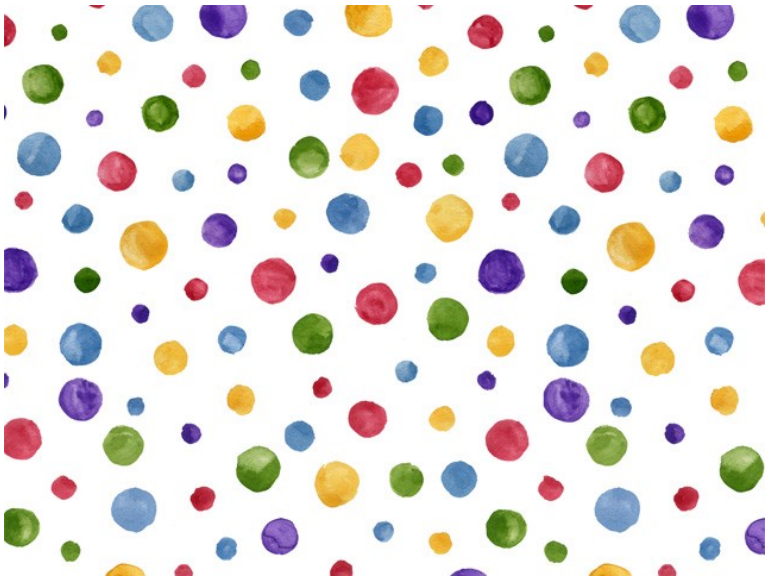
Published in Keeping Stock

Paul Kohlhaas

Feb 7, 2017 ·
4 min read ·
Listen

An Introduction to Polkadot and Parachains

The Polkadot Paper gained much attention in November last year by introducing the concept of parachains. Many haven't had a chance to properly review it yet and I thought it would be time for a brief guide and TL;DR. I also outline a few thoughts on why research on interoperability is crucial for the entire blockchain industry, as well as individual chains. In addition to the paper I recommend the video of the Inaugural Parity Meetup to gain a solid understanding.



Why do we need a Multi-Chain Fabric?

A future of multiple blockchain networks is increasingly likely. A Web 3.0 architecture of buzzing public blockchains, private consortium ledgers, anonymous zero knowledge proof chains and all the countless applications running on top of each of them. Not one chain to rule them all, but a world of diversity where individual chains serve specific use cases and specifications.

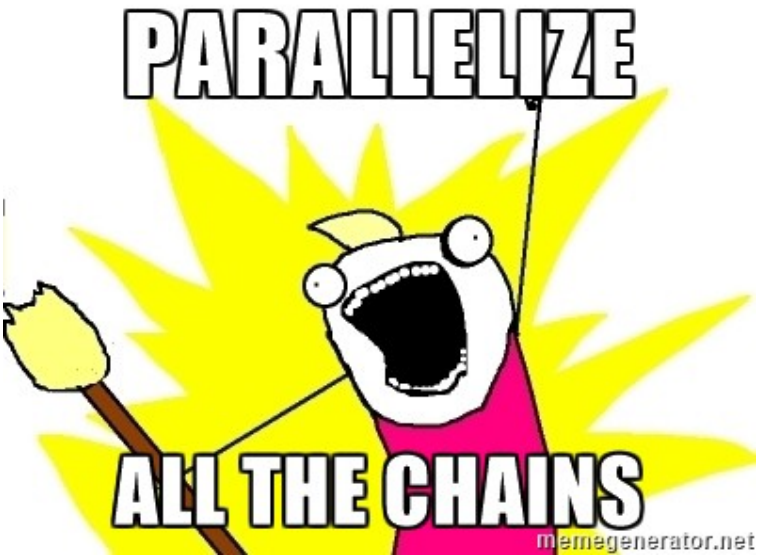
While a public blockchain can operate in a decentralized manner within its own network it still remains severely isolated towards others. Without third-party APIs a blockchain is only able to send data and assets within its own network. Currently, centralized exchanges remain the only mechanisms to transfer values

between networks. Smart contract systems like BTCRelay provide innovative solutions but remain complex one-way communication paths.

Ideally, applications and smart contracts being developed on systems like Ethereum should be able to transact seamlessly with assets and data on other ledgers in order to achieve the scale the industry is hoping for.

Enter the Polkadots

Throughout the past eight years, different blockchains have introduced different specifications. Bitcoin introduced the notion of trusted accounting and transactions. Ethereum introduced a decentralized world computer. Polkadot is the internet of blockchains. An inter-chain.



Polkadot is a relay mechanism that facilitates authenticated transactions from one blockchain to another. The idea is to *para*llelize chains that want to join Polkadot and create parachains. For more information on parallelisation, relay's and interoperability Vitalik's recent paper for R3 provides an excellent overview.

At the base layer, a Relay chain coordinates consensus and transaction delivery between member chains. The relay chain connects through all of the parachains, similar to the concept of sharding in Ethereum. It also facilitates the finalization of transactions. This is paramount because it would be impossible to move a message from one chain to another without achieving finality.

Parachains lose the function of finality and they gain the ability to communicate. But most importantly they retain the sovereignty of confirming their own validity.

> *Parachains are designed as extensible elements that can be plugged into the relay chain as validatable, globally coherent data structures.*

Simply put, Polkadot provides pooled security that is equal to all members, regardless of the protocol they operate on. Second, it enables trust-free transactions between all its member chains. An inter-chain that acts as a pool of secured messaging between blockchains.

General Design Rules

> ***Minimal**: the relay chain has no additional functionalities*
>
> ***Simple**: zero additional complexity or smart contracts are possible on the protocol*
>
> ***General**: no unnecessary requirements, limitations or constraints should be placed on parachains*
>
> ***Robust**: the protocol serves as a simple and*

Paul Kohlhaas

1K Followers

> *secure base layer. Nothing more*

Consensus Mechanism

Consensus in Polkadot is reached via a Proof of Stake mechanism that utilizes an intrinsic network token called DOT. The ownership of DOT allows participants to perform a validator role and participate in the consensus mechanism. DOT tokens also provide holders with a voting stake to add, remove or modify existing parachains, as well as participate in governance decisions of the protocol. (Note: the specifications around DOT tokens were specifically discussed at the Parity Meetup in Berlin, not in the paper).

Gavin Wood points out the precise governance mechanism has yet to be determined, but is likely to borrow from existing political structures.

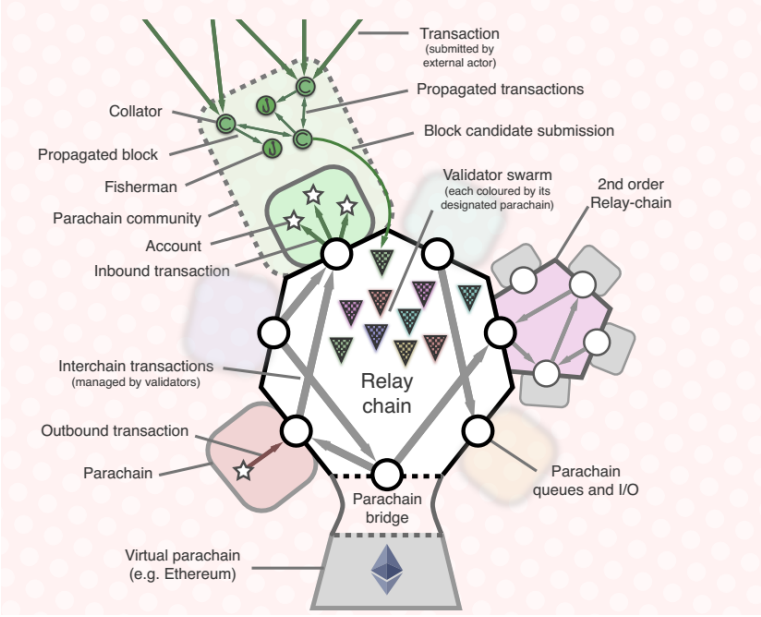
The Polkadot paper defines three cryptoeconomic network functions necessary for the protocol to operate.

Validators verify and finalize parachain candidates into blocks and receive token rewards.

Collators gather parachain transactions into Proof of Validity block candidates and receive transaction fees.

Fishermen monitor, or "fish" in the network for any misbehavior and receive a proportion of the staked bond of any bad actors.

The above should be viewed as a simplification and the paper defines these cryptoeconomic characteristics in much more detail. A future post will define these characteristics in more detail.



A summary schematic of the Polkadot system from https://github.com/polkadot-io/polkadotpaper/raw/master/PolkaDotPaper.pdf

Conclusion

> Polkadot is embarking on a very important and worthwhile research journey into inter-chain operability. The project provides a way to make significant advances in scalability through parallelizing transactions through the network and run many chains in parallel. This will benefit applications and ecosystems on all chains, especially in the increasing relevant context of public and private chain interoperability.