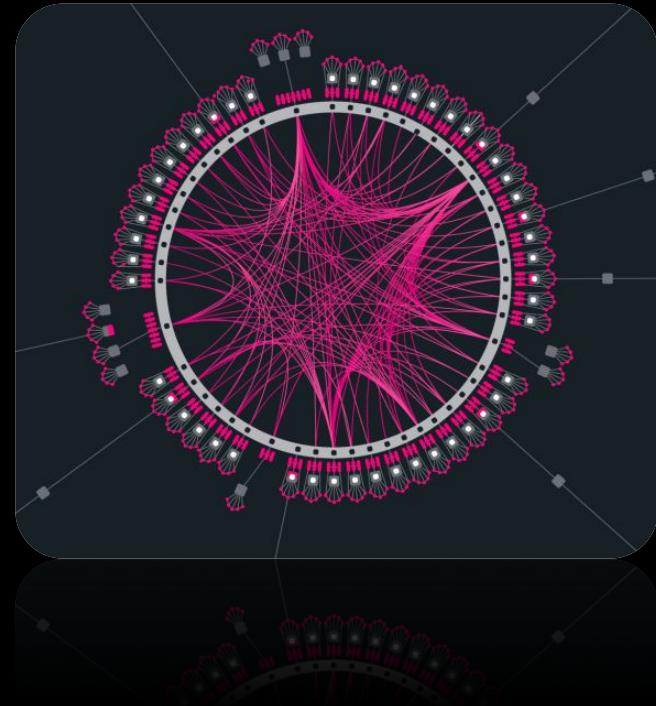
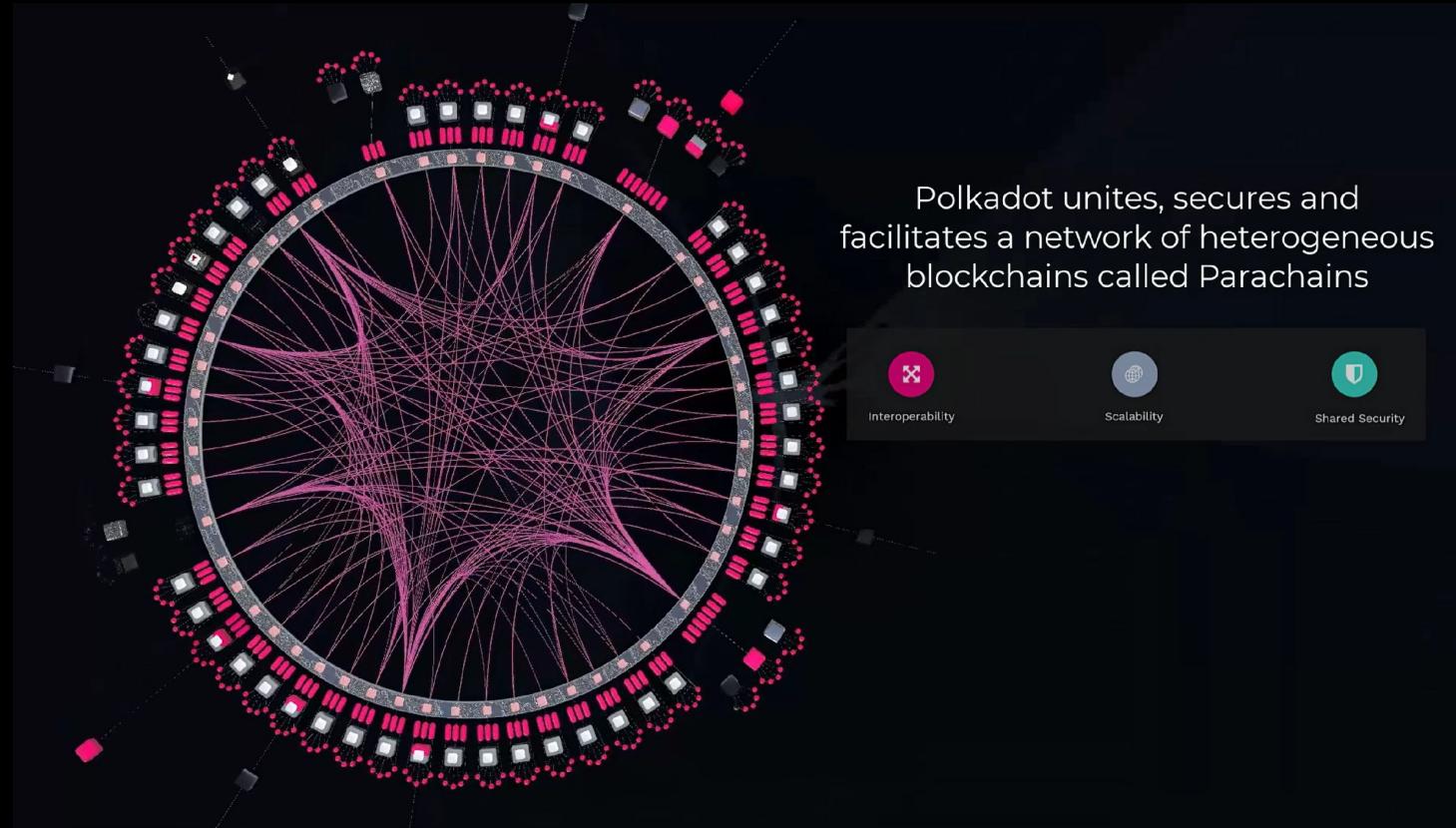




# Polkadot 101

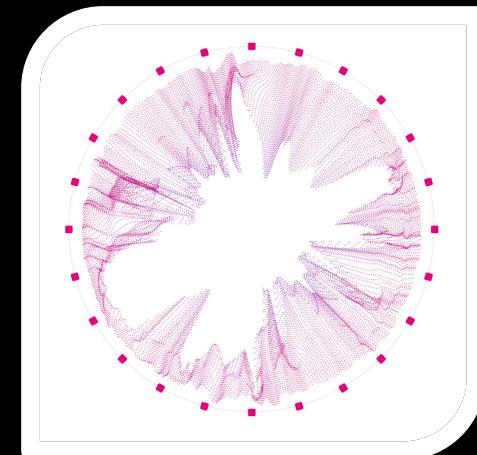


Polkadot is a heterogeneous multichain that connects and secures blockchains with pooled security and interoperability.



Polkadot can provide security for sequential parachain blocks in parallel

“Polkadot is **built to connect** public and permissionless networks, private and consortium chains, oracles, and future technologies that are yet to be created.”



## Polkadot Architecture (Layer 0) :

### RELAY CHAIN

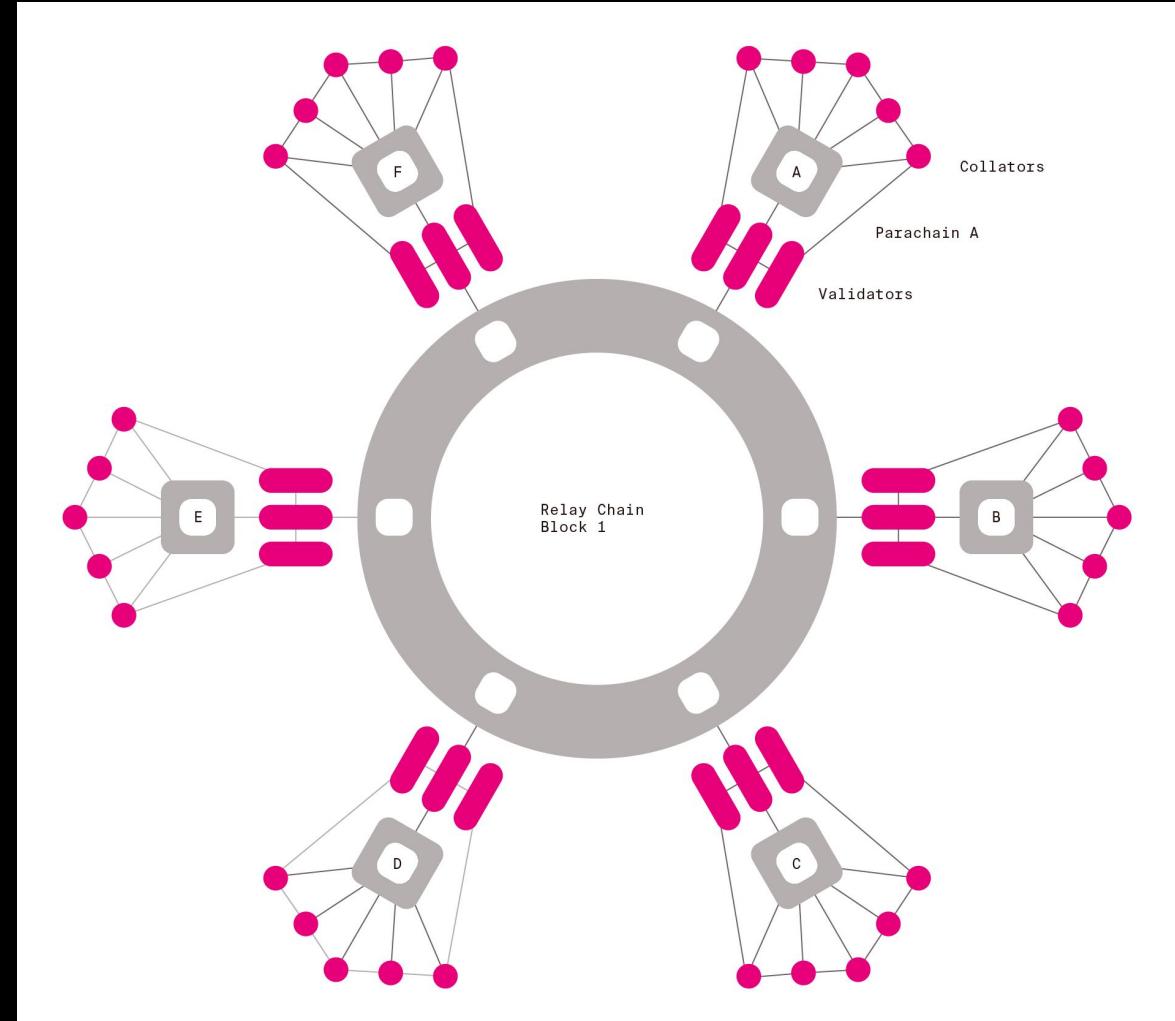


The connector chain of Polkadot that provides strong economic security and an interoperability protocol.

### PARACHAINS



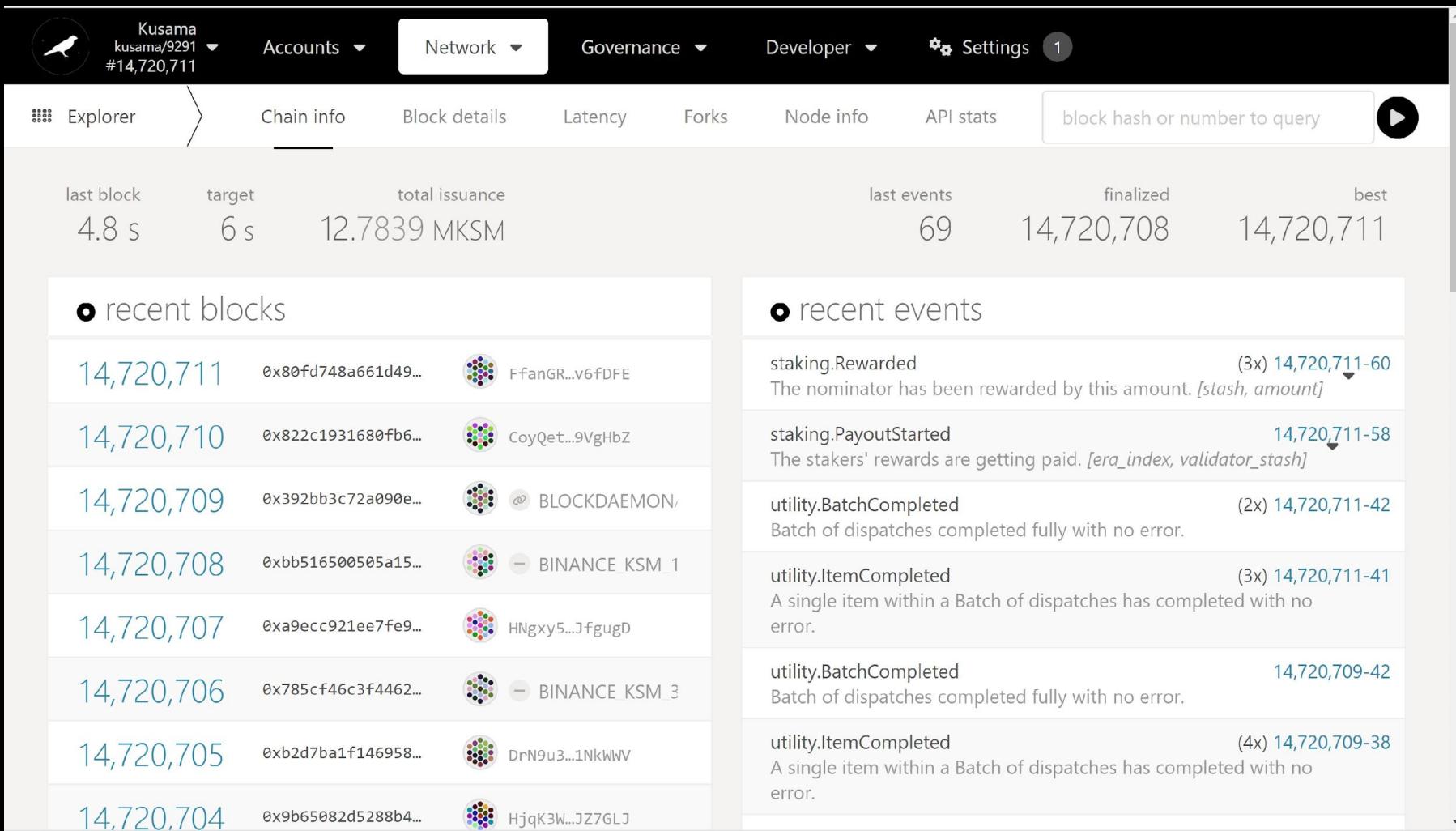
Third-party chains that connect to Polkadot for interoperability, scalability, and pooled security.





# Kusama: Polkadot's Canary Network

# Kusama Network



The screenshot shows the Polkadot.js.org interface for the Kusama Network. At the top, there's a navigation bar with tabs for Accounts, Network (selected), Governance, Developer, and Settings. A search bar at the top right allows querying by block hash or number. Below the navigation, there are summary metrics: last block (4.8 s), target (6 s), total issuance (12.7839 MKSM), last events (69), finalized (14,720,708), and best (14,720,711). Two main sections are displayed: "recent blocks" on the left and "recent events" on the right.

### recent blocks

Block Number	Hash	Validator
14,720,711	0x80fd748a661d49...	FfanGR...v6fDFE
14,720,710	0x822c1931680fb6...	CoyQet...9VgHbz
14,720,709	0x392bb3c72a090e...	@ BLOCKDAEMON
14,720,708	0xbb516500505a15...	- BINANCE KSM 1
14,720,707	0xa9ecc921ee7fe9...	HNgxy5...JfgugD
14,720,706	0x785cf46c3f4462...	- BINANCE KSM 3
14,720,705	0xb2d7ba1f146958...	DrN9u3...1NkWWV
14,720,704	0x9b65082d5288b4...	HjqK3W...JZ7GLJ

### recent events

Event Type	Block Number	Description
staking.Rewarded	(3x) 14,720,711-60	The nominator has been rewarded by this amount. [stash, amount]
staking.PayoutStarted	14,720,711-58	The stakers' rewards are getting paid. [era_index, validator_stash]
utility.BatchCompleted	(2x) 14,720,711-42	Batch of dispatches completed fully with no error.
utility.ItemCompleted	(3x) 14,720,711-41	A single item within a Batch of dispatches has completed with no error.
utility.BatchCompleted	14,720,709-42	Batch of dispatches completed fully with no error.
utility.ItemCompleted	(4x) 14,720,709-38	A single item within a Batch of dispatches has completed with no error.

Blockchains can be built to do a few things really well



Custom blockchain built on top of Polkadot



Blockchains can also be built to attempt to do a lot things





web3  
foundation



Polkadot connects a network of custom-built blockchains

Blockchains are custom-built on Polkadot for specific uses

Example custom blockchains: IOT, finance, insurance, gaming, music, identity, government, data storage

# The challenges of custom Blockchains



**Overhead**

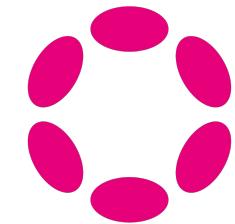
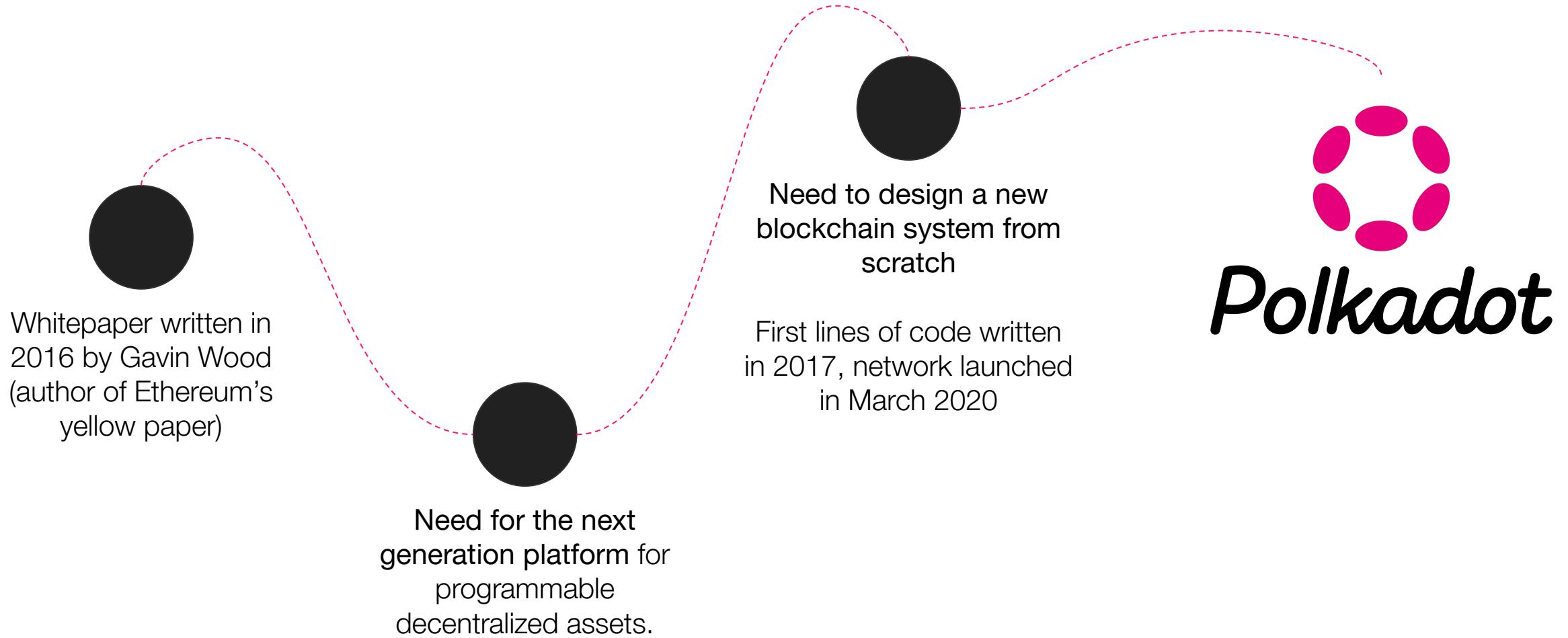


**Isolation**

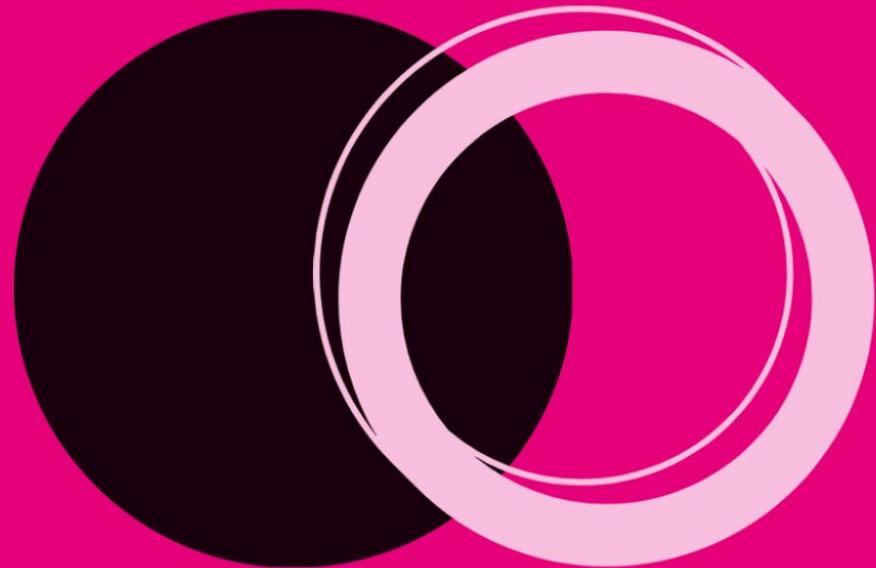


**Security**

## The path to Polkadot



**Polkadot**

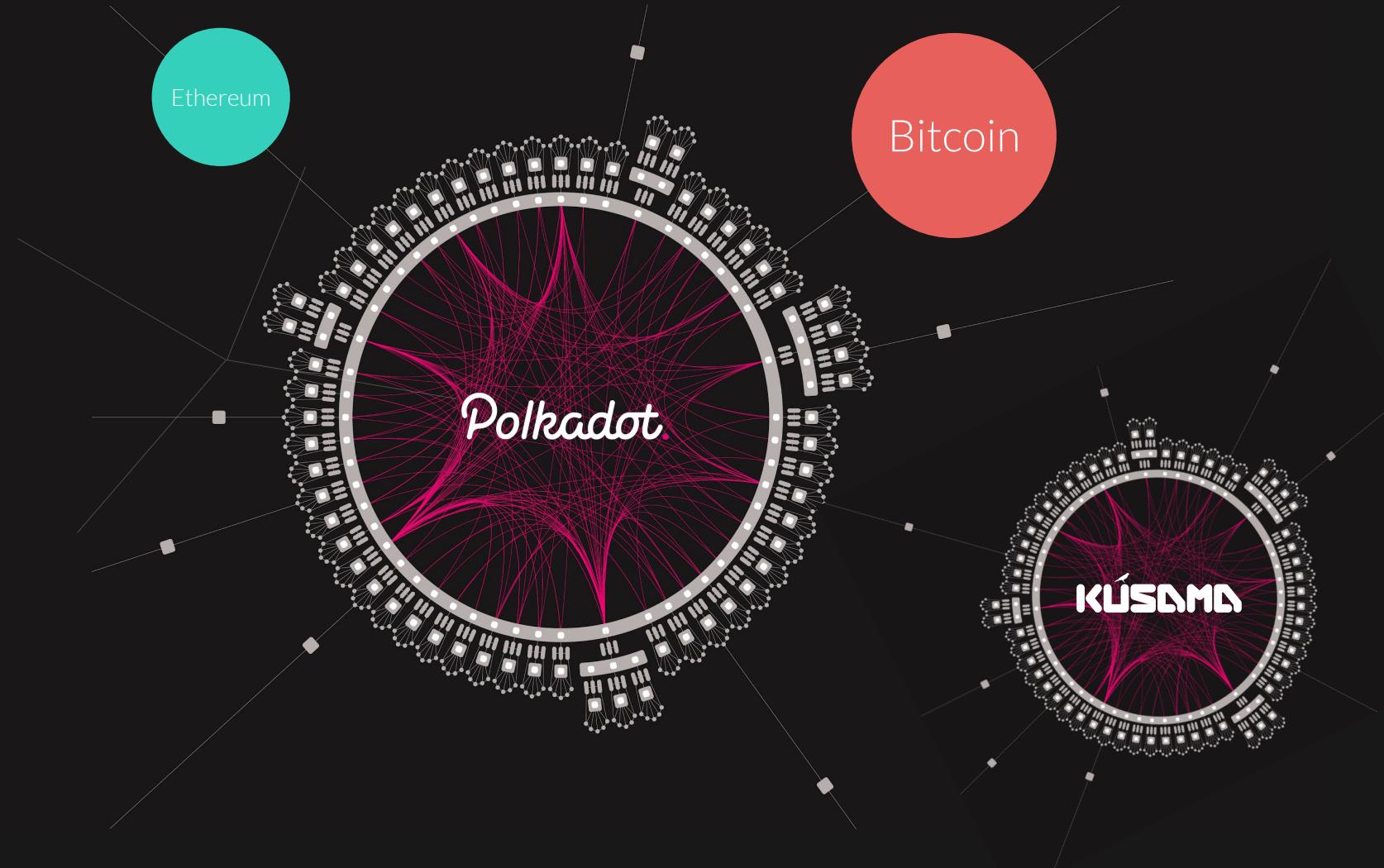


# Blockchain Interoperability



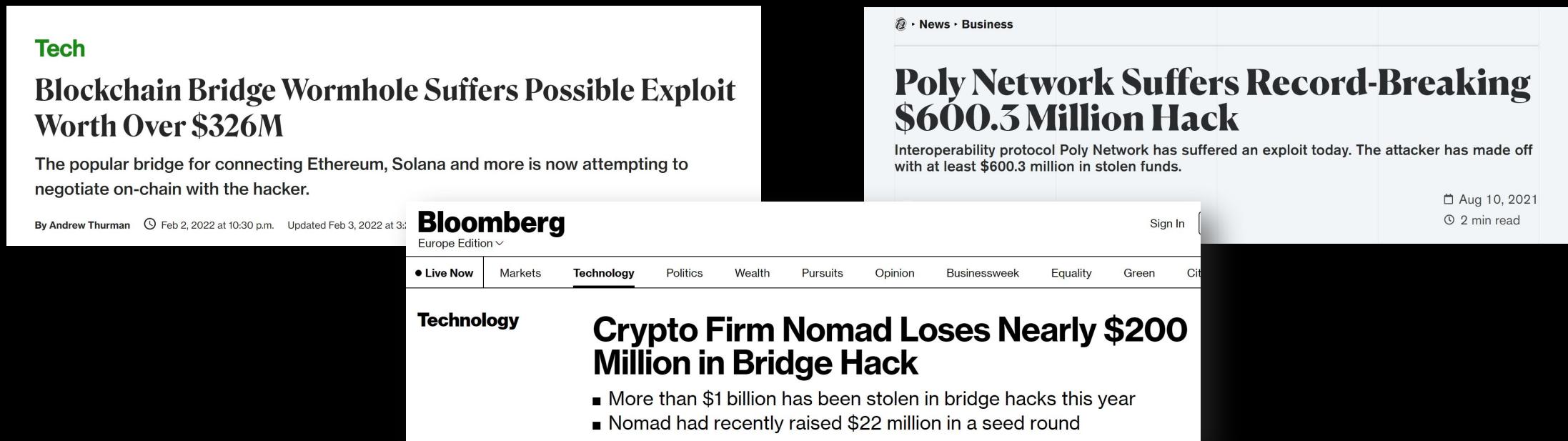
# Bridges

Polkadot.



# Bridge Security

The more value on them, the more susceptible they are for attacks



**Tech**

**Blockchain Bridge Wormhole Suffers Possible Exploit Worth Over \$326M**

The popular bridge for connecting Ethereum, Solana and more is now attempting to negotiate on-chain with the hacker.

By Andrew Thurman | Feb 2, 2022 at 10:30 p.m. | Updated Feb 3, 2022 at 3:

**Bloomberg**  
Europe Edition ▾

• Live Now Markets **Technology** Politics Wealth Pursuits Opinion Businessweek Equality Green Cities

**Poly Network Suffers Record-Breaking \$600.3 Million Hack**

Interoperability protocol Poly Network has suffered an exploit today. The attacker has made off with at least \$600.3 million in stolen funds.

Aug 10, 2021 | 2 min read

**Technology**

**Crypto Firm Nomad Loses Nearly \$200 Million in Bridge Hack**

- More than \$1 billion has been stolen in bridge hacks this year
- Nomad had recently raised \$22 million in a seed round

# Interoperability – Key Terms

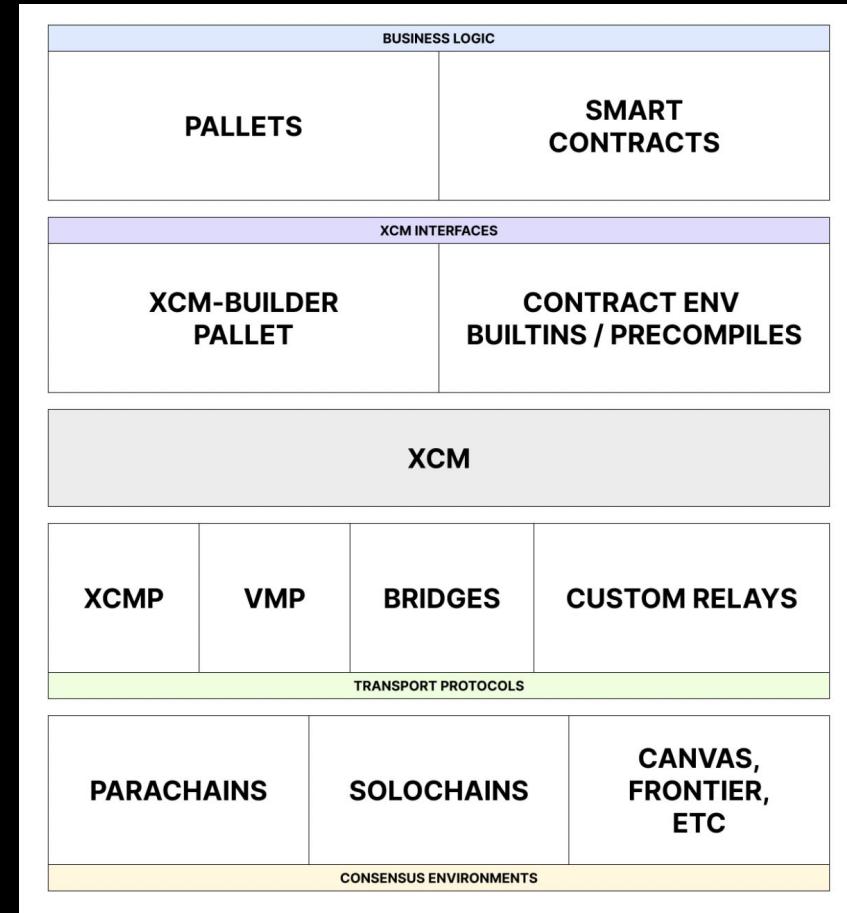
XCM – Cross Consensus Message Format

XCMP – Cross Chain Messaging Protocol

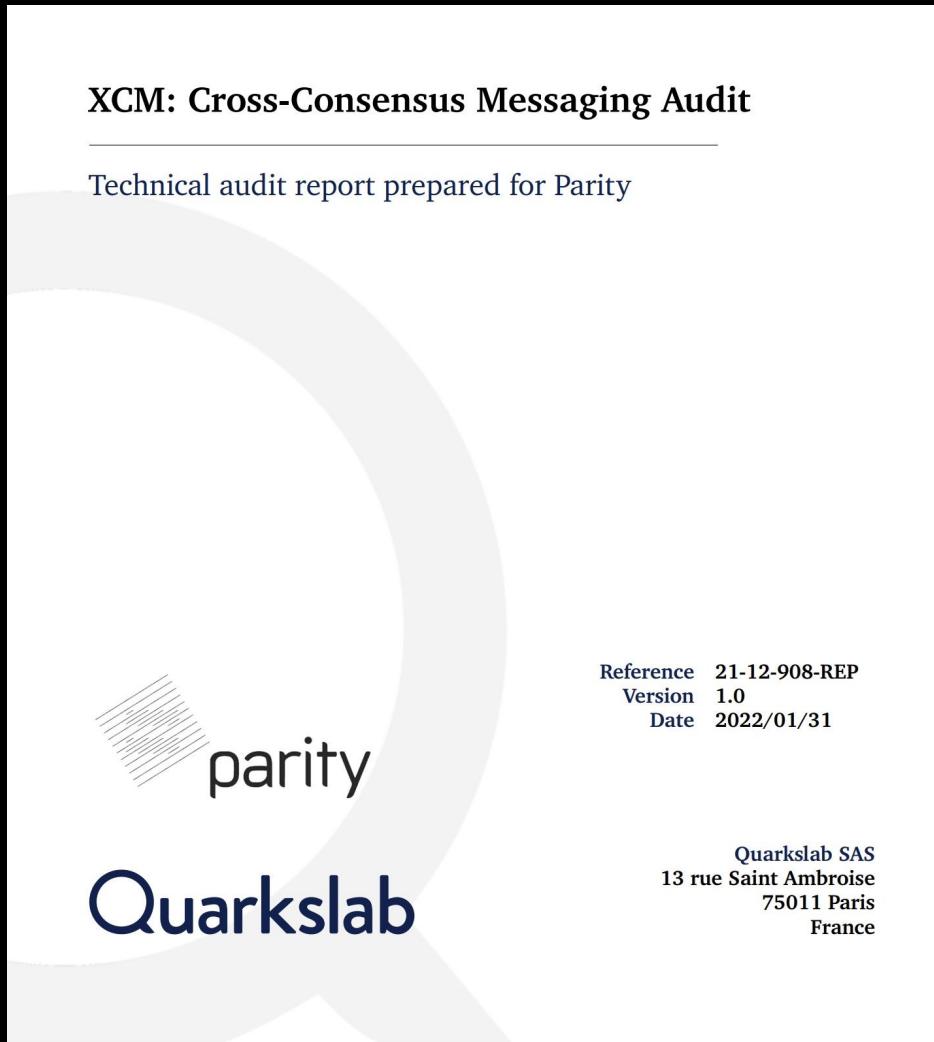
What is the XCM format?

What is the difference between XCM and XCMP?

How to transfer assets using XCM?



# XCM code Audit



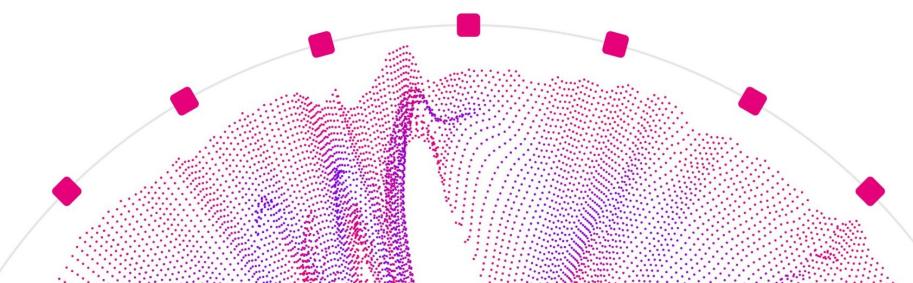
Cross-chain-related security issues, like incorrect lock/unlock or burn/mint on both chains, or any fairness issues between chains.

This also includes logical bugs, denial-of-service and any misconfiguration (of default settings) that can have a security impact.

The audit did not reveal any meaningful security-related issues.

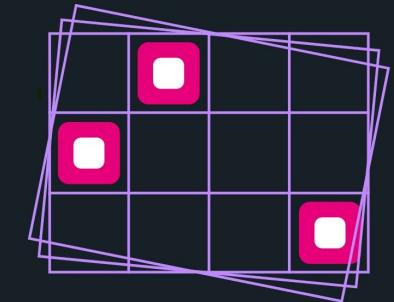
# Secure communication for a multichain world.

Polkadot unites blockchains and brings an end to the era of siloed networks. With XCM, Polkadot enables secure cross-chain exchange of any type of data, unlocking new products and services that have never been seen before.

[Start Building](#)

## Unlocking the potential of asynchronous composability

On single isolated blockchains, messages are sent and executed synchronously (in a single instant). This works well for many things, but rules out functionality that requires freedom from time constraints, such as on-chain scheduling. Cross-chain XCM messages are asynchronous, allowing developers to trigger functions across several chains to take place variably over time.



## Get ready for the era of interoperability

XCM is a language for building innovative new cross-chain applications and services. Giving applications the ability to span multiple blockchains allows them to leverage the key features and strengths of each for new interoperable use cases.



web3  
foundation

# Polkadot



Connects  
networks  
together



Handles heavy traffic  
at scale



Industry-leading  
security



Enables  
custom-made  
platforms built for  
specific apps



Revolutionizes online  
governance through open,  
community-driven  
decision-making

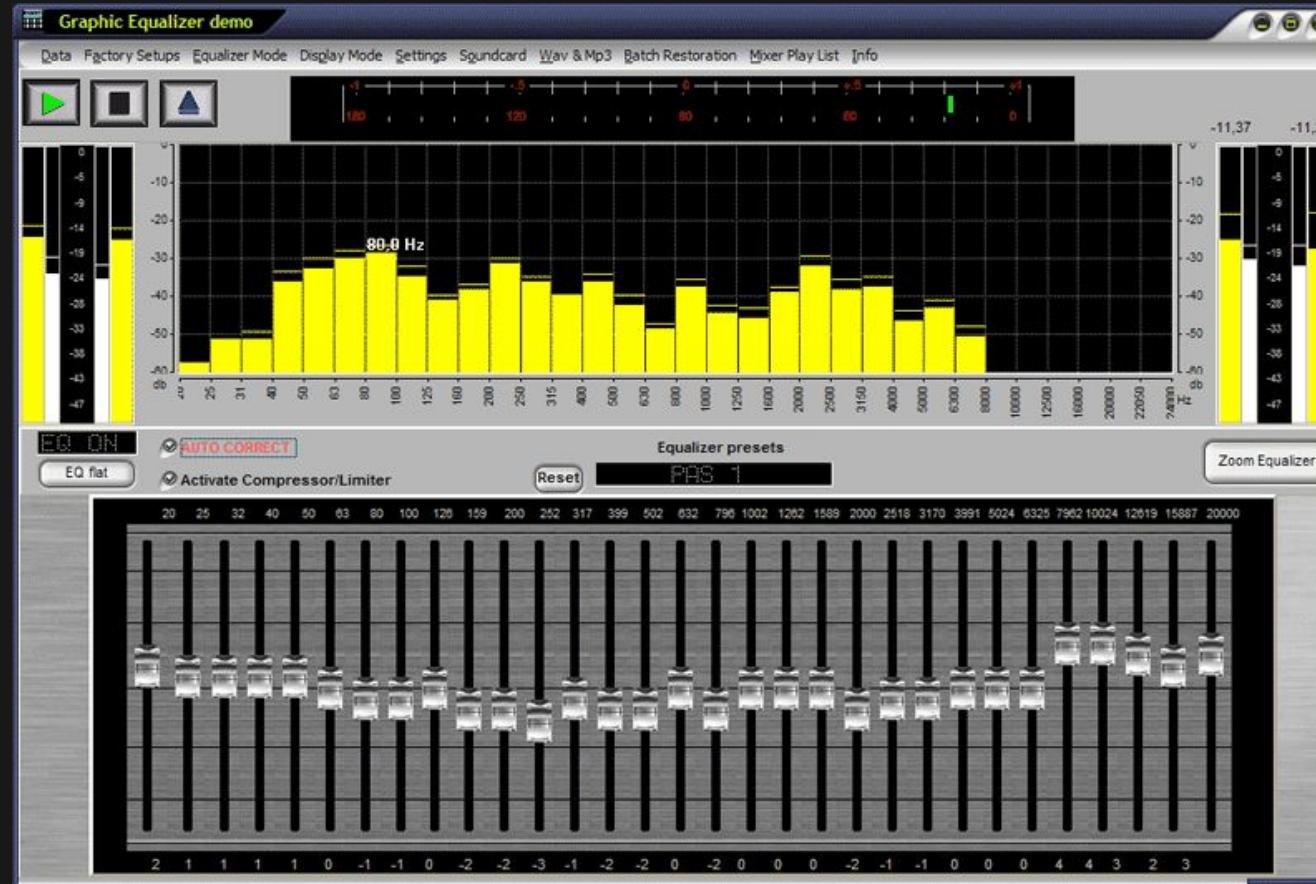


Self-upgrades  
allowing it to be  
future-proof

# Blockchains on Polkadot are custom-built and optimized for specific uses, like a producer would use a music equalizer



Customization



 Polkadot

Connects networks together



Handles heavy traffic at scale



Industry-leading security



Enables custom-made platforms built for specific apps



Revolutionizes online governance through open, community-driven decision-making



Self-upgrades allowing it to be future-proof

# Blockchain governance

- 1 No governance
- 2 One person or small group decides on the network's future
- 3 The community proposes and votes on decisions that impact the network's future

# Total On-Chain Governance

The screenshot shows the Polkadot Explorer interface with the following details:

- Network:** polkadot/9270
- Accounts:** #12,130,576
- Network:** Network dropdown menu
- Explorer:** Selected tab
- Chain info:** Tab
- Block details:** Tab
- target:** 6 s
- recent blocks:** Recent blocks section
- Governance:** Democracy (2), Council (2), Treasury (6), Bounties (4), Tech. comm.
- Developer:** Code info

# Stake and Conviction Weighted Voting



Peter: Votes **No** with 10 DOT for a 128 week lock period  $\Rightarrow 10 \times 6 = 60$  Votes

Logan: Votes **Yes** with 20 DOT for a 4 week lock period  $\Rightarrow 20 \times 1 = 20$  Votes

Kevin: Votes **Yes** with 15 DOT for a 8 week lock period  $\Rightarrow 15 \times 2 = 30$  Votes

Even though combined both Logan and Kevin vote with more DOT than Peter, the lock period for both of them is less than Peter, leading to their voting power counting as less.

## Governance -> Execution

Polkadot nodes run software which in turn runs a “blob” of Wasm bytecode. This bytecode is stored on-chain and is modifiable via the system itself.



 Polkadot

Connects networks together



Handles heavy traffic at scale



Industry-leading security



Enables custom-made platforms built for specific apps

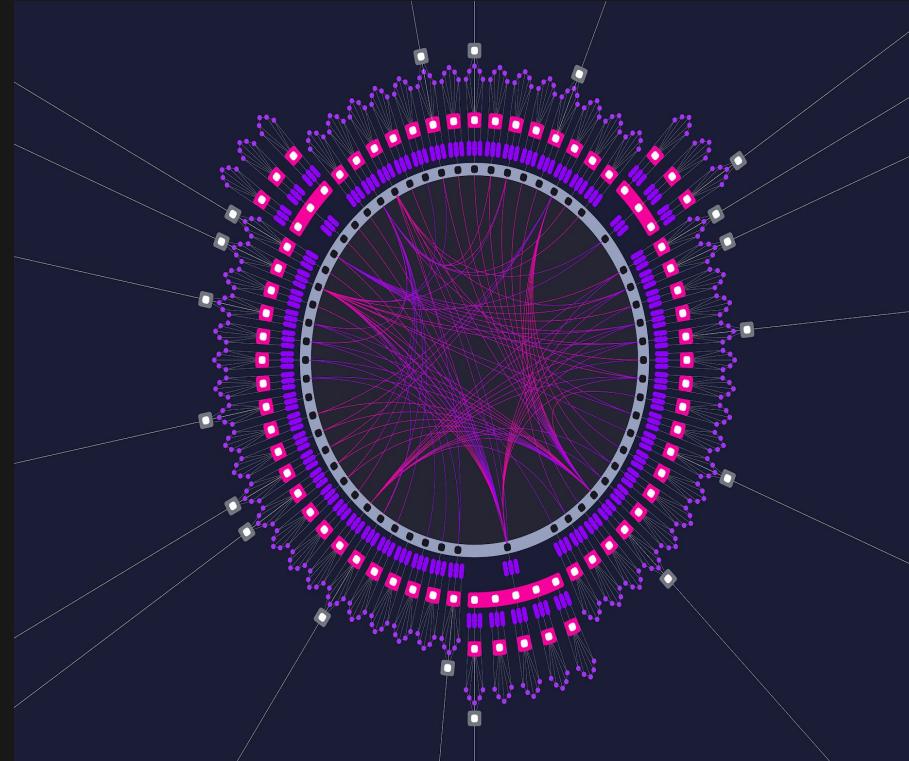


Revolutionizes online governance through open, community-driven decision-making



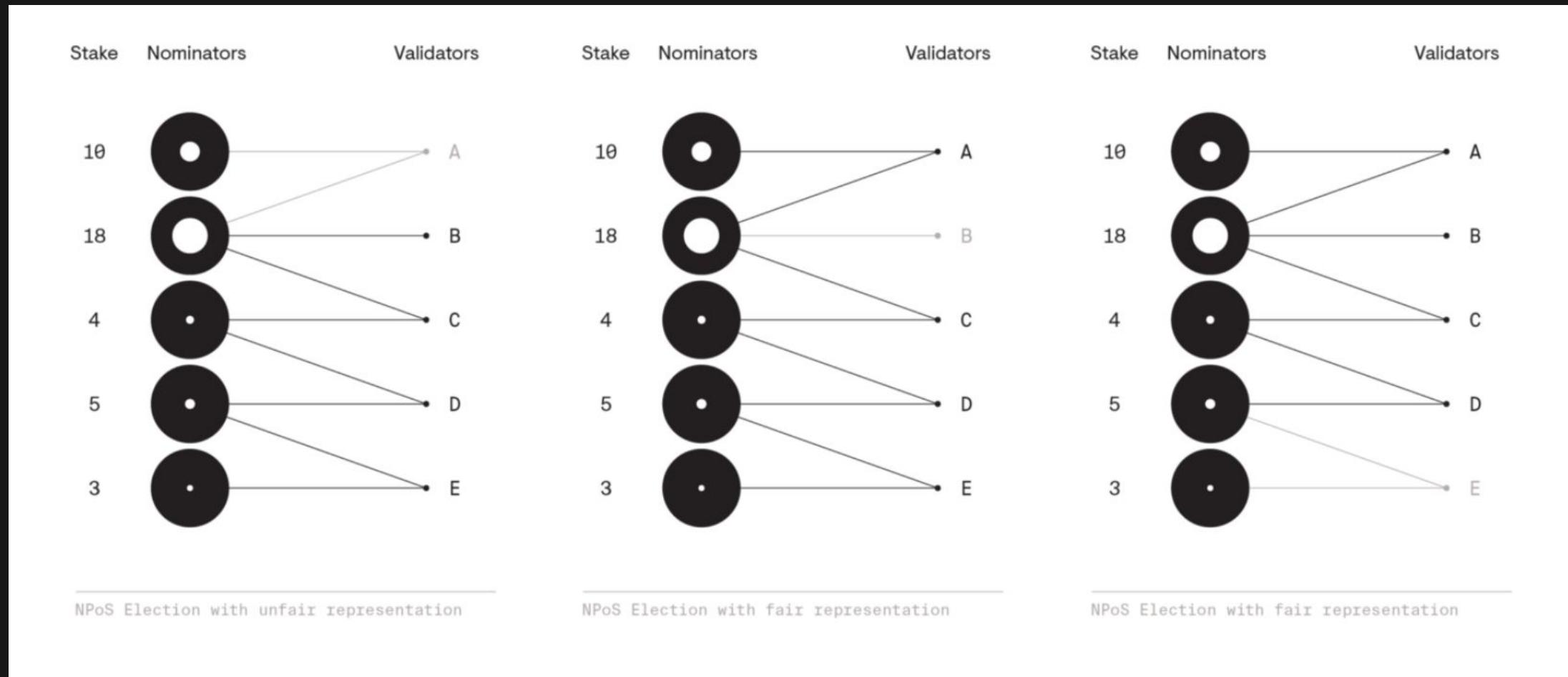
Self-upgrades allowing it to be future-proof

**Polkadot makes security easy for new blockchain teams by allowing them to plug right into an existing security system**

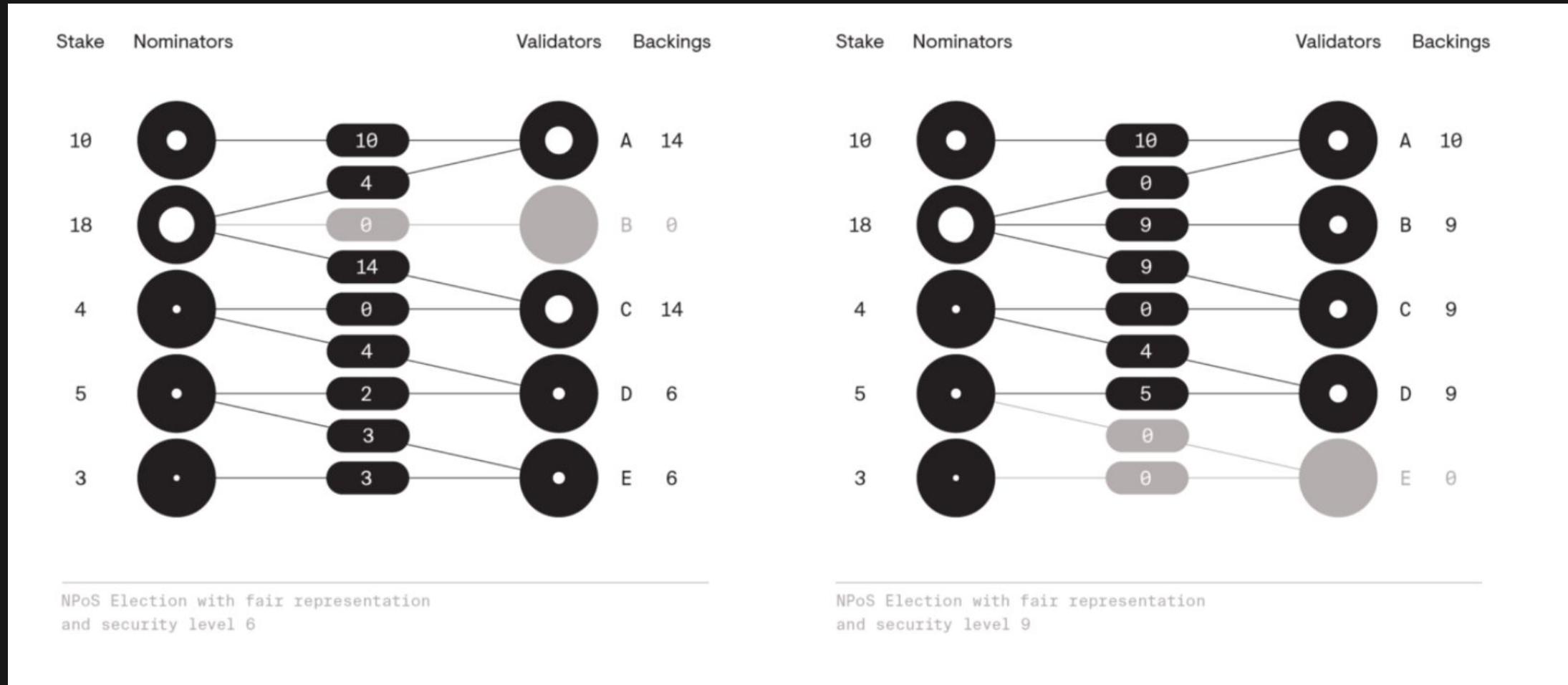


**...and focus on what they do best, coding.**

## Proportionally Justified Representation in NPoS



# Proportionally Justified Representation in NPoS

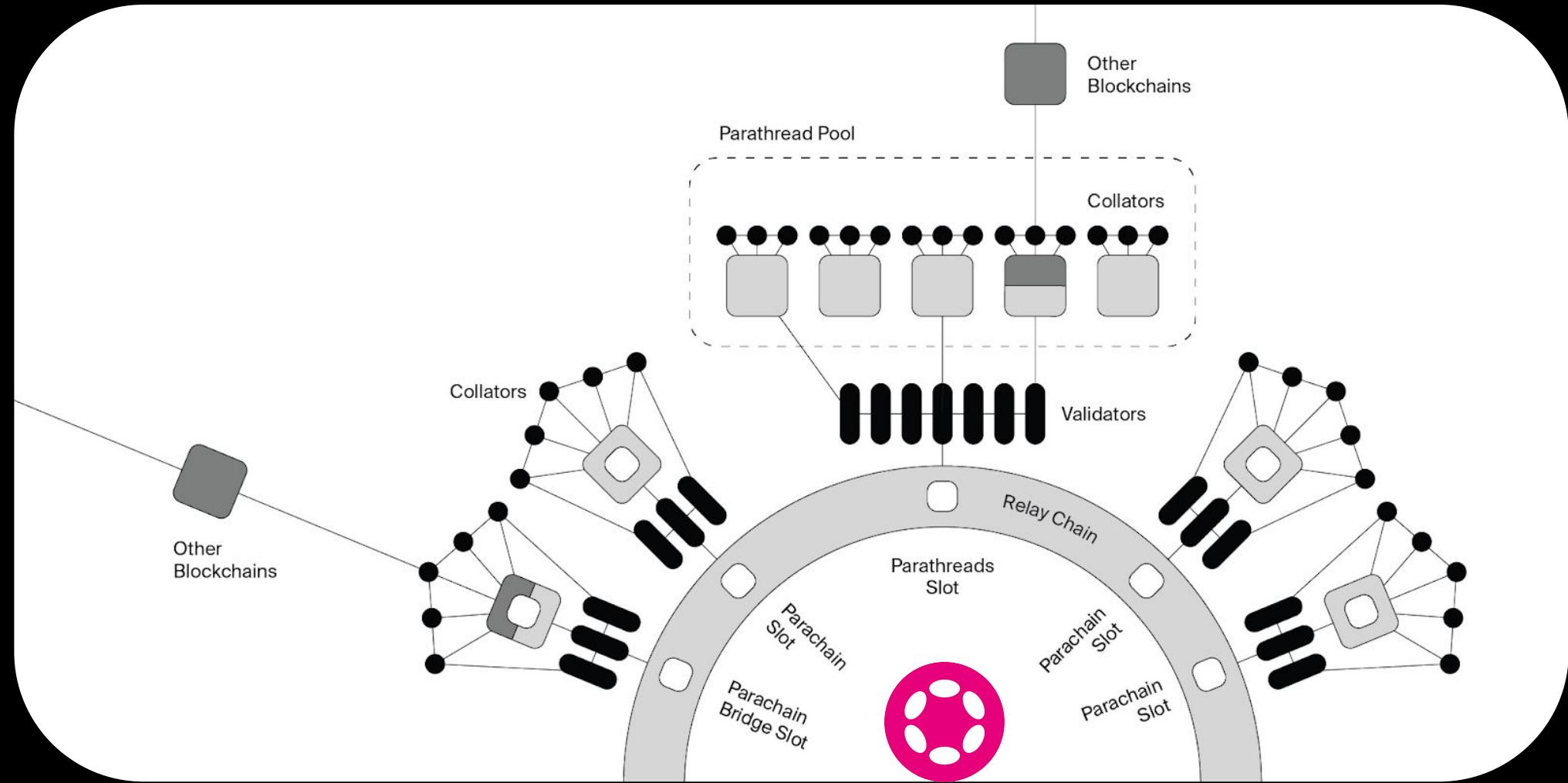


## Nominated Proof of Stake

Polkadot is secured by the economic power of the DOT token itself. There is no “mining” (via proof-of-work), but rather block production from the set of most highest-staked validators.

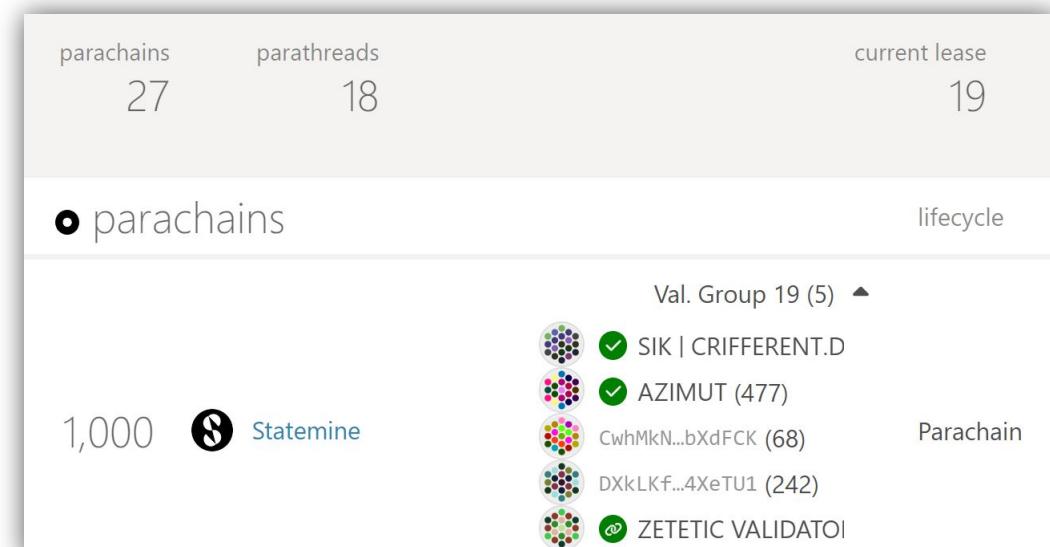
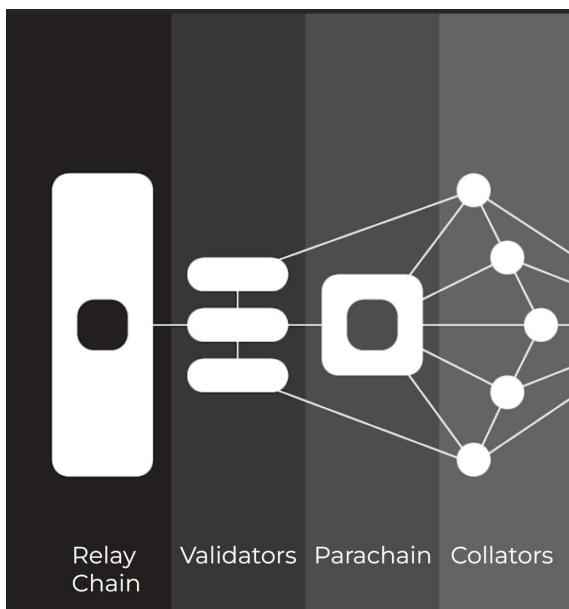
That is, if you wish to produce blocks, you (or your nominators) must “bond” enough stake (DOT tokens) to get into the top  $n$  slots. At that point, your validator will receive an approximately equal number of DOT tokens as any other validator.

# Polkadot Network Architecture



# Validators and Collators

- The parachain selects a collator to submit a block to the relay chain
- Polkadot shuffles and assigns a set of validators to this parachain
- The collators and validators open connections to submit a block.



<https://polkadot.js.org/apps/#/parachains>

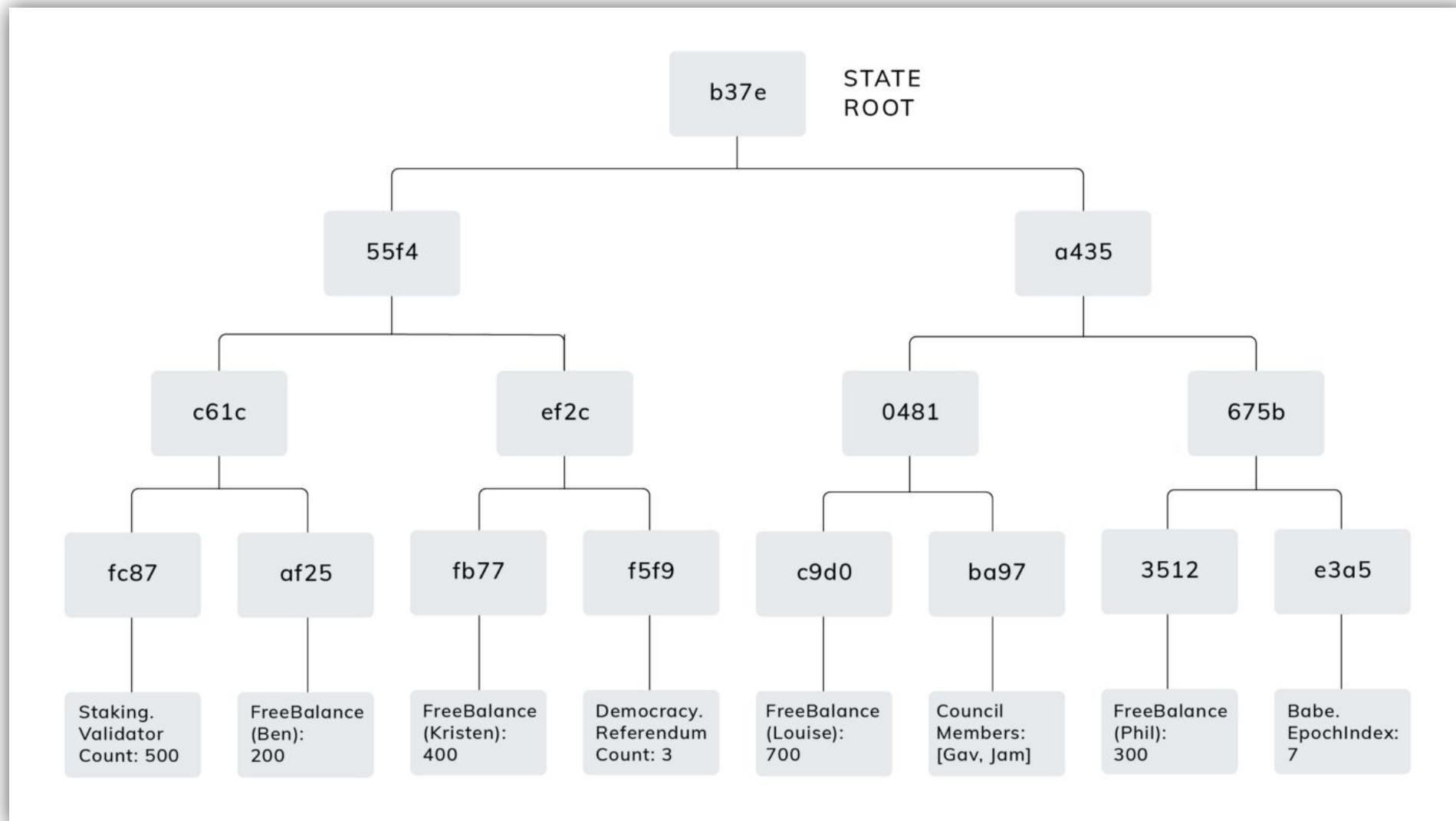


# Path of a Parachain Block

A screenshot of a dark-themed web page. At the top left is the Polkadot logo and "EN" text. To the right are links for "Lightpaper", "Whitepaper", "Wiki", and social media icons for GitHub, LinkedIn, and Twitter, along with a "Support" button. The main navigation menu includes "Technology", "Community", "About", "Blog", "Build", and "Contact". The title "The Path of a Parachain Block" is centered above the content. Below the title is the date "February 6, 2020" and categories "Polkadot", "Parachains", "Parathreads". A small profile picture of the author, Joe Petrowski, is next to the text. The central image is a dark, abstract graphic composed of various colored rectangles (purple, blue, green, yellow) with diagonal hatching, arranged in a grid-like pattern. A cursor arrow is visible on the right side of the image.

<https://polkadot.network/blog/the-path-of-a-parachain-block/>

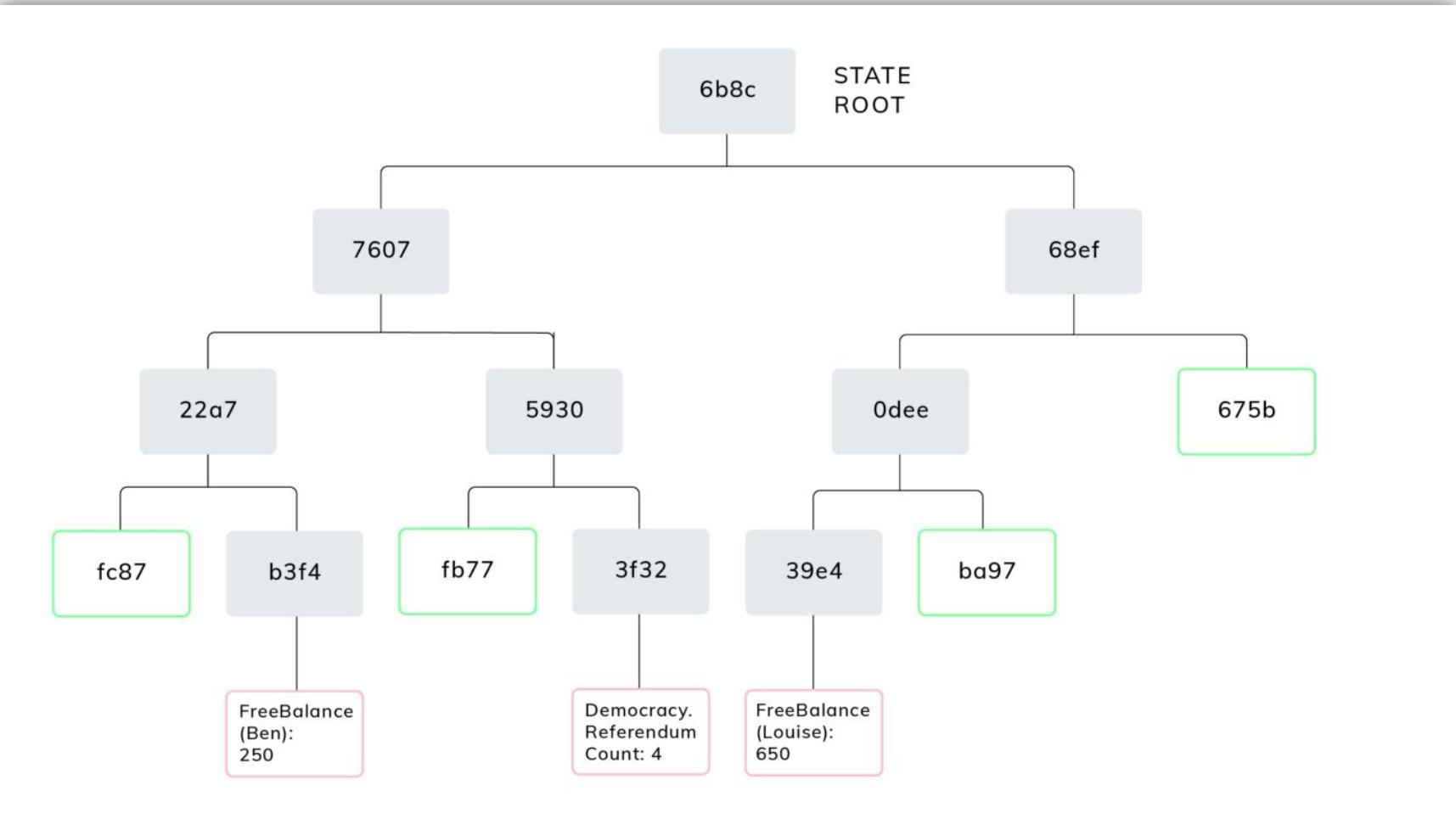
# Parachain State



# Parachain State Transition

```
parent_hash: 7a42
number: 2
state_root: 6b8c
extrinsics_root: 3bf9
digest: vec<consensus, ...>
```

```
democracy.on_initialize(),
balances.transfer(
    Louise,
    Ben,
    50
)
```



## Proof of Validity

A validator can verify a state transition without having access to the entire state. It only needs:

- The block (list of state transitions)
- The values in the parachain's database that the block modifies
- The hashes of the unaffected points in the Merkle tree.

```
parent_hash: 7a42
number: 2
state_root: 6b8c
extrinsics_root: 3bf9
digest: vec<consensus, ...>

democracy.on_initialize(),
balances.transfer(
    Louise,
    Ben,
    50
)
```

 Polkadot

Connects networks together



Handles heavy traffic at scale



Industry-leading security



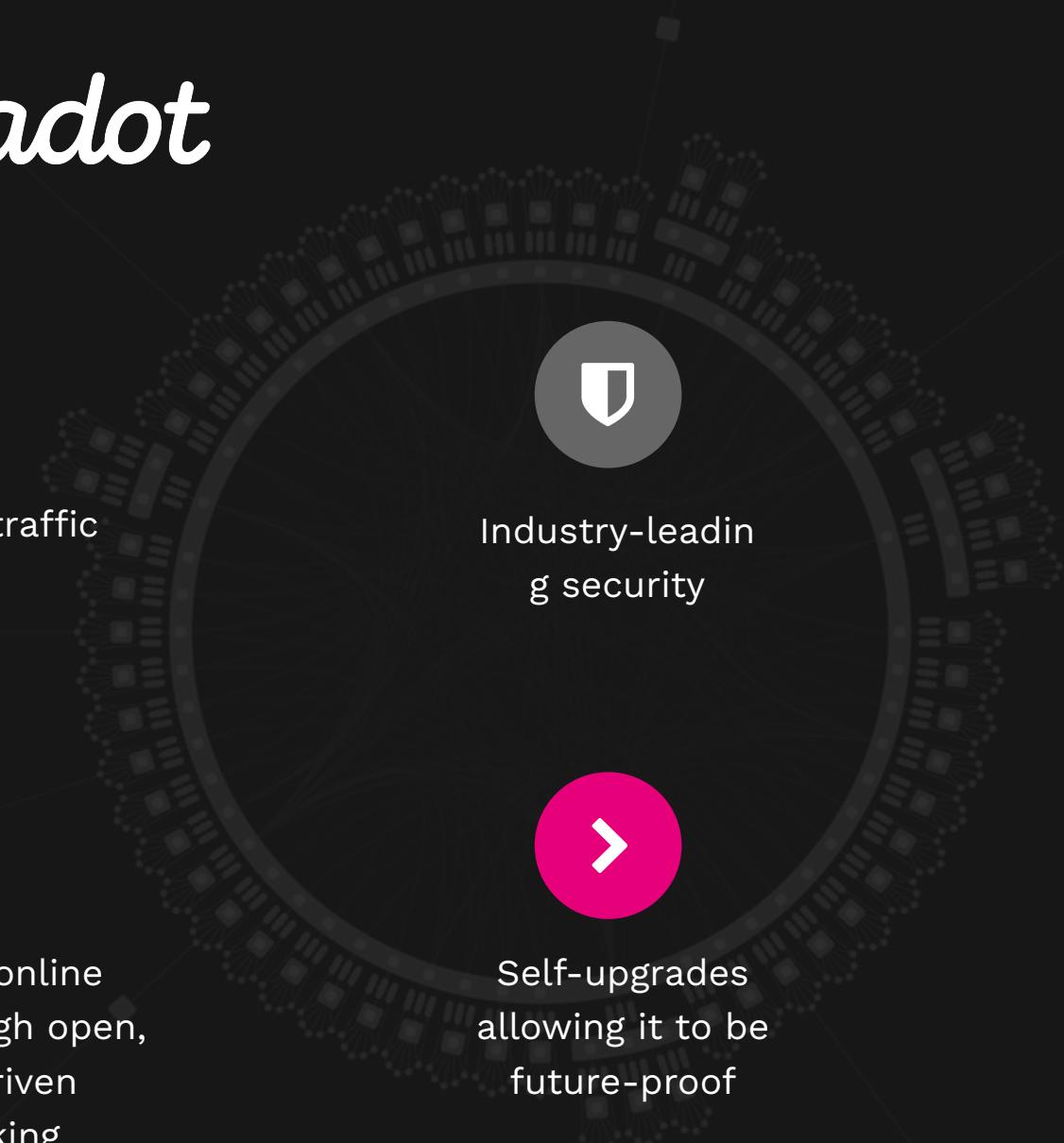
Enables custom-made platforms built for specific apps



Revolutionizes online governance through open, community-driven decision-making



Self-upgrades allowing it to be future-proof





# Polkadot and Parachains can easily upgrade without forking the chain



Future-proof

Legacy  
blockchain  
upgrades

