An Analysis of Polkadot as an Initiative for Inter-Communication Between Multiple Blockchains

Daniel Ramos, Gabriel Zanko, *MobileyourLife – Bogotá, D.C., Colombia*

Abstract

Blockchain functionalities regarding security rely on the interaction between the nodes that participate in the consensus process, shielding the information stored in the chain from outside influences due to the availability of the contents of the chain to all the involved parties. However, this also prevents for multiple chains to communicate to one another to exchange relevant information.

Polkadot created a system where multiple parallelized chains can simultaneously store information while a separate, inter-connecting layer that fulfills the need of allowing the communication between chains, performing the consensus for validation, and monitoring the behavior of nodes so security is properly maintained.

Index Terms **– Polkadot, blockchain, security, scalability, intercommunication, interoperability, parallelized.**

I. Introduction

In a recent research document, we covered Zcash[2] and how its vision and implementation is focused on combatting one of the issues that are inherently associated to blockchain and its functionality: privacy. Due to the growth in popularity of this technology and the increase in accessibility, individual and institutional users with specific needs which are not covered by the normal instances of blockchain are more common, and this fact has an obvious negative impact in the image of blockchain.

Since every chain is considered to be its own network, where the nodes partake in the consensus algorithm to verify which contents are valid and belong to the next block, the possibility of intercommunication between different protocols becomes nearly impossible. This may seem unimportant for most individual users, since simple operations in exchanges could work to move certain funds from one blockchain to another, but institutional clients that handle multiple accounts and wallets, or users looking to diversify their portfolio in an easier manner.

Polkadot, an initiative by Gavin Wood which we covered in an article some time ago, is looking towards implementing ways to facilitate intercommunication between multiple blockchains through the use of independent parallel chains that communicate through a core blockchain, which is responsible for consensus and security.

In this new document, we will go into further detail on how Polkadot looks towards implementing this mechanism and set a precedent for interoperability and scalability without sacrificing security, along with its future among the big players in the market and how it can shape the way new users interact with their assets.

II. Main Proposal And Functioning

Starting with the release of his paper in 2016[1], where he explained the hypothetical way in which a system that acted as an underlying connection between multiple blockchains, Gavin Wood has been developing his idea to its current, tangible state, establishing a system that works through the interactions of individual "parachains" via the "relay chain" that acts as the foundation.

II.a. Network Structure

Parachains are independent, parallelized data structures that act as the different blockchains handled by Polkadot. These chains have the capacity to support their own token(s) and optimize their functionality for specific uses or intentions, much like the platforms that can be built on the Ethereum network.

The main advantage of the implementation of parachains comes in scalability, since assets which are handled by large numbers of transactions could be "split" into multiple parachains, thus benefiting from the parallelized consensus and security of the relay chain. On top of this, they also offer the creation of *parathreads*, which act as lesser-scale, temporary chains for projects that do not require continuous connection to the network.

The difference between this concept and traditional blockchains is that parachains are not in charge of the consensus mechanism that validates their transactions, which we will explain later, and can even gather information that has already been validated from external sources like Bitcoin or Ethereum. This is possible by the use of *bridges* and allows for the creation of parachains which replicate the movements of the original ones, while taking advantage of the improvements brought by Polkadot.

As mentioned, the relay chain is the bedrock on top of which the rest of the network is built. It is the part of the network in charge of communicating all the multiple parachains, of ensuring the security of the information – as it stores the headers of each parachain and preventing reorganization or double-spending – and is also the stage where the consensus algorithm is applied, which involves the interaction of nodes with multiple roles, all of this while avoiding excessive centralization of functions.

II.b. Roles and hierarchy

The consensus mechanism implemented in Polkadot relies in the interaction between multiple roles, each one ensuring that the information stored in the relay chain is valid. Through a Nominated Proof-of-Stake system, a large number of ***nominators*** cast their votes into the selection of ***validators***, which later stake an amount of DOT tokens to participate in the consensus and select the transactions that will be stored in the relay chain. The information received by the validators is collected by the ***collators***, which take transactions from each shard of the parachains and sending it to the validators. The last role in the ladder are the ***fishermen***, which ensure that all other roles are fulfilling their functions and reporting bad behavior to validators, maintaining the correct functioning of the chain.

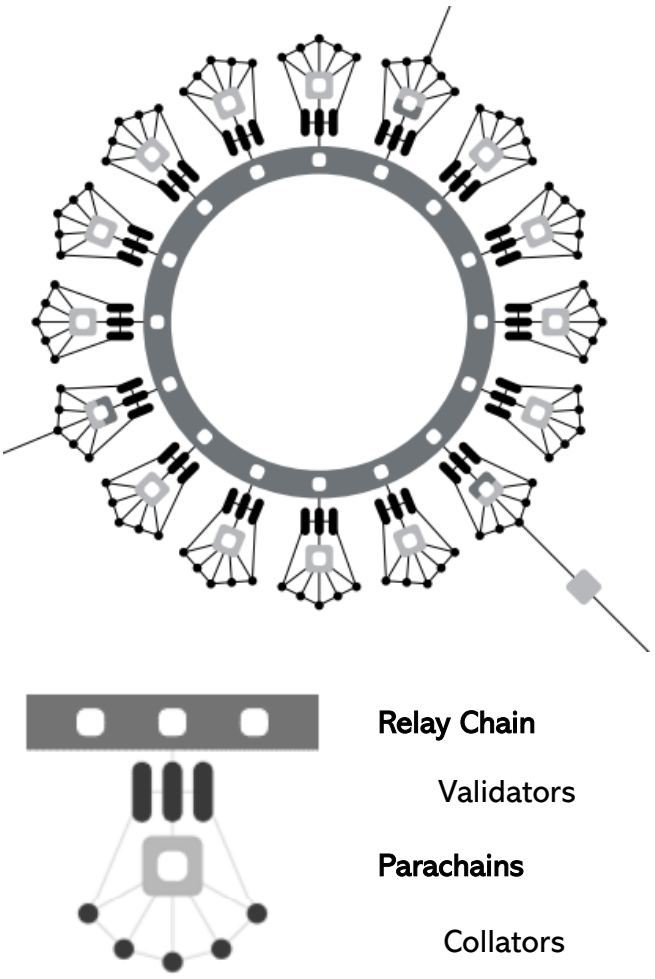

Figure 1.: Visual representation of the functionalities of Polkadot's network. The relay chain and parachains, functional units of the network, are represented in lighter colors, while darker shapes represent distinct roles that work directly on the information gathered for the chains: collators gather information from external sources and validators verify that the information in the parachains is correct and can be stored in the relay chain.

Multiple studies have shown how the implementation of hierarchy-based consensus algorithms helps towards mitigating blockchain's weakness in scalability[3,4,5], and in conjunction with the mentioned ability to create multiple parachains to support assets, Polkadot represents a clear improvement over other existing mechanisms.

II.c. Governance and the DOT token

Governance in the Polkadot network is also based in a hierarchy of roles, where elected ***Council Members*** represent the more passive stakeholders in processes like proposing referenda or vetoing malicious proposals. Besides the Council Members, the ***Technical Committee***, active teams of users involved in the building and maintenance of the network, can propose emergency referenda.

This system is supported by the DOT token, which is used in the staking for the consensus algorithm and given as a reward for good behavior, whereas bad actors lose their stake. This token also gives its holders complete control over the protocol, as they become participants of the relay chain and manage processes besides the consensus algorithm, like upgrades and fixes to the protocol. Finally, the DOT token is also required to create new parachains, and an equivalent of tokens is destroyed when a non-useful or outdated parachain is removed from the network.

III. Projects Built on Polkadot

With the growth that Polkadot has seen in the last few years, many projects have found the ground they needed to build their platform in this network, taking considerable advantage of scalability and fast validation times.

ChainLink, another platform that has experienced a steady growth in the past months, is an *oracle chain* built on Polkadot, whose main purpose is to gather data from other blockchains and networks and making it available for all the contracts in Polkadot. This interaction is made possible due to Polkadot's support for smart contracts, which also power projects like Edgeware and the current testnet for Charred Cherry.

In the financial side, ChainX and Katallasos have focused on building financial chains that allow users to hold and manage multiple assets in one single portfolio, given the existence of bridges with big chains like Bitcoin, Ethereum, Litecoin, Zcash, and many other. This interconnection also allowed Speckle OS to focus on the creation of *identity chains*, which do not link assets, but rather allow the use of fewer accounts to access multiple parachains: since the identity stored in this parachain is also verified and validated in the relay chain, it could also be used "outwards" to create accounts in other parachains.

IV. The Future

Given how the system established by Polkadot facilitates the management and secure, decentralized storage of not only transactions, but almost every kind of file, it could be a great basepoint for Internet-of-things projects where multiple devices and manufacturers can connect and communicate with each other through the relay chain, without sacrificing their independent security measures and turning the user experience for the better.

Again, we see how projects like Polkadot, lead by individuals and groups with not only the required technical knowledge about the functioning of blockchain, but also the creativity to propose new solutions and the drive to see them become a reality, are the main force that will take this still-revolutionary technology to a state where most of its inherent problems are almost unperceivable, while also maintaining the sense of community that keeps a blockchain healthy and plowing the fields so other enthusiasts and visionaries can plant the seeds for the future of not only blockchain, but the handling of digital information and communications.

V. References

1. Wood, Gavin (2016) "Polkadot: Vision for a heterogeneous multi-chain framework". Retrieved from: https://polkadot.network/PolkaDotPaper.pdf

2. Ramos, Daniel & Zanko, Gabrel (2021) “A Review of Zcash as a Cryptocurrency Platform Aimed Towards Maintaining Privacy Between All Parties” Mobileyourlife.
3. Oktian, Yustus & Lee, Sanggon & Lee, Hoon. (2020). Hierarchical Multi-Blockchain Architecture for Scalable Internet of Things Environment. Electronics. 9. 1050. 10.3390/electronics9061050.
4. Sahoo, S., Fajge, A. M., Halder, R., & Cortesi, A. (2019). A hierarchical and abstraction-based blockchain model. Applied Sciences, 9(11), 2343.
5. Ismail, Leila & Materwala, Huned. (2019). A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. Symmetry. Symmetry 2019, 11(10). 10.3390/sym11101198.