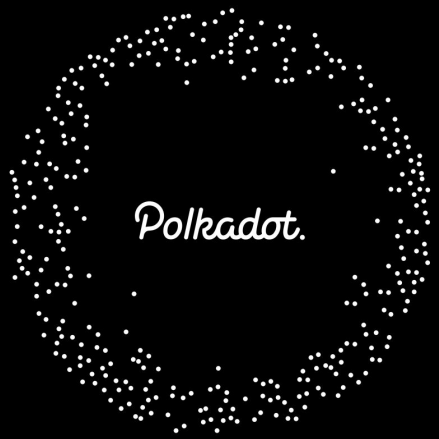


Intro to Polkadot: Architecture, Terminology, and Fundamental Concepts

Bill Laboon
Head of Education and Grants at Web3 Foundation

Twitter: @BillLaboon
Email: bill@web3.foundation

Bill Laboon is the Head of Education and Grants at the Web3 Foundation. Before this, he was a lecturer in the Computer Science Department of the University of Pittsburgh, teaching courses in software quality assurance, software engineering, and blockchain technology. He is a frequent speaker at conferences on a variety of topics, including cryptocurrency, software quality, and the ethics of software development. He is the author of two books: A Friendly Introduction to Software Testing, an undergraduate textbook; and Strength in Numbers, a near-future novel set in a world in which cryptocurrency has eliminated traditional money. Bill has a BS in Computer Science and Political Science from the University of Pittsburgh, as well as an MS in Software Design & Management from Carnegie Mellon University.

Polkadot.

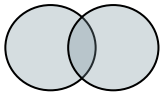
Overview

What is Polkadot?

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

Why Polkadot?

Polkadot aims to be a foundation for other protocols...



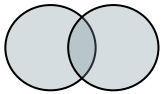
Interoperability

… speeding up the evolution of the decentralised web

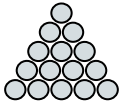
- makes interaction between existing blockchains easier

Why Polkadot?

Polkadot aims to be a foundation for other protocols...



Interoperability



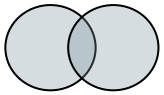
Pooled security

… speeding up the evolution of the decentralised web

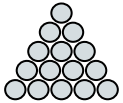
- makes interaction between existing blockchains easier
- enables easy and secure deployment of blockchains with new and interesting value propositions

Why Polkadot?

Polkadot aims to be a foundation for other protocols...



Interoperability



Pooled security

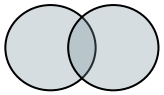
Heterogeneous chains

… speeding up the evolution of the decentralised web

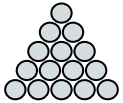
- makes interaction between existing blockchains easier
- enables easy and secure deployment of blockchains with new and interesting value propositions
- allows dApp devs to leverage capabilities of multiple chains

Why Polkadot?

Polkadot aims to be a foundation for other protocols...

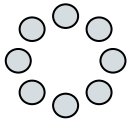


Interoperability



Pooled security

Heterogeneous chains

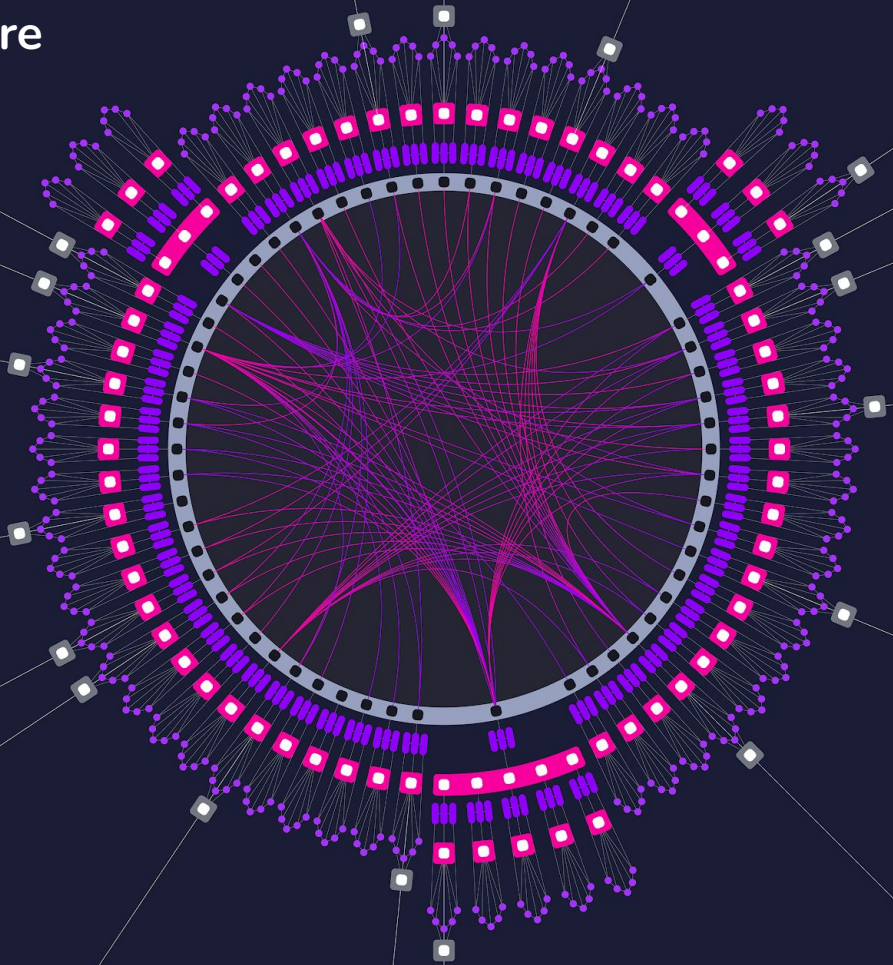


Thought-through governance

… speeding up the evolution of the decentralised web

- makes interaction between existing blockchains easier
- enables easy and secure deployment of blockchains with new and interesting value propositions
- allows dApp devs to leverage capabilities of multiple chains
- evolves with the needs of token holders through governance

Polkadot Architecture



Polkadot Architecture:

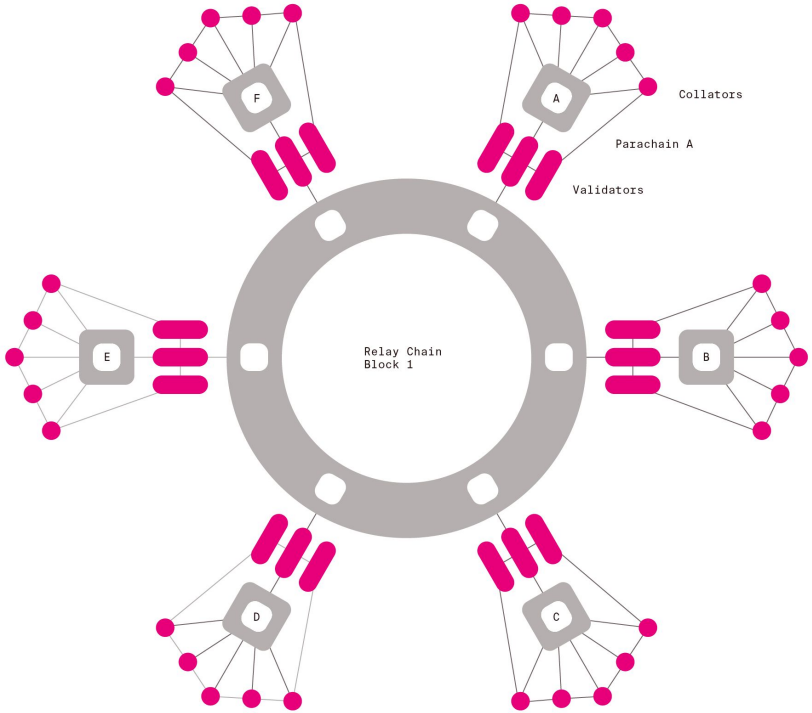
Polkadot.

RELAY CHAIN

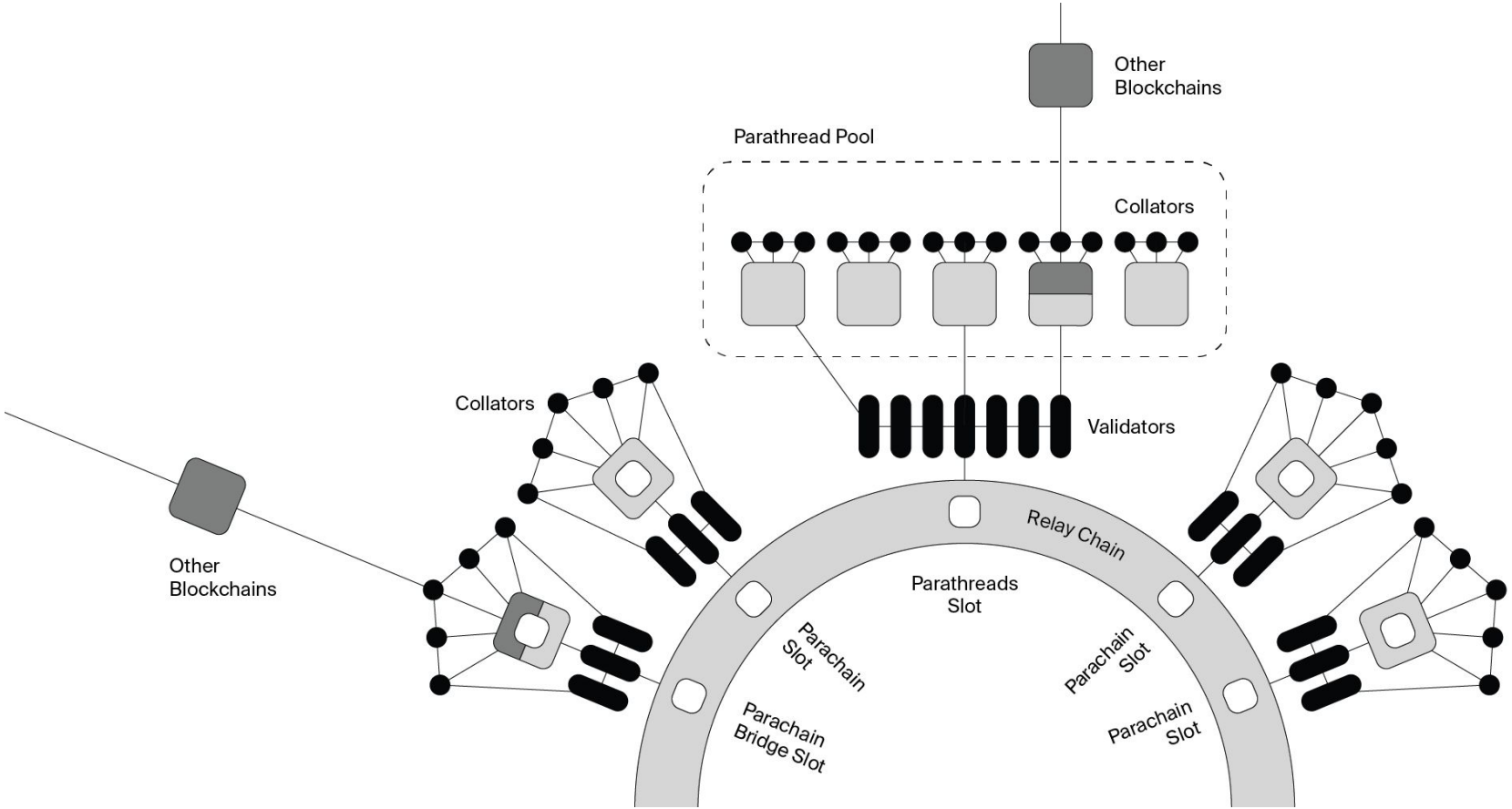
The connector chain of Polkadot that provides strong economic security and an interoperability protocol.

PARACHAINS / PARATHREADS

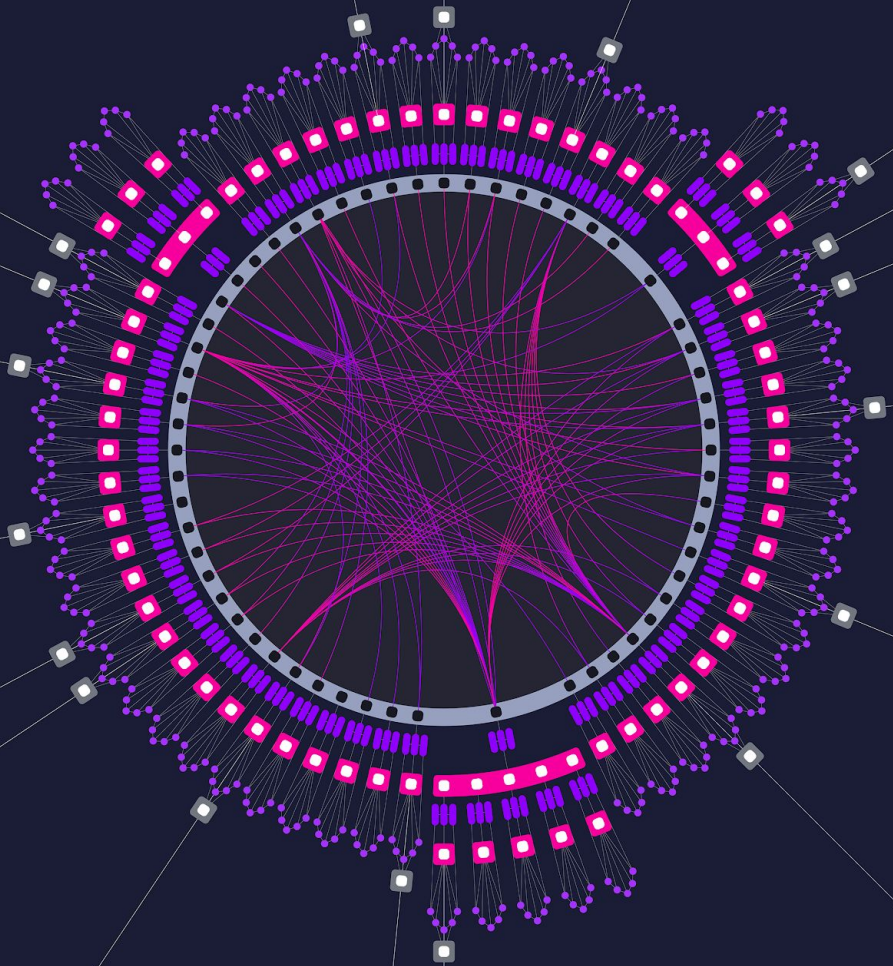
Third-party chains that connect to Polkadot for interoperability, scalability, and pooled security.



Overview of System



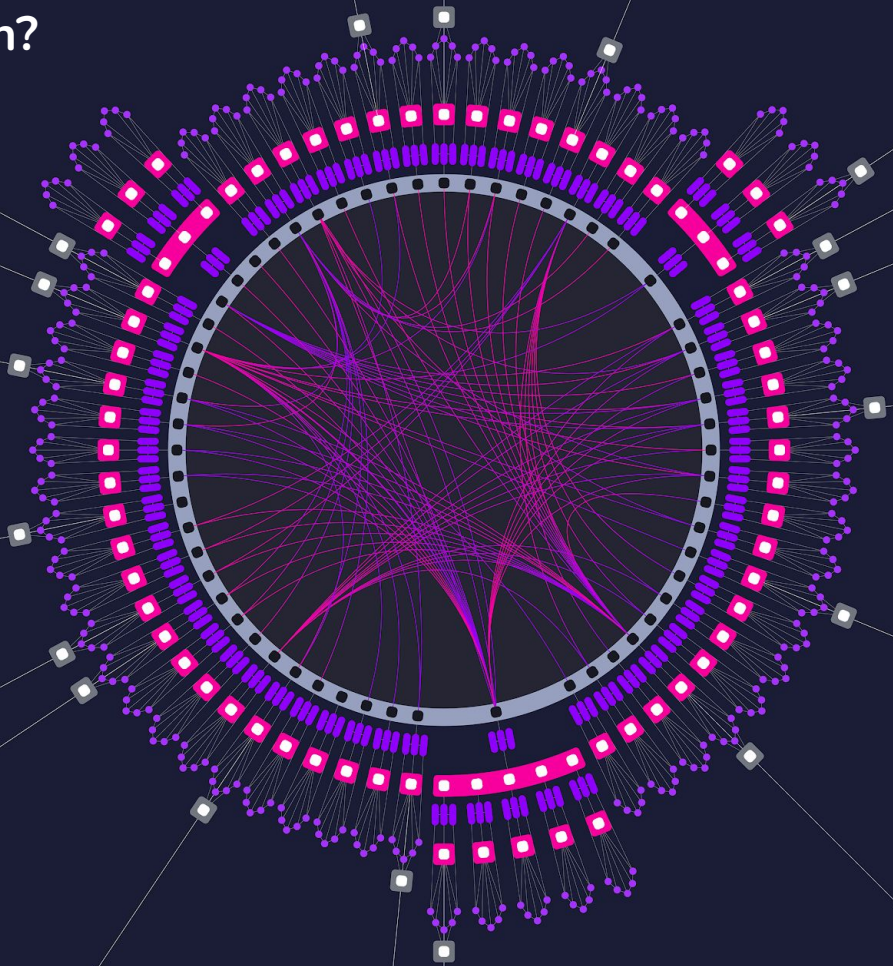
Substrate



Substrate

Polkadot.

Why Be A Parachain?



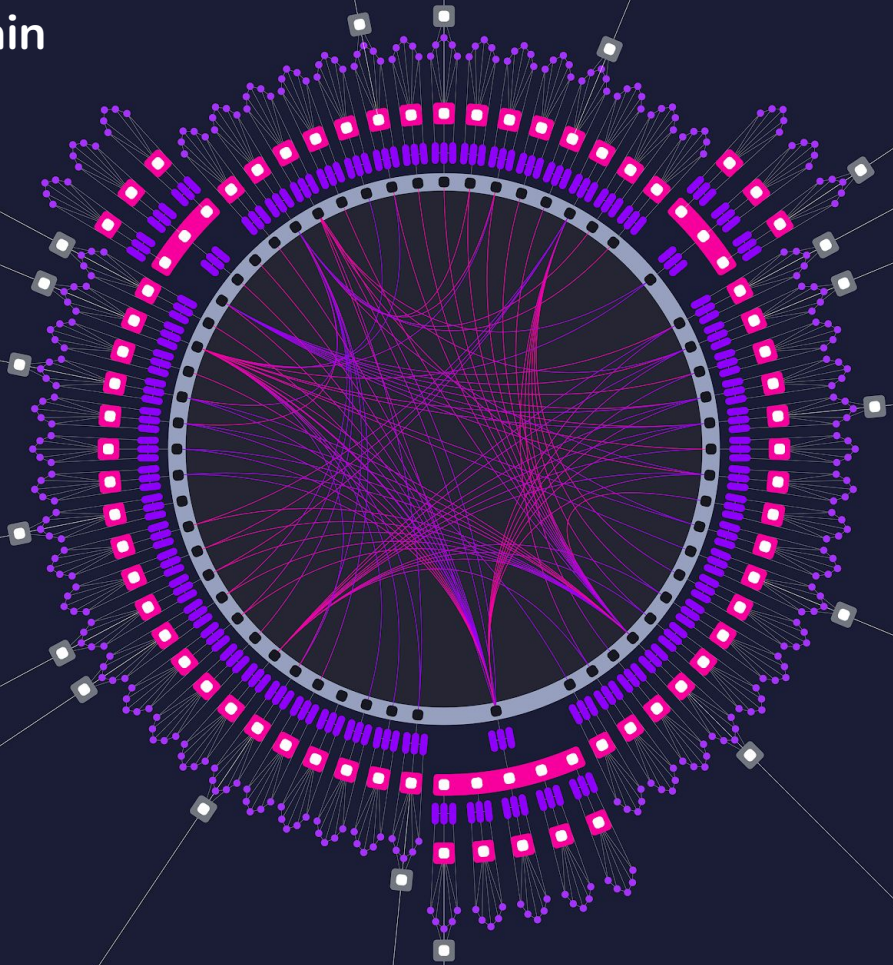
Shared Security

- **Any chain connected to the relay chain shares in the security of all chains in the network.**
- Verification and finalization of blocks is performed by the validators on the relay chain

XCMP

- **X**-**C**hain **M**essage **P**assing.
- Guarantees the delivery of messages between parachains and parathreads.
- XCMP will **not** put messages on the Relay chain, only a hash for each inbound and outbound queue.
- Current version (HRMP) does put messages directly on the relay chain

Becoming a Parachain



Parachain Auctions

- Approximately every two weeks (one week on Kusama), a new auction occurs for a parachain slot
- A candle auction (an auction where the exact end time is unknown, and in our case is determined retroactively) is held
- DOT are locked for that period by the system itself; unlike an ICO, these DOT are not sent to the project developers, but are locked by the runtime during the lease period and automatically returned afterwards

Crowdloan Functionality

- In order to compete for a parachain slot, projects can have DOT holders lock their DOT on behalf of the parachain
- This is all done in an automated and trustless way; the relay chain runtime handles this

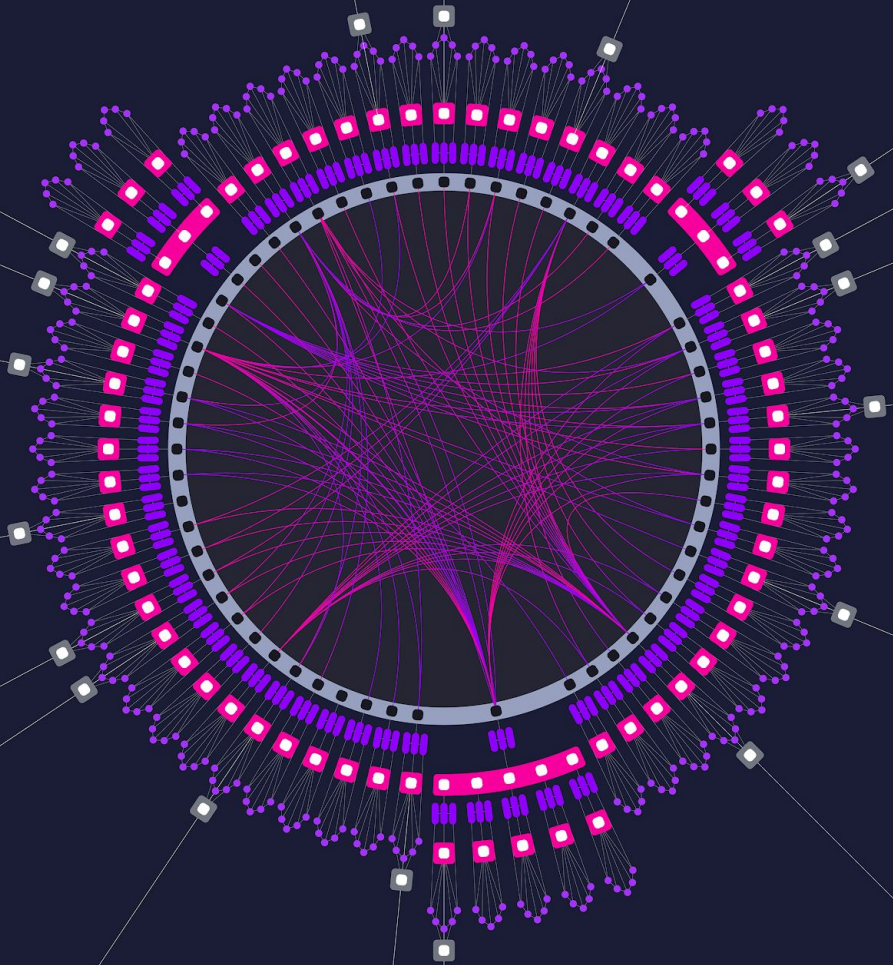
Slot Length

- Parachain slots last up to two years, biddable in three-month slot times (one year on Kusama, with six-week slot times)
- After slot expires, can become a parathread (PAYGO), or solochain

Note

- A common misconception is that you MUST win a parachain slot to run a project on Polkadot
- This is ONLY true for parachains / parathreads
- Other projects can run on top of parachains, and most are well-suited towards running as a smart contract rather than a parachain

Kusama

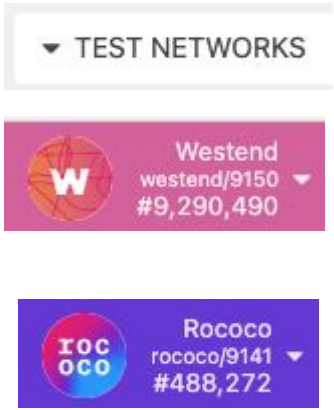


KUSAMA

Kusama: Polkadot’s Canary Network

Kusama is not a testnet!

Internal Testnets



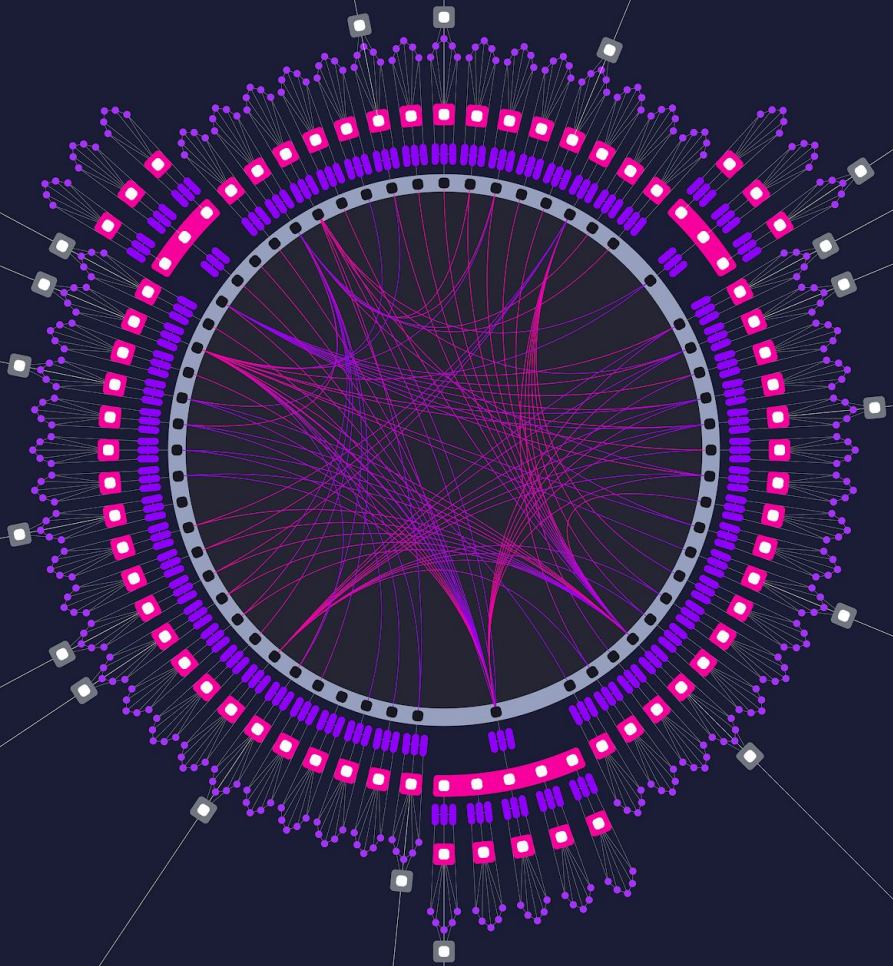
No economic value

Economic value

CODE

Expect chaos.

Nominated
Proof-of-Stake

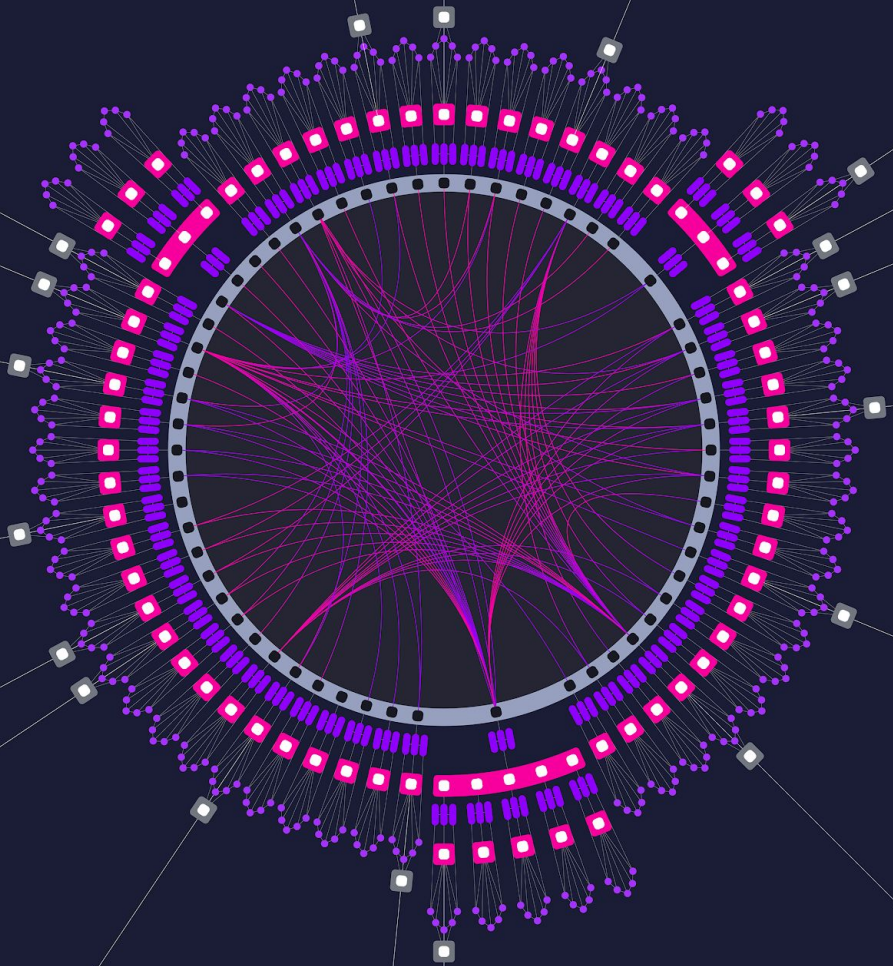


Nominated Proof of Stake

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.

Hybrid Consensus



FINALITY

- ➔ Finality in classical blockchain model is probabilistic
- ➔ Other mechanisms (e.g. Tendermint) have provable finality
- ➔ BUT the big drawback is that they are vulnerable to stalling
- ➔ AND Polkadot may occasionally need to revert blocks that have been recently added (in case of conflicting information about parachains)
  - ◆ This should be rare, so ideal situation is a situation where we generally have fast finalization, but block production can continue and we let finalization “catch up” when ready

Polkadot.

Hybrid Consensus

- ➔ Best of both worlds - block production can always continue as long as one validator is online
- ➔ Finalization is done via a separate finalization gadget
- ➔ In ideal circumstances, block finalization can be rather fast (a few blocks, empirically ~ 20-30 seconds on our canary network Kusama)
- ➔ With minor issues, can delay finalization while further checks are done
- ➔ In the event of severe network partitioning or malicious attack, block production can continue but we temporarily fall back to probabilistic finalization

Polkadot.

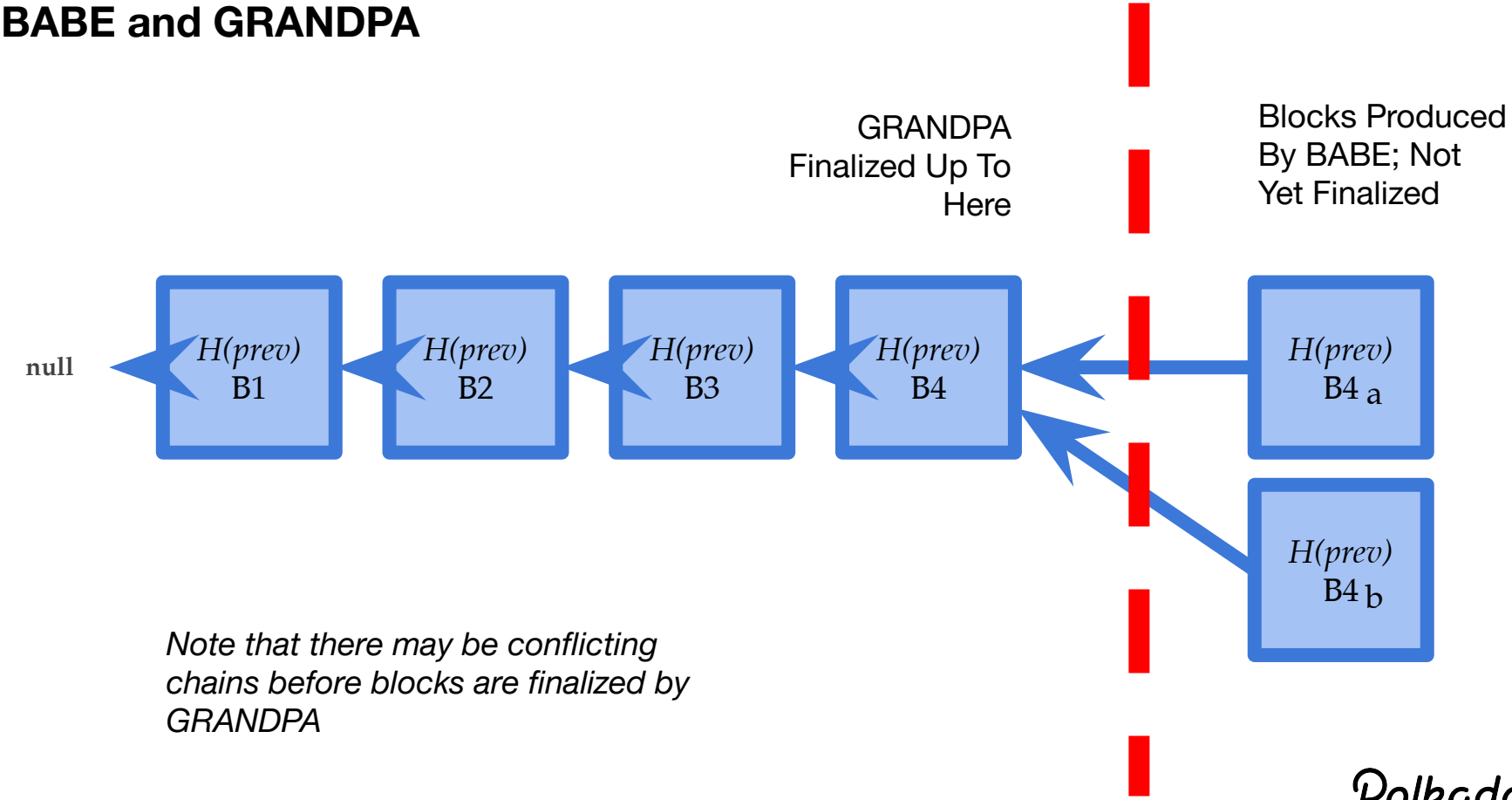
BABE and GRANDPA

➔ **BABE (Blind Assignment for Blockchain Extension)**
- ◆ Validators randomly select themselves to produce blocks
- ◆ Validators selected by amount of stake (tokens)
- ◆ For "young" blocks that are newly created

➔ **GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement)**
- ◆ Finalizes blocks separately
- ◆ For "old" blocks.. blocks must be produced before they are finalized

Polkadot.

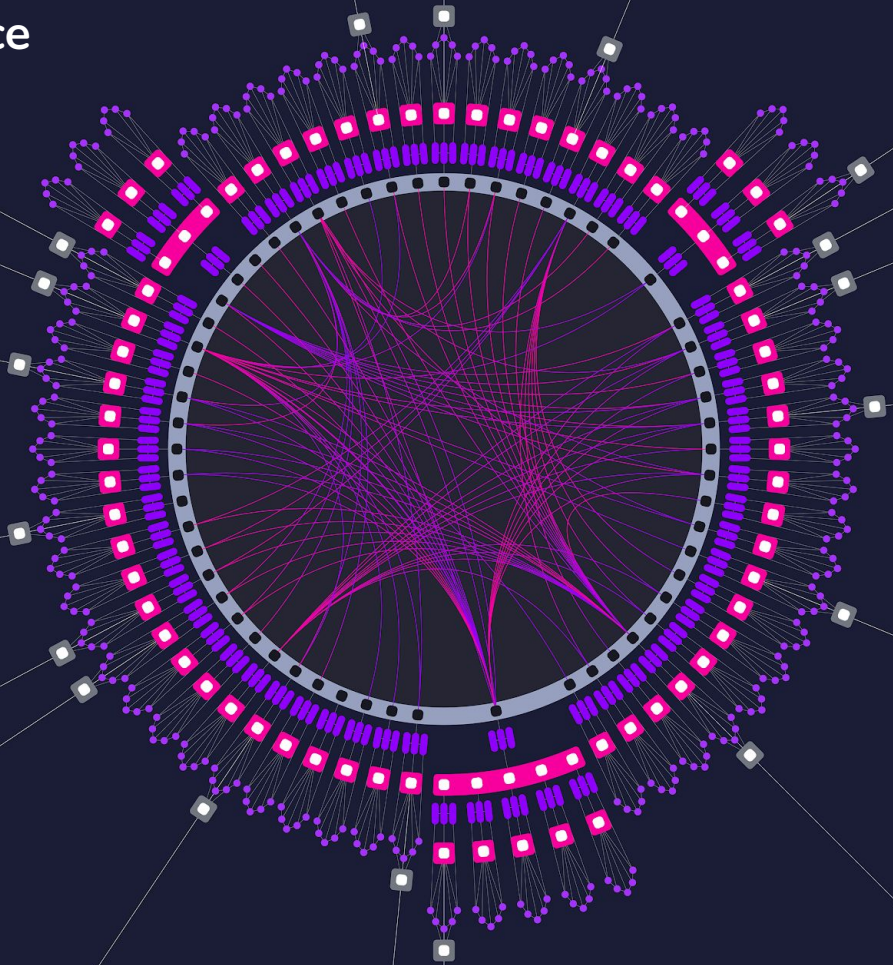
BABE and GRANDPA



Note that there may be conflicting chains before blocks are finalized by GRANDPA

Polkadot.

Polkadot Governance



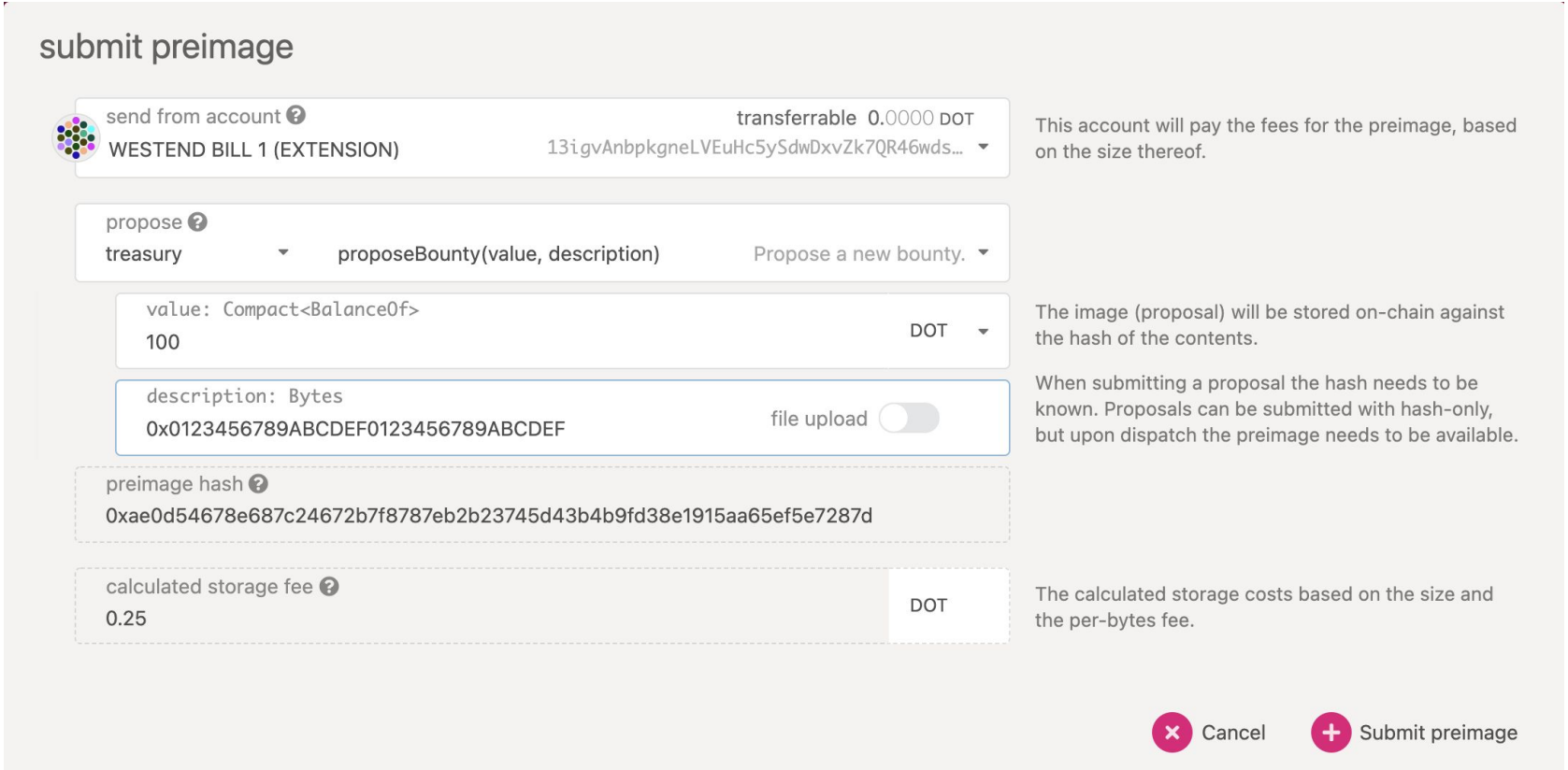
Governance

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.

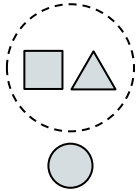
This means that many parameters, up to and including the actual code of the core relay chain state transition function, can be updated.

Governance determines how we allow that to happen.

Example Proposal

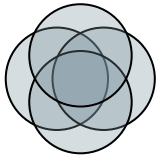


Polkadot Governance - Goals



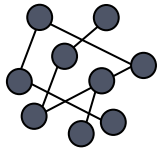
Ability to make good decisions

- Fair representation
- Ability to decide despite limited voter attention (low turnout) and high friction



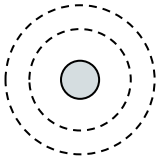
Coherence

- Ability to keep the community united and to avoid forks



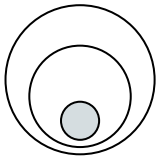
Preserving decentralised qualities

- No party should be privileged over another a priori



Security

- Avoidance of loopholes and unintended behaviour



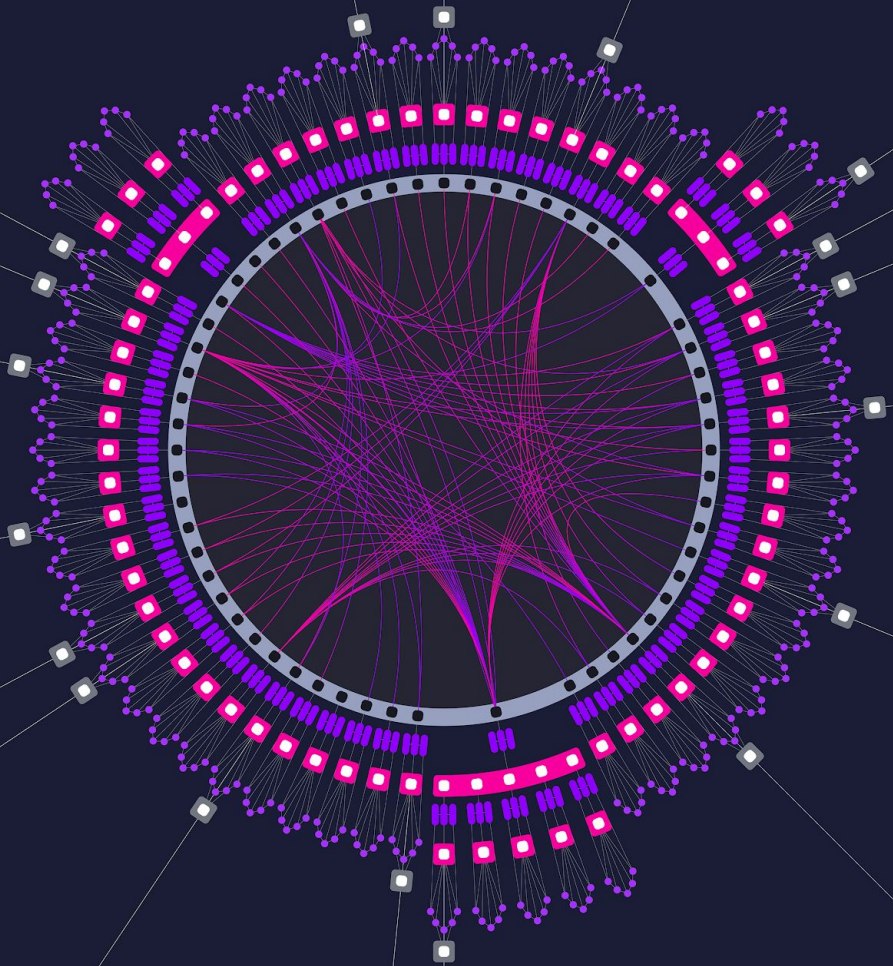
Scalability

- Ability of the governance mechanism to allow many participants to consider many proposals

Governance

All changes to the protocol must be agreed upon by stake-weighted referendum; the majority of stake can always command the network.

Substrate



Substrate

Polkadot.