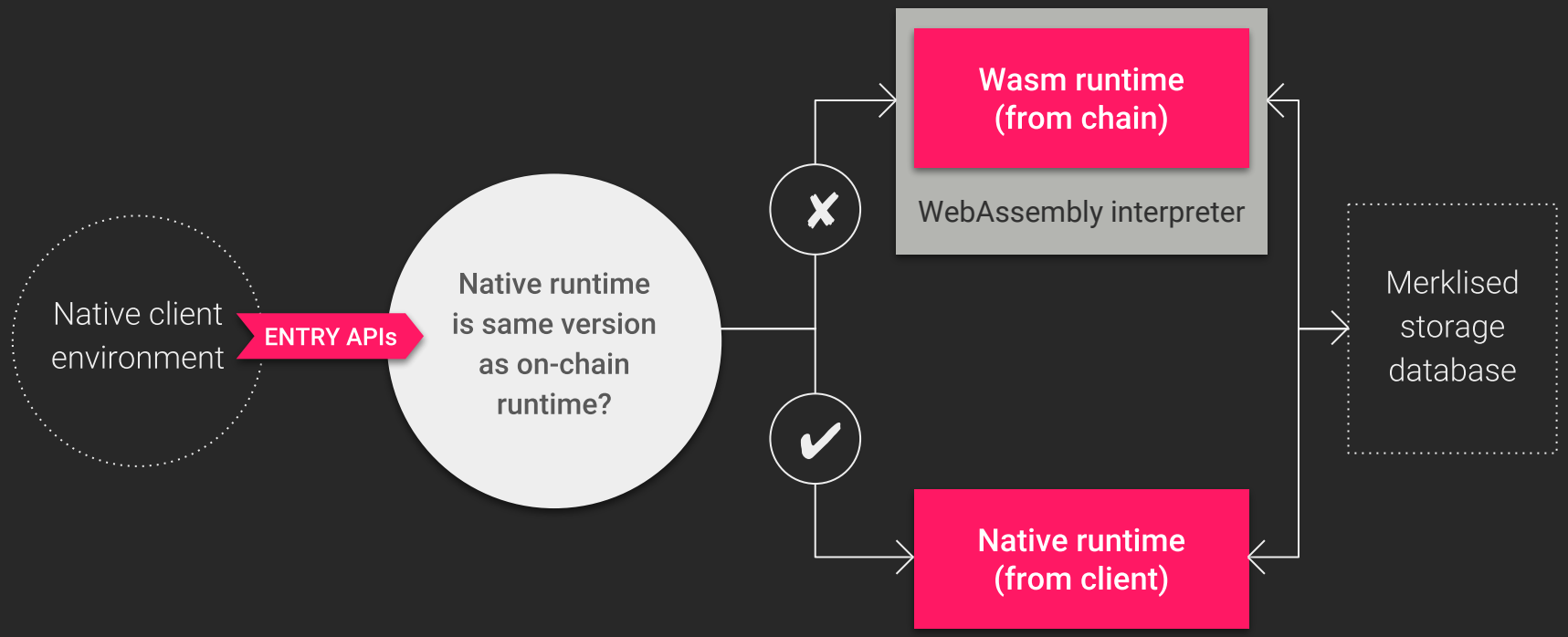
Wasm stored on-chain

Written in Rust

Built into native

Substrate building components

parity



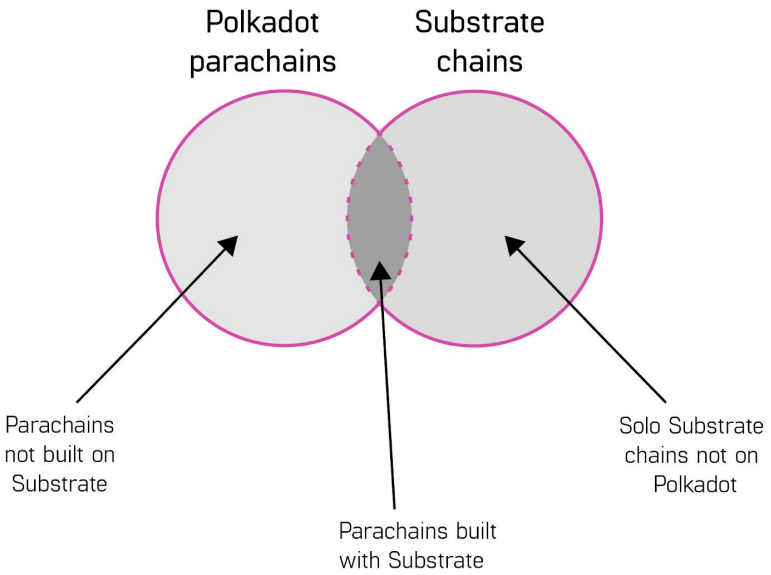
Forkless runtime upgrades

parity

Polkadot	Protocol	“Ethernet”
Substrate	Software	“PC”

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

parity

We're hiring!

parity.io/jobs

parity

github.com/paritytech/substrate
parity.io
@ParityTech

github.com/paritytech/polkadot
polkadot.network
@polkadotnetwork

github.com/w3f
web3.foundation
@web3foundation

Questions?

fabian.s@parity.io
@kafabisch

parity

THE STATE OF CHAINS
Substrate

SOLO CHAIN

Consensus

Needs economic incentivisation

Completely Sovereign

SOLO CHAIN + BRIDGE

SAME + CONNECTIVITY

Communication Possible

Restricted state possible

Own consensus possible

Completely sovereign

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

	2018 June	Oct	Nov	Dec	2019 Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec
Polkadot	**POC-2**	**POC-3** Final Consensus GRANPA			**POC-4** Interchain Messaging Final Staking Algo		**POC-5** Audit - Ready Security Final Slashing & Consensus	Polish & Optimisation			**1.0 RELEASE CANDIDATE 1**		1.0 RCL	1.0 FINAL	**GENESIS**	
Substrate	**POC-2**	**1.0 beta**			**1.0 RCI** Docs Final API Consensus		**1.0**	**1.1** Improved SC Tooling		**1.2** Collator Parachain Node	Bridge beta					

Compound Your Crypto

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

GET STARTED

Decred 12.5%	Livepeer 155.5%	Tezos 8.0%	Algorand Q2-19
Cosmos 15.0%	Dash 7.0%	Ethereum Q4-19	NuCypher 75.0%

$2.5BN+

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

BATTLESTAR

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