Polkadot Primer

Mira Christanto

Feb 25, 2021

By Mira Christanto and Wilson Withiam

Many investors have probably heard of Polkadot, but when attempting to learn about it couldn't get past the Polkadot-specific jargon. To date, this inability to sift through the jargon has been costly, as Polkadot has quickly risen to the top 5 cryptoassets, and become one of the most exciting emerging blockchain ecosystems in the industry. If your eyes have glazed over previous explanations, this is a great place to finally understand Polkadot's vision and the implications for the ecosystem if it succeeds.

We outline Polkadot's background, how it works, its strengths, and its risks. Polkadot's ambitions are big and their founder, along with a large community of developers, has been on track to take on the challenge.

What's Polkadot's background?

The original Polkadot whitepaper was released in October 2016, by Gavin Wood - co-founder of Ethereum. He's also credited for creating Ethereum's Solidity smart contract programming language and for Ethereum's launch. Much of the material within Polkadot's whitepaper came from Gavin's early research on how to scale Ethereum. When he left Ethereum in 2016, he founded two entities that would create Polkadot, called Parity Technologies and the Web3 Foundation (W3F). W3F is the non-profit R&D arm while Parity is a for-profit software company commissioned by the W3F to develop and upkeep Polkadot.

How much money did they raise?

Their fundraising history, managed by the W3F, is as follows:

- In October 2017, Web3 conducted the Polkadot private sale and raised $145 million in ETH for 50% of the DOT token supply. A few months after, due to a bug, $98 million (68%) in those ICO funds were permanently locked-up. This wasn't Parity's first issue as they were hacked for 350,000 ETH (then $30 million) in July 2017. Polkadot's team executed their development plans with the remaining $47 million.
- June 2019: The Web3 Foundation sold 500,000 DOT to private investors. The actual amount raised in this round is unconfirmed but rumored to be $60 million, which would have valued the project at $1.2 billion.
- July 2020: Polkadot raised another $43 million (3,982 BTC) in a private token sale at $125 per token ($1.25 post redenomination -- more on this below).

It's uncommon for a token project to have three private sales, which speaks to the demand from investors and projects to work with Polkadot. Prominent investors include Pantera, Placeholder, Three Arrows Capital, and Polychain.

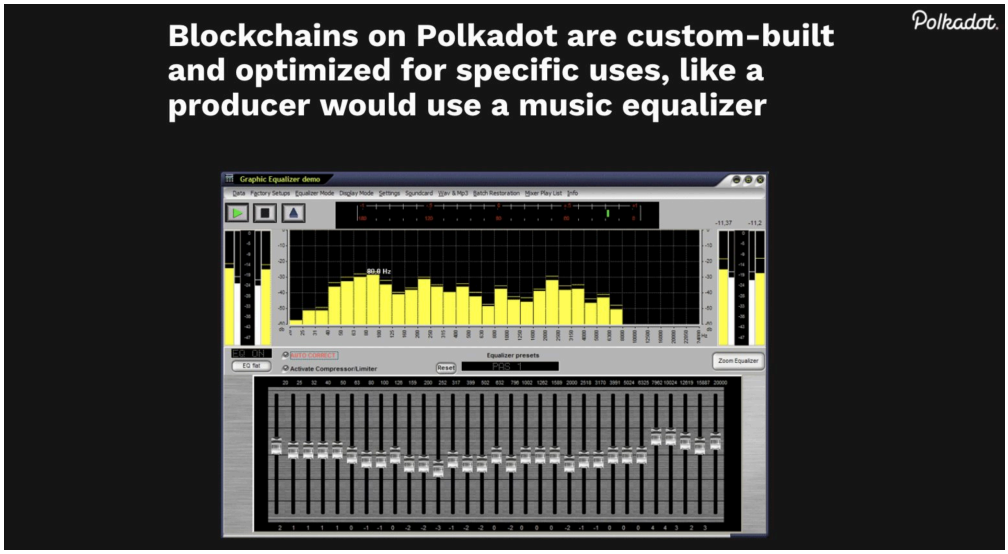
What's Polkadot trying to do?

Polkadot seeks to be a multi-chain platform that incorporates interoperability and allows for scalability. Existing blockchains are typically silos. For example, without a bridge, it's impossible to transfer information from Bitcoin's blockchain to Ethereum's blockchain. Polkadot, as a "meta-protocol," seeks to connect all the blockchains so they can process information in parallel. In other words, Polkadot aims to be a protocol of protocols -- a Layer0 solution connecting all the Layer1 blockchains (e.g. Bitcoin and Ethereum) and their applications (e.g. ERC-20 tokens). This idea can also be referred to as a "consensus enforcer."

Polkadot has also replaced the use of "hard forks" to upgrade its network with a combination of automated node updates and on-chain governance. This stands in opposition to blockchains like Bitcoin and Ethereum, which require users to actively coordinate and execute protocol design changes. Nodes that fail to upgrade get booted off the network. Most protocols with on-chain governance systems aren't that different. While users can signal their support for proposed changes using their token holdings, node operators must manually update their setups to remain synced with the network.

Polkadot uses a similar on-chain governance model where users can vote with their tokens to implement changes. But the logic used to call and execute any newly introduced features or bugfixes lives within the chain, not the client software. While running new software releases provides some performance benefits, node operators don't have to manually account for each network change. They can run old client software and remain in sync with the network because nodes simply adapt to the chain's logic. It's a no-node-left-behind approach that prevents the Polkadot blockchain from unexpectedly splintering, which could be disastrous for a network that manages consensus for multiple chains.

Finally, Polkadot aims to make it cheap, but secure, for new blockchains and apps to launch. Polkadot's development framework is called "Substrate", which is a blockchain-building framework for coders. Substrate is modular, as developers can hand-select from a list of pre-built building blocks (called pallets) to construct a new blockchain on Polkadot. This customizability enables projects to optimize their chains for specific uses or verticals (such as DeFi, Privacy, Stablecoins, Oracles, Liquidity, and others). It also allows Polkadot chains to adapt to the needs of developers. For instance, Substrate has an Ethereum Virtual Machine (EVM) module. While Substrate's base language is Rust, the EVM module opens the door for developers to port Ethereum's Solidity contracts to Polkadot blockchains.



Source: Dan Reecer

How is Polkadot going to achieve this?

The Relay Chain

To understand how it works, we take a look at the structure of Polkadot. It is essentially a series of blockchains that all connect to a single underlying layer. These interconnected chains are called "Parachains" (short for parallel chains since they run in parallel), and they all plug into a network known as the Relay Chain.

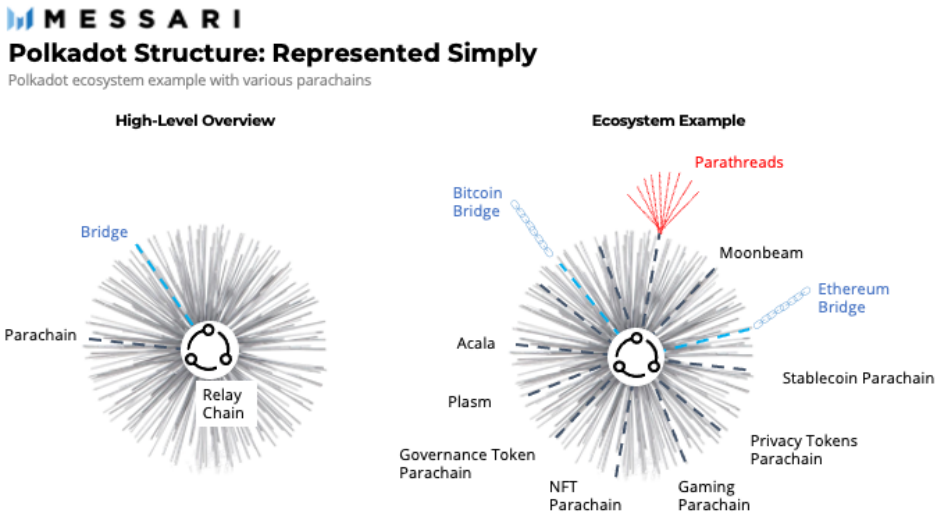
The Relay Chain is the central hub of the Polkadot ecosystem. It manages Polkadot validators and coordinates security for active Parachains. The Relay Chain is deliberately simplistic compared to Parachains. It doesn't support application development and shouldn't be confused with a smart contract platform. Instead, it serves three primary roles within the greater Polkadot ecosystem: security, interoperability, and governance.

- **Security:** The Relay Chain manages all validators within Polkadot's Proof-of-Stake (PoS) system. If someone is staking DOT, they are staking on the Relay Chain. Polkadot validators help secure and process transactions for both the core layer *and* active parachains. Parachains are essentially renting the security provided by these validators and stakers. Parachains won't need to bootstrap a validator set and enough economic security to dissuade would-be attackers. Instead, they'll each receive a share of the security provided by the Relay Chain (more on shared security below).

- **Interoperability:** The Relay Chain will also be the central communication layer for all parachains. It will route and validate the information passed between different parachains in exchange for fees. The whole system resembles how Internet Service Providers (ISPs) deliver Internet access to users. In this case, the Relay Chain acts as ISPs and parachains support the end-user applications.

- **Governance:** The Relay Chain houses Polkadot's on-chain governance system. All Polkadot proposals and network changes approved by DOT holders get processed on the Relay Chain. While each parachain can have an independent governance system, the decisions carried out by the core governance layer may have an impact on all connected

chains. Parachain teams will likely play an active role within Polkadot's on-chain governance system.

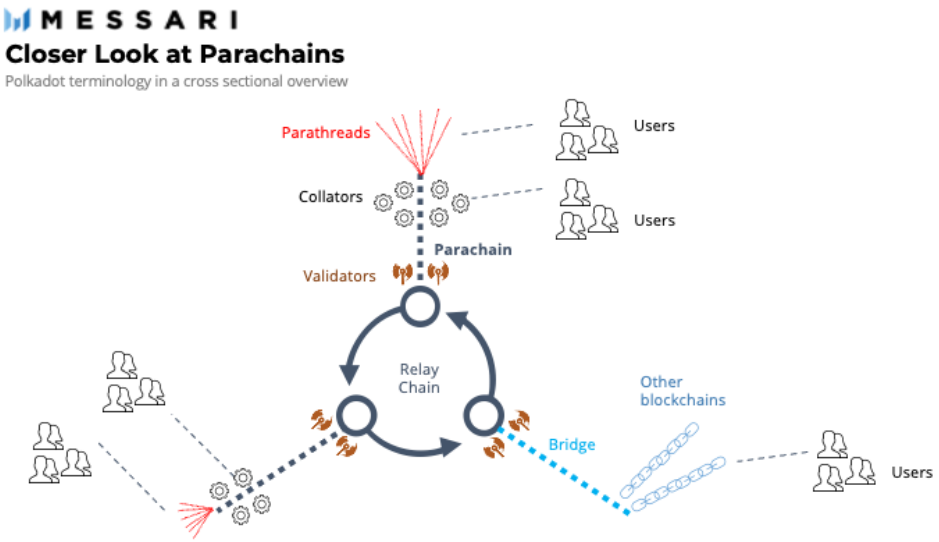


Parachains and Parathreads

There can be 100+ different Parachains connected to the Relay Chain. These chains fall under two broad categories:

1. **Layer-1 Chains:** Each parachain can be application-specific and offer one primary function, or they can provide a more general platform for application development like Ethereum. For example, some will be customized for various use-cases like privacy tokens, decentralized exchange, or gaming. This is because the same function would likely optimize for similar requirements including governance. Polkadot's Relay Chain also doesn't have smart contract support; therefore, the ecosystem will require chains that serve as general application development platforms. These parachain slots are acquired through an auction process (explained below) and managed by for-profit projects. Parachains can have their own tokens, and each one gets to produce a block for every Relay Chain block.

2. **Common Goods Chains:** These chains will typically consist of bridges to existing Layer 1 networks like public or private blockchains (e.g. private government, corporate or consortium chains). "Common goods" Parachains are awarded a parachain slot for free through a governance vote because they're helpful to the Polkadot ecosystem. For instance, a bridge to Bitcoin or Solana helps bring liquidity and an existing user base to the Polkadot ecosystem. Interlay and ChainX are bridging to Bitcoin while Snowfork, ChainSafe and Centrifuge are bridging to Ethereum.



Other projects that want a Parachain will bid for a slot in auctions. So Google Maps can try to win an auction for a parachain to go live. Users can then elect to use this specialist app (Google Maps) but if it fails or goes away, users still access all the basic functions through those pre-programmed apps.

Why would a project pay to be a Parachain? There are two clear advantages to plugging into the Relay Chain in place of launching an independent chain: instant economic security and built-in interoperability.

Unlike other Layer-1 blockchains, Parachains don't need to spend the time and money establishing a validator set and building up enough economic security to make attacks cost-prohibitive. Instead, they can outsource their security needs to the Relay Chain and focus on catering to their end-users. The Parachain model ideally allows developers to spin up new Layer-1 blockchains without requiring a large amount of upfront capital.

One drawback of letting up to 100 chains share the economic security offered by Polkadot validators is that an issue or an attack on Polkadot could take down the entire system. There's also the potential that the aggregate value of Parachains exceeds the value of the security provided by Polkadot, which would appear to open an attack vector. However, acquiring enough DOT to launch an attack will be difficult if validators and Parachains bond most of the supply.

In terms of interoperability, Parachains will be able to communicate and transfer information with each other by using the Relay Chain as an information router. For example, Chainlink's decentralized oracle network could have a dedicated parachain. Separate DeFi or Identity Parachains would be able to query off-chain data (e.g. identity-based digital signatures or verifiable claims) by sending requests to Chainlink's oracles through the Relay Chain. Users must pay a fee to validators when transferring data outside of a Parachain and onto the relay Chain.

The use of parachains moves storage and computation requirements away from the core layer. While Ethereum must store every smart contract and network interaction in perpetuity, Polkadot's Relay Chain will only store and process the snippets of information it receives from parachains. Parachains will handle the majority of user activity, enabling the Relay Chain to be relatively storage-efficient. If Polkadot's design is as efficient as designed, it might be able to increase its number of parachain slots beyond 100 without significant performance degra-

dation. Moving activity to parachains makes room for more parachains in the system (up to a point), which benefits the entire ecosystem.

Parathreads are a subtype of Parachain that periodically send information to the Relay Chain for a fixed cost. Whereas Parachains remain connected to the Relay Chain while occupying a parachain slot, Parathreads can choose to pay for Polkadot's security guarantees as they need it. The relationship between Parathreads and the Relay Chains resembles a pay-as-you-go model that should be cheaper than acquiring a parachain slot. For example, a weather company might only need to check rainfall data every 24 hours, or an insurance company might only need to process claims every 12 hours. In these cases, paying for a parachain slot (which allows projects to secure a block of transactions every six seconds) wouldn't be cost-efficient.

How might a project become a parachain?

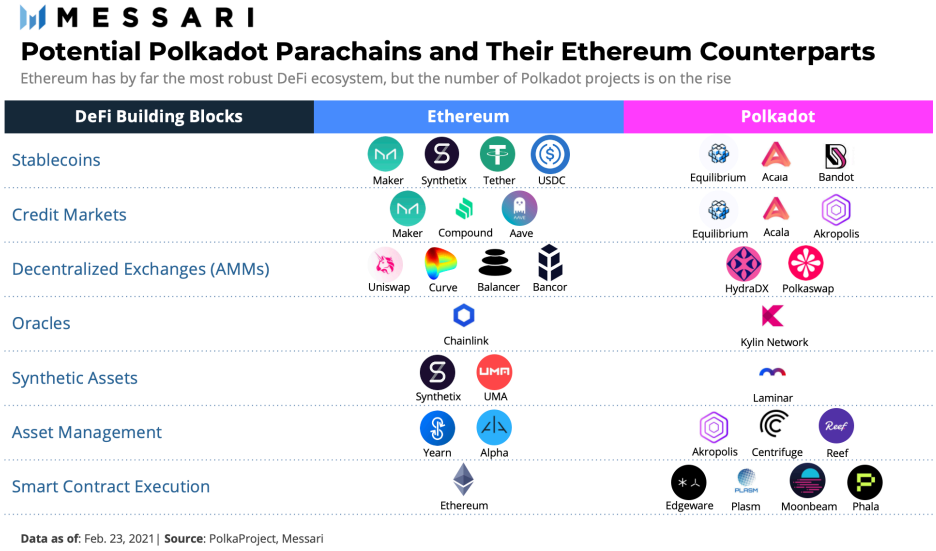
Parachain auctions haven't started yet (rumored to be this summer) but when they do, projects can post DOT as collateral to make a bid to secure a Parachain slot for a period between six months to two years. This can be from the project's own treasury, private funding, or from DOT that is loaned from their community. To incentivize their community, the project might issue native tokens in exchange. This is what's called a Crowdloan which is Polkadot's alternative to an ICO. These delegated DOTs are locked in the Polkadot relay chain and are never actually touched by the parachain team. The DOT can then be reclaimed after the lapse of the parachain slot period.

Each parachain slot will be gradually auctioned to projects using a "candle auction" which randomly selects a point in time within a known time range. The project that has the most DOT committed at that time will win the auction. This is to prevent accelerated last-minute bidding as you see in eBay.

Some projects want to be the first to win a Parachain while others want to wait. The first Parachains may end up having a first-mover advantage. For instance, the first smart contract platform to launch as a Parachain will become the go-to option (and the only option) for app developers looking to build on a Substrate-based chain. As we've seen with Ethereum, ecosystem and developer network effects in crypto are powerful. The platform with the most projects and active users could end up being the most valuable.

However, first movers will face an uphill battle trying to attract developers and users when the rest of the network is barren. Application-specific parachains (or lesser-known projects) might benefit from waiting until a well-defined user base and the potential for cross-chain interactions emerges.

The other potential advantage to waiting is a lower price-point for Parachain slots. The first crowdloans should generate a lot of attention from DOT holders, and these initial parachains may end up paying more for their slot (either by being forced to acquire more DOT or distributing a greater percentage of their native token supply to lenders). Second-movers could end up securing a slot for less if the demand for crowdloans subsides. Projects shouldn't wait too long to acquire a slot, however, as the number of Parachains the Relay Chain can support is finite. Laggards will likely be forced to overpay for a Parachain slot as Polkadot nears its max parachain capacity. Timing will be a critical factor in a project's strategy for acquiring a parachain slot.



What does the DOT token do?

DOT has a handful of key uses including bonding, staking, transaction fees, and governance.

- Bonding: as mentioned above, if you want to secure a parachain, projects have to commit DOT. If projects no longer want to have a parachain, the DOT gets unlocked and returned.
- Staking: This is important to the consensus on the relay chain. "Validators" stake DOT for a chance to be nominated to generate new blocks on the core relay chain. This also incentives good behavior as dishonest validators will see their stake slashed. "Nominators" (people staking) select the validators on the network to which they'd like to contribute their DOT. They nominate their DOT on up to 16 validators and earn a portion of the Validator's block rewards.
- Transaction fees: DOT is paid to transfer data to the Relay Chain. This can also be done in the native token of the parachain.
- Governance: DOT has on-chain voting for upgrades, changes to network fees, auction rules for obtaining a parachain, and other proposals. For example, there was a vote that passed with 86% in favor of re-basing DOT for August 2020 by 100x, where 10 million DOT was divided to 1 billion DOT.

Who are the natural buyers of DOT?

- Teams that want to have a parachain will have to commit enough DOT and/or get their community to delegate their DOTs to them to help reach the minimum amount to win the parachain slot. This means both teams and users and also likely the supporters of those platforms require DOT
- Parachains will have to accumulate DOT (through their users) to pay transaction fees to send data

- "Fisherman" stake DOT to monitor the behavior of validators and collators and are rewarded if they identify any misinformation
- Voting rights: For on-chain governance, DOT is required to have your say on the future of the blockchain. The W3F said that it would not participate in governance unless a tiebreaker vote was required.

How does Polkadot voting work?

Voting is done by all DOT holders, the Polkadot Council (13 elected members), and the Polkadot Technical Committee. There's a minimum voting threshold that is dynamically determined, depending on voter turnout.

Anyone can propose an initiative they want the Polkadot Treasury (more details below) to fund, but they must stake 5% of the total amount of DOT they think the project will cost (with a minimum of 100 DOT). If it's accepted, the 5% will be returned and the initiative will be funded. If it's rejected, the DOT is burned. Admittedly, this is a relatively high burden for the proposer if they want the Treasury to fund an initiative. The first vote was for a 100:1 redenomination, with a turnout of a third of tokens even when W3F and Parity Technologies abstained.

One of the uncertainties with Polkadot is that contentious events can be undone, damaging Polkadot's immutability properties. In September 2020, there was a controversial proposal to restore the slashed stake of a Validator that had gone offline for 14 hours. Incidentally, the Validator was named Web3Italy but was entirely unrelated to the W3F. While a member of the W3F said he would vote against the proposal, it was still passed by the community.

In DeFi, there are several major exploits a year. Some believe that exploits are fairly within the constructs set by smart contracts, while others believed these events should be rolled back. In contentious cases like this, it sets a precedent if anything can be undone with a successful vote and transactions can be nullified.

How does Polkadot deal with disagreements to avoid a hard fork?

Typically, when there are major or contentious updates to a blockchain, a fork is required. The new code is implemented and nodes have to agree to run with the new code. If they don't, then the community is divided by a hard fork.

With Polkadot, blockchains can update through on-chain voting mechanisms built into the Relay Chain. Participants can vote on upgrading and securing the network. Even Parachains can have their own governance mechanism -- which is why it makes sense for them to specialize by use-case.

DOT Supply and Tokenomics

Issuance: Polkadot has no cap on supply. The network will issue staking rewards in perpetuity to encourage users to stake and ensure a high cost of an attack on the Relay Chain. There is 10% annual inflation available to stakers and validators for contributing resources to the network's security. While this inflation rate is static, the amount of new issuance validators can receive is dynamic and depends on the amount of DOT staked. Validators will receive all newly minted DOT if 50% of DOTs are staking. If the actual staked amount deviates from this "target value" (either above or below), the proportion of rewards dedicated to validators will change to incentivize users to stake (if below) or un-staked and seek yield elsewhere (if above). New issuance that doesn't go validators ends up in the treasury. **Token Burn:** 1% of

any Treasury funds not spent during its 24 day budget period will be burned. Amounts staked in relation to a rejected governance proposal will also be burned. **Token Locked:**

- When validators stake, they're locking up DOT to earn a share of those block rewards.
- Projects and the community that delegates DOT to the projects have to bond their DOTs to secure control over that parachain.
- As of December 31, 2020, 63% of all DOTs in circulation are being staked on the network.
- When validators stake, they're locking up DOT to earn a share of those block rewards.
- Projects and the community that delegates DOT to the projects have to bond their DOTs to secure control over that parachain.
- As of December 31, 2020, 63% of all DOTs in circulation are being staked on the network.

Who might list Polkadot next?

Huobi, OKEx, Binance, and Kraken were early to list Polkadot. Huobi also created a $5 million development fund and Binance a $10 million fund to support crypto projects building on Polkadot.

All eyes are now on Coinbase. The largest exchange in the U.S. said in September 2019 that it was considering a DOT listing, and its custody arm already supports DOT and Polkadot staking rewards.

How does Polkadot's Treasury work?

The Treasury funds ecosystem projects and initiatives. Funding requests must be approved by Polkadot's Council. The Treasury currently holds a warchest of over 12 million DOT. Its size is set to increase at around ~1.6 million DOT per year, funded from a portion of Polkadot's 10% annual issuance. At current prices, the Treasury is worth around ~$400 million.

Besides new issuance, the Treasury also accumulates DOT from a portion of network fees, any slashed stakes from uncooperative or unattentive validators and collators, and fees paid by Parathreads. The accumulation to the Treasury is complicated to estimate because the Treasury receives more when there's either too little or too much staking participation.

Last year, Polkadot's Treasury funded 23 proposals worth 118,466 DOT. Separately, in 2020, Web 3 Foundation's grants had funded over 200 projects.

What is Kusama and why does it exist?

Kusama is also a scalable network of specialized blockchains built using Substrate and nearly the same codebase as Polkadot. Kusama is sometimes referred to as a "canary network" because it's a lower-value network that can flag errors with new features before they get deployed on Polkadot. Similar to Polkadot, it has a native token KSM and Kusama has not launched its Parachain auctions, rumored to be in March 2021.

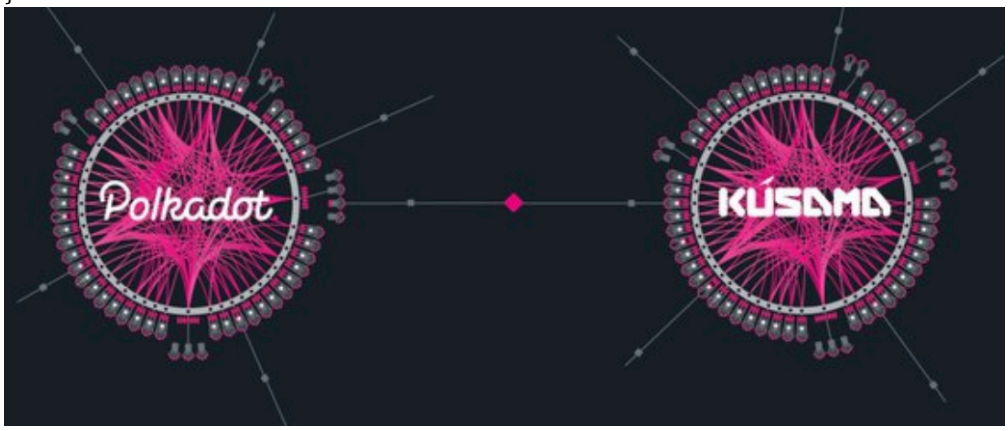
Many blockchains have a testnet, which has no monetary value. The reason Polkadot chose to have a middle ground between testnet and mainnet is because governance and voting can't really be tested in a valueless testnet where there are no monetary consequences to the outcome. Therefore to truly simulate voting, Kusama has lower barriers to entry, enables swift governance and upgrade processes, but incentivizes the community to behave realistically.

Yayoi Kusama

The network is an experimental development environment for teams that want to iterate quickly in preparation for deployment on Polkadot. Kusama's voting timetable (on-chain governance) is seven days, which is four times faster than Polkadot's 28 days. Kusama's risk-taking and nimble mentality have meant that the community has developed independently of Polkadot.

Finally, having two blockchains means that for the same amount of work, developers can launch with double the tokens and funding. For example, the team behind Acala (rumored to be bidding for the first Polkadot parachain) will launch Karura on Kusama. While Polkadot doesn't see itself as a competitor to other blockchains, this is a financial incentive to attract developers.

The two ecosystems will also be bridged, so it makes sense for the tokens by the same project to have different names and different tokens to avoid confusion.



So do they have a testnet?

The testing is done on testnets called Westend or Rococo. Rococo is the parachain testnet, and Westend is a more generic testnet similar to Ropsten (Ethereum's testnet). The typical progression for a parachain will begin with Rococo before moving to the Kusama mainnet and end by being deployed to Polkadot's mainnet.

What are the key risks around Polkadot?

Regulations

- The largest external risk to Polkadot is a Ripple-like lawsuit by the SEC. Polkadot's fundraising rounds have noticeably been outside of the US. In October 2020, Polkadot had announced a crowdfunding mechanism called Initial Parachain Offerings (IPOs). However, this sounded too much like a security IPO, so they've changed the name to Crowdloans.

Competition

- Polkadot is competing for developers and users. While Polkadot is not a smart contract platform like Ethereum, Solana or Cardano, they are undoubtedly competing to win mindshare from the same user base and developer pool.
- Developers that want to build on a Parachain must wait for a Parachain with the appropriate functionality to launch. Therefore, teams might choose to develop their application on another platform rather than wait for Polkadot to enable full Parachain functionality.

Polkadot Ecosystem

- Delays: The parachain auctions have not launched yet. It's a technically complex upgrade that might face further delays.
- Wallets: Within the Polkadot space, it's unclear how DOT is distributed among private sale investors and whales. It's also unknown which crypto funds or ecosystem projects own the most DOT
- Inflation: The schedule is currently aggressive. It is dynamic and difficult to project how many newly minted DOTs will end up in circulation.
- Bugs: As mentioned above, one of Parity Technologies' first products led to lost user funds due to a bug and then an exploit. The team and treasury are far more developed now and Polkadot believes the initial developer hiccups are behind them. They are also well-funded, which has allowed them to pay for third-party security audits.

Learn more from Mainnet 2021

Watch main stage programming from Messari's annual summit Mainnet 2021 to learn more about this exciting topic. Hear Dan Roberts and Gavin Wood discuss the ecosystem in their session, "In Conversation with Polkadot's Gavin Wood". See **more programming** on the event portal.

Video: https://www.youtube.com/embed/bg1-vHYuE20