Polkadot: A Decentralized Blockchain Champion or a Hype Balloon?

By: Sujit Magesh Shanmugaram

Student ID: 1004496119

For: APS 1050 Blockchain Technologies

Introduction

Polkadot, a novel blockchain project, was founded by Dr. Gavin Wood, along with co-founders Peter Czaban, and Robert Habermeier in 2016. (1) Blockchains are a system or a record of transactions which are stored and linked recursively on a peer to peer network containing many users and computers. The primary purpose of blockchain technology is to decentralize the many aspects of the internet and technology by instead relying on the immutability of record-keeping in the absence of trust.

Dr. Gavin Wood is not new to the blockchain space. He co-founded Ethereum, the second largest cryptocurrency by market cap, and invented the Solidity language. Solidity is a high-level language mainly useful for designing and implementing smart contracts within Ethereum. Smart contracts are programs which govern the behavior of accounts within the Ethereum Virtual Machine. (2) Dapps, decentralized applications, are applications which run on the basis on smart contracts. Dapps are useful for many reasons, including cost reduction, privacy, and transparency, however the main benefit comes in the form of censorship resistance. No single entity controls the use of Dapps and anyone can look through the source code should they choose to.

What makes PolkaDot unique is its seamless integration with Substrate, enabling the use of Parachains. (3) Parachains are application specific blockchains attached to the relay chain which facilitate the integration of other blockchains, including ones from external networks such as Bitcoin and Ethereum, into the PolkaDot network. Enabling cross-chain communication, PolkaDot aims to be a hub of blockchains with a special emphasis on security, privacy, and decentralization. Further, PolkaDot's underlying vision facilitate the rise of a decentralized internet, Web 3.0. In partnership with the Web3 foundation based in Switzerland, Web3.0 looks to leverage blockchain technologies to link applications with each other rather than a central entity, effectively creating a network of decentralized protocols.

In doing so, Polka dot must address complex issues facing existing blockchains such as scalability, security, forking, immutability, consensus, and of course, true decentralization. Polkadot has many unique and progressive solutions to staking and governance, but to what extent are they sustainable? Relatedly, should users of Bitcoin and Ethereum consider using DOT, or will the framework and governance structure of Polkadot doom itself to fail?

The Web 3.0

In order gain understanding of the Web3.0, blockchains and Polkadot's vision of connecting the two, one must first understand the predecessors, Web1.0 and Web2.0. Web 1.0 refers to the first stage of the internet. In this first iteration of the web, users could search for information and read it. (4) There was very limited ability to interact meaningfully with the static webpages and with other users. The internet was effectively a "read-only" file. Although Web1.0 was effective in making information available to anyone at any time, it lacked the ability to allow users to participate in the content being shared. As such, this network was popular for many brick and mortar businesses who wanted to increase exposure to their products. Users quickly found that this sort of web content was far too limiting.

Web2.0 was a response to the obvious gap in Web1.0's functionality. The rise of Web2.0 brought the ability of users to interact with web, now a "read-write" web. Web2.0 dramatically changed the way users used the internet. Users could now interact with each other and with the now dynamic webpages to create a much more intuitive user experience. Some of the most prominent websites which showcase the full extent of Web2.0's functionality are YouTube and Reddit. YouTube is built almost exclusively by its content creators while the YouTube entity itself only acts as a medium for its users to find and generate content. Youtube makes profit primarily through advertising and promotions, which is directly proportional to the quality and

quantity of users and content available on their platform. Although Web2.0 brings huge potential to connect users with each other, critics have pointed out that it has become overly centralized. The centralization, they assert, has led to an excessive focus on profits, causing mass surveillance, data breachers, censorship, and decreased privacy. Because YouTube has a large incentive to support its advertisers, it has often censored content to appease them, which has caused much controversy in the past. (5)

For these reasons, a decentralized, free web is highly favorable. In response, the Web3.0 model seeks to overturn the Web2.0 model by leveraging blockchain technology to link users to each other in a peer to peer network. Due to the immutability and security of the blockchain network, content cannot be censored or hidden by any corporate entity or governmental organization. However, because of the disorganized nature of blockchain technology and the associated increase in data, and the need to intelligently sift through the data is present. Although such capabilities are already in existence in Web2.0, they remain markedly biased and centralized. For example, in early 2021, the trading app RobinHood received a 1 star rating on the Google Play Store. (6) Google's AI sifted through the reviews and removed all reviews which it believed were made by bots. Although Google's AI did its job correctly, Google is within its right to remove any review, even if a review is legitimate. In the leap to a decentralized, peer to peer internet, there must be confidence that an AI will display only unbiased information. If Web3.0 is fully implemented, advancements in AI technology and deep learning would need to be made in order to provide users with the most personalized but unbiased data possible. (7)

Polkadot is the flagship project of the Web3 Foundation – a non profit organization founded in mid-2017 in Switzerland by Peter Czaban, Robert Habermeier and Dr. Gavin Wood. Soon after founding Web3, Gavin Wood also founded Parity technologies and began a joint project between Web3 and Parity to produce Polkadot. The Web3 foundation focuses on fundamental research into cryptography, algorithms, economics, and networking. (8) The underlying cause of Parity Technologies, The Web3 Foundation, and Polkadot is to create, develop, and raise awareness for blockchain technologies that will create a more transparent and decentralized internet.

How does Polkadot Work?

Polkadot's validation protocol is slightly more complex than Bitcoin's or Ethereum's. The base connectivity layer for the Polkadot network is known as the Relay Chain. (9) The main purpose of this central chain is to perform governance, stake transactions, and share security with the network. The capabilities of the Relay Chain alone are deliberately limited – even smart contracts are not supported on the base chain alone. (10) This allows the base chain to be lightweight, ensuring the chain length is optimized as transactions are built over time. In order to enable more key functionalities such as smart contracts, much of the computation is instead delegated to Parachains and Parathreads, which are application specific data structures that are globally coherent and "cross validatable" by the main Relay Chain. (11) The key constraint of a Parachain is that they must be verifiable by the main chain. Most commonly, Parachains are individual blockchains, but there is no requirement for them to be so. Parachains are the reason for Polkadot's claim to support up to 1,000,000 transactions per second. (12) This speed far exceeds the capabilities of Bitcoin and Ethereum 2.0, which max out at 8 and 20 transactions per second, respectively. Multiple Parachains on the Relay Chain can communicate amongst themselves, preventing the main chains from becoming too congested. Parachain slots currently are only obtainable through a bidding process, and successful bids typically run core elements of the Polkadot framework – such as staking, privacy, interoperability, and smart contracts. Ultimately, the purpose of parachain auctions is to allow the Polkadot network to scale through specialization.

The Polkadot network has three node types: Validator nodes, Nominator nodes, and Collator nodes. Each Parachain network, as well as the main Relay Chain, has its own separate nodes. The three main functions of the Validator are:

1. Verifying: The Validator nodes must verify that the information contained in the blockchain and the blocks are authentic. Validators of the Main Relay chain must guarantee that each Parachain attached to the main chain follows its own unique rules. (13) Validators of a Parachain participate in an off-chain consensus mechanism, which is pre-determined by the Parachain creators.

2. Block authoring: Validators must also create new blocks to add on their chains, based upon the information they validate, and from the consensus mechanism from other validator nodes. What makes Polkadot different from other blockchains such as Bitcoin is that the consensus mechanism used is Proof of Stake (PoS). Bitcoin in contrast, uses Proof of Work (PoW), otherwise known as the Nakamoto consensus. Although Nakamoto consensus comes with excellent security and is highly effective when coming to a decentralized consensus, it is also extremely energy intensive and lacks provable finality, which is the guarantee that a produced block is finalized. The mechanism by which validators produce blocks between each other is through BABE (Blind Assignment for Blockchain Extension). A random lottery is drawn, accounting for each Validator's stake, and the Validator with the "winning" number is given the privilege of producing the next block on the chain. (14) This minimizes stalling the block production process, and more importantly, separates the "finality" process from production.

3. Finalization: Polkadot's finality gadget is known as GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement). In contrast to bitcoin, which reaches consensus for each new block added to the chain, GRANDPA reaches consensus based on each chain. This opens up the possibility to reach consensus for multiple new blocks on a chain in a single round. (15) At this point, there can be multiple chains in waiting to be finalized. Validators must vote on these chains, and once a consensus on 2/3 plus one Validators is achieved, the chain is finalized. Because the finalization and block production mechanisms are separated, the slower finalization process can take place more efficiently, leading to a large decrease in processing power when compared to other Byzantine fault algorithms (BFT). In this case, as long as 2/3 Validators are honest while at most 1/5 are Byzantine (dishonest), then the system will maintain integrity.

Another question naturally arises from the analysis of Validators: What if over 1/5 Validators are Byzantine? In other blockchains such as Bitcoin, the system maintains integrity so long as the total honest hash power of the network is 50% plus one nodes. This means that as long as the honest miners control at least 50% of the computational power of the network, the blockchain is tamper-proof. Compared to Bitcoin, Polkadot is seemingly less secure, as it only requires a fifth of the validators to be dishonest for the network to be tampered with. However, the Proof of Stake consensus mechanism makes it very hard for Byzantine validators to gain power. The first hinderance to dishonest validators is the limit on the total number of Validators on Polkadot network, which is currently 1000. (16) For an individual – typically a corporation with enough resources – to become a Validator node, it must first provide a stake. This stake is dynamic and changes over time depending on the market price of DOT, as well as the total interest in becoming a Polkadot validator. (17) Currently, the minimum stake to enter a bid as a validator is 1.7 million DOT, which is equal to over $40 million USD at the current market exchange rate between DOT and USD. For most individuals – and even most corporations – this amount discounts them from participating as a Validator.

In Bitcoin's current stake, individual miners cannot hope to make any profit either, as the total hash power of mining determines the probability of receiving rewards from the blockchain. Individuals with low hash powers instead join off-chain mining pools, which "crowdsource" hashing power to develop a more stable income stream. Polkadot, in anticipation of "pools" forming off the main chain, have developed a system in which pools can be formed on-chain through the use of nominators. Nominators can sponsor validators by

providing a portion of the total stake to the Validator in exchange for a share of the Validator's reward from the network. Because the pools can be formed on-chain, the rewards can be sent directly to the nominators based upon the portion of stake the Nominator supplied to the Validator. The purpose of a stake is to ensure that only the individuals or groups with high investment in Polkadot's success are given the power to modify and verify the blockchain. Currently, Nominating requires a minimum stake of 120 DOT. However, the more important consideration is that there is a hard cap of 22 500 Nominators on the network. Having more than the minimum stake will not qualify more Nominators if the cap ahs already been reached

Although validators may have high incentive to upkeep the network integrity, there is always the chance that a validator can become dishonest. For this reason, Polkadot automatically punishes Validators and their Nominators for misbehavior through a mechanism named "slashing", which stores in the treasury a portion of the stake put up by the Validators. (16) The rationale for this action, as opposed to redistributing the slashed funds or to delete them forever, is that the slash may in part be reverted in situations such as faulty runtimes. This forces Nominators to have high standards for their Validators and encourages the nomination of more reliable Validators. Another notable property of slashing is that the value of slashes are calculated as a percentage of the total amount staked by the Nominators, while rewards from the blockchain for participating as a Validator are not. This means that there is a far greater liability to slashing than there is reward to being a Validator. This encourages higher standards for Validators and increases the overall system integrity because the stakeholders have a lot more to lose in the event of misbehavior. This system is called Nominated Proof of Stake (NPOS).

The third and final node type in the Polkadot ecosystem is known as the collator. Collators aggregate transactions from users into block and produce state transition proofs for Validators based on the block candidates. (18) Unlike Validators however, Collators do not verify transactions. This means that there is no meaningful benefit to have an unlimited number of Collators on the network. Although the main purpose of Collators is to generate block candidates for validators, they also enable cross-chain communication. This is the main mechanism by which Parachains are able to communicate with each other.

An intended limitation of Parachains however, is that the blockchains used between them must follow the same consensus protocol as the main Relay Chain. This can cause some incompatibility issues when attempting to communicate with other existing blockchains such as Bitcoin, which uses proof of work consensus as opposed to nominated proof of stake. The solution to this in Polkadot is known as a Bridge. Bridges allow interoperability between blockchains with sovereign and diverse rules through either a centralized or more decentralized channel. (19) In the case of the Bitcoin Bridge, btc can be "teleported" across into tokens representing btc on the Polkadot network, known as PolkaBTC. These tokens can also be "burned" to retrieve back the same bitcoins. This property of Polkadot's network allows for cross-network communication, which could pave the way for more complex and intuitive DApps to enter the Polkadot ecosystem.

There is also another pseudo-entity on the Polkadot ecosystem known as a Parathreada. Because the total number of Parachain slots on the Relay Chain are limited, the slots are typically given to high profile projects with excellent Polkadot use cases and large computational effort. Smaller projects may be left without an opportunity into the network, which may hamper creativity. For this reason, a set number of Parachain slots allow a group of smaller projects to operate within a single Parachain slot. (9) Another important distinction between Parachains and Parathreads is that Parachainsa are always connected to the Relay Chain whereas Parathreads are only connected when it is necessary. Parathreads provides more equitable access to the main Relay Chain, which will allow smaller projects to still contribute to the network.

Polkadot Governance

Polkadot's governance system is extremely sophisticated when compared to blockchains like Bitcoin, which has no governance at all. Polkadot claims that this governance model will allow it to "evolve gracefully over time at the behest of its stakeholders". To do this, Polkadot has implemented novel on-chain governance rules such as voting mechanisms in order to give its holders a say in the project's future. In Polkadot, there are three main groups who hold power in deciding the course of the project. The most basic group are the DOT token holders. Each holder of the DOT is given voting power proportional to the amount of DOT they own. These votes can influence referendums regarding forks, changes to the network, and can be used to elect the other two groups who hold power in the Polkadot network.

The second group which holds power in the Polkadot network is known as the Council. The purpose of the council is to represent passive stakeholders in Polkadot. Any DOT holder has the right to run for one of the 13 rotating council member positions. The only condition is that the candidate must post a bond of 100 DOT, which will be forfeited if the candidate loses their bid for a council member seat. (20) If the candidate is successful, then they can serve as a council member for a term of one week, after which the process to select new council members is restarted. The constant cycling of council members allows the stakeholders of DOT to constantly voice their opinions of the council members through the on-chain voting mechanism. The bond of 100 DOT prevents voter fragmenting by allowing only serious candidates to be voted and elected. Council members are elected using Phragmen election algorithm, which allocates votes based on the sentiment and expressed indications of the electorate as a whole. In this way, a DOT holder may indirectly vote for as many candidates at once, but only those who more closely align with their views.

The elected council members have three main responsibilities:

1. Proposing new referenda: Council members represent the passive stakeholders of DOT. As such, they must propose referenda which reflect the issues facing DOT holders and evolve the Polkadot network to maintain integrity in the system. Referenda will be explained in more detail shortly.
2. Cancelling malicious referenda: Any DOT holder can propose a referendum after bonding some DOT as collateral. This could result in some referenda being antithetical to the Polkadot network or it could be harmful in the long-term. It is the duty of the council members to weed out any malicious or trivial referenda.
3. Electing the Technical Committee: The third and final core duty of Council members is to elect the technical committee, which is the third group which holds power in the Polkadot system. Technical committee teams can be added and removed by the Council members through a simple majority vote.

As it relates to proposing referendums, the Council must reach a simple majority to pass. For Council motions – which are decisions which cannot to be voted upon by DOT holders – the Council must reach unanimous support. For motions which fail to garner such support, but still reaches a supermajority (greater than 60%), then the motion becomes a referendum, which can be voted on by DOT holders. At any point, all council members hold the right to veto any proposal or referendum. If a proposal is resubmitted after a certain period of time, it may not be vetoed by any member again.

Before getting to the third and final governing group of Polkadot, it is important to understand the purpose and mechanism of referenda in the Polkadot ecosystem. There are two main types of referenda – public referenda and Council referenda. Public referenda can be proposed by any DOT holder after a bond is posted. Although there is a minimum bond amount that must be posted when submitting a proposal, the more relevant parameter is that there can be a maximum of 100 referenda in queue, and only the 100 referenda with the highest bond amounts can be listed. In order to increase the bond amount for a proposal to be able to bring it to the proposal queue, referenda proposals can be "seconded" by other members of the Polkadot community. An important consideration which must be made before proposing a referenda is that

all DOT bonded will be held in limbo until the referenda is brought to the Council table. (21) Thus, it is possible that the DOT placed in bond may be held indefinitely, as there is no guarantee that the proposals in queue will be brought to the Council table. There is also no way to remove a proposal once it has been made. This ensures that only serious proposals are made by the community.

The second type of referenda is known as the Council referenda. These referenda do not have to go through the proposal queue as with public referenda. In this case where referenda proposals pass the Council unanimously, the referenda will benefit from Adaptive Quorum Biasing. This type of referendum is far easier to pass, requiring a supermajority – 60% of the vote – to reject. In the case where a proposal passes with anything less than unanimous consensus, but more than 50% support of the Council, the proposal becomes a referendum which requires a simple majority to pass. A proposal which does not garner at least 50% support from the Council fails. At any one time, only one referendum may be active on the chain, with the exception of emergency referenda. All non-emergency referenda have a fixed enactment time of 28 days, which is the delay between a referendum being approved, and the point at which it is enacted. Emergency referenda do not have such delays, in order to protect the integrity of the network.

As mentioned, the third and final governing group of Polkadot is known as the technical committee. The technical committee is in charge of enacting the proposals and successful referendums of the Council. Similarly to the Council, the technical committee also have the ability to table emergency proposals, which can bypass the enactment cooldown. Typically, the technical committee use this ability to impose emergency big fixies or to rapidly enact new features into the runtime. The committee also has the ability to "cancel" successful referenda proposals in special scenarios, if there is unanimous agreement. The Council also has a similar ability, however only requiring a supermajority. This is a failsafe built into Polkadot's governance system in order to protect the system in case there is an issue found in a proposal after it has passed a referendum.

No matter if a proposal is submitted by a common DOT holder, a Council member, or a member of the technical committee, all changes to the Polkadot network will need to go through a referendum in order to be enacted. The intention behind this unique functionality of Polkadot is to allow all members of the Polkadot community, weighed by stake, to contribute to the network's future in a democratic fashion. (22)

The Treasury

The Treasury is a separate account on the Polkadot network which is a restricted account holding funds that are intended to be used by the Council. (23) Some examples of Treasury fund use cases are auditing, marketing, community events, outreach, software upgrades, and monitoring services. The Treasury is a collection of funds built from transaction fees, slashing, Parathread auctions, etc, and can only be controlled via a proposal submitted by the Council. Anyone can propose a spending proposal to the Council by creating a special Treasury proposal. A key distinction between a referendum proposal and a Treasury proposal is that a user must bond a the greater of either 100 DOT or 5% of the proposed funding. If the Treasury proposal is approved, then the bond is returned to the proposer. However, if a proposal is denied, then the bond is burned. There is no way for a user to unsubmit a proposal after it has been submitted, in order to ensure that all proposals are serious and to avoid spam to the Council.

Forking

Forking is a term both feared and loved in the cryptocurrency world. Over time, some blockchain technologies may serve communities who grow dissatisfied with the functionalities offered by an existing implementation of a cryptocurrency. If a modification of the functionalities is possible, then the users of a blockchain may consider a fork in order to change the problematic functionalities. (24) If a change is not too

disruptive, the community may consider a soft fork, which is backwards compatible with the previous versions. (25) In most cases however, a change to the protocol of the blockchain to create any meaningful changes, which requires a hard fork. This creates two versions of the blockchain, one for the old version, and one for the modified version. For this reason, hard forking can be undesirable for some blockchain technologies. One of the most notable and successful hard forks in cryptocurrency history is the Bitcoin Cash fork. Bitcoin is the largest cryptocurrency by market cap, however, it faces issues with scalability – specifically with transaction speed. For this reason, on August 1, 2017, a subsection of the Bitcoin community decided to introduce a hard fork to the Bitcoin protocol, increasing the block size from 1MB to 32MB. This would increase the total transactions per block, assuming the block time is kept constant. The most obvious side effect was that a new cryptocurrency was produced as a result of the hard fork, known as Bitcoin Cash.

The reason that forking happens after a protocol update is that some nodes may still be running the older version, while others switch to the new version. The idea of a blockchain itself makes it difficult to solve forking. Blockchains re decentralized systems with a special focus on anonymity. (26) Thus, it becomes difficult to coordinate updates with anonymous users that must be agreed upon by an entire community. The Polkadot network solves the issue of forking in multiple ways. The founding principle of Polkadot is to ensure that the majority stake can always command the future of the network. (26) Akin to a democracy, Polkadot ensure that the minority must follow the majority, but there are always channels for the minority to voice their opinions. The progressive referenda system achieves this purpose. After a referendum passes a proposed modification to the network, all nodes are forced to update to the latest version, eliminating the possibility of creating a hard fork and eliminating any friction in the community caused by the duality of forking. As blockchain technology evolves, the need for updating outdated methods is ever prevalent, and Polkadot's solution looks towards democracy as a potential solution to this problem.

What is a DOT?

In Polkadot, money is power. As btc is to Bitcoin and eth is to Ethereum, DOT is the fundamental token of the Polkadot network. Similarly, the smallest denomination of a DOT is known as a Planck, which is a reference to the Planck Length, which is the smallest distance in the universe. (27) In the Bitcoin and Ethereum networks, the smallest possible denominations are known as the Satoshi and the Wei, respectively. There are exactly 10,000,000,000 Plancks in a DOT token. Aside from being used as a currency for a transaction between two parties, there are three main practical use cases for DOT in the Polkadot network:

1. DOT for Consensus: The integrity of the network relies on honest users. To create a trustless system, the system must ensure that misbehavior is punished, and good behavior is rewarded. Active users, otherwise known as users who place their DOT at risk of slashing via staking, are also rewarded for good behavior via distributions the network through controlled inflation of the DOT. (27) This disincentivizes malicious actions, as the holders of the most Polkadot are in control of the validation of the network. If the public opinion of the integrity of the network is negatively swayed, the associated token price will go down, impacting the most staked players the most.
2. DOT for Governance: As previously mentioned, DOT hold value through use in governance. Key functions in the Polkadot pseudo-democracy include referenda proposals, Treasury proposals, weekly voting on Council members, and even running for a Council position. (27) The highest stakeholders in DOT also hold the most influence on the network, both off the chain and on the chain. Higher stakeholders are assigned more power through their votes and can more easily influence the decisions made by the Council.
3. Parachain Slot Acquisition: As stated before, Parachain slots are limited to approximately 100. These slots are leased to relevant projects as determined by the Council. The fees associated with leasing are

bonded for the duration of the lease and are returned after the Parachain is free to lease to a new project.

DOT is an inflationary currency. Polkadot is designed to inflate itself at a rate of approximately 10% annually, with distributions going to the Treasury and to Validators as rewards. The amount going to Validators or the Treasury is determined by a formula, which is a function of the total proportion of DOT being staked. According to the Polkadot website, an ideal staking rate of 50% stabilizes the networking. (16) If the stake rate falls, then the security of the system becomes compromised. If the stake rate rises, then the liquidity of DOT is reduced which is also undesirable. Thus, a middle ground should be found. By viewing the Polkadot live staking website, it can be seen that approximately 53% of the total coin supply is currently staked. (28) DOT holders who do not stake are at risk of devaluation of their holdings, as there should be approximately a 10% decrease in price per year due to inflationary forces alone. Thus, it is highly recommended that any DOT holder with a sizeable DOT portfolio stake their holdings to prevent this loss.

Transactions and Fees

In Polkadot's main Relay Chain, there are a limited number of Validators (currently 1000), and therefore are limited computational resources. Polkadot assigns fees to each transaction to prevent users from overloading the network. There are 3 main fee types associated with completing transactions on the chain – a per-byte fee, a weight fee, and a tip fee. (29) Per-byte fees, also known as length fees, are a flat fee added per byte of the transaction. The weight fee is a multiplier to the length fee which accounts for the time and effort required to execute the transaction. The purpose and operation of the fee is similar to "gas" in the Ethereum blockchain. This accounts for computational power required by validators to complete the transaction. The final fee type is optional – the tip fee. Tips can be added onto a transaction in order increase the priority of a transaction. Validators are more likely to validate transactions with higher tips, as it provides them with more DOT rewards. Of the total fee, only 20% goes to the Validator nodes, while the remainder go to the Treasury, although this ratio can be subject to change by the Council. (29)

Although transactions are used primarily for transferring tokens such as DOT, they can also be used for recording events related to Polkadot's operation on the chain. These are called operational transactions. Some examples are misbehavior reports, council operations/ logs, and election operations. Validators must prioritize operational transactions by reserving 25% of a block's space for these emergency transactions.

It should be noted that any transactions which occur on Parachains or Parathreads do not necessarily need to own DOT in order to pay the transaction fees, as is the case on the Relay Chain. This is because Parachains and Parathreads have their own economic model, and therefore do not need to follow the same rules.

Polkadot's Funding Strategy

Before talking about the specifics of Polkadot's funding strategy, it is important to understand the cryptocurrency industry's equivalent to an initial public offering (IPO), an initial coin offering (ICO). (30) A startup looking to raise funds for a specific product or service may consider an IPO in order to meet the minimum funds to get started. Similarly, a new cryptocurrency startup would be interested in an ICO to raise their funds. A key distinction between ICOs and IPOs is that IPOs typically deal with large banks or investors, meanwhile ICOs typically deal with supporters, similar to a crowdfunding event. This makes it difficult to regulate ICOs, resulting in a large portion of them being unregulated. This regulation allows a much broader range of structuring methods as compared to IPOs.

There are three main types of ways in which ICOs can be structured. The first is a static pool of tokens with a predetermined price. (30) This type of sale is typically associated with large entities buy a large sum of tokens at an agreed cost. The second is known as a dynamic pool, which also has a limited number of tokens, but the

price varies based upon the market and the demand for the token. There also a second version of the dynamic pool, which has a predetermined price, with no hard limit on the number of tokens which are expected to be sold. The dynamic pool methods are typically associated with crowdfunding ICO strategies, as it is hard to predict either the total number of tokens or the price at which tokens will sell, while keeping the other constant.

When Polkadot began selling its tokens, it had a goal of distributing a total of 10,000,000 DOT tokens. Of that, 30% (3,000,000 DOT) were reserved to be held by the Web3 Foundation. (31) The first ICO was held on October 2017 and was successful in raising over $140 million USD. (32) The method of the ICO was a "Spend All Second Price Dutch Auction" – that is to say that the sale is capped and would close after a certain amount of ETH had been raised from the sale of DOT. Unlike other capped dynamic pool sales, in Polkadot's case, both the number of tokens (5,000,000) and the price of the token are kept constant. However, the price that each participant spends on a token will be dependent on the total amount raised, divided by the total number of tokens. The people who spend more will be distributed a proportional number of tokens. In this way, all participants are equitably distributed the tokens. After the initial ICO, each DOT was sold at $0.29 USD. At this point, out of the 10,000,000 DOT offering milestone, Polkadot had achieved 80%. The remainder was left for smaller, future pre-launch distributions.

In August 21 of 2020, Polkadot had decided to redenominate the DOT supply by a factor of 100. This meant that all those who had purchased 1 DOT prior now held 100 DOT, making the effective DOT in circulation approximately 1 billion. According to the Polkadot live staking website, there are approximately 1.16 billion DOT in circulation today. (28) Further, based on the current market price, investors had made a 9730% return on investment since the ICO!

Strategy Considerations

The Polkadot blockchain was created as a response to the failures of similar projects such as Bitcoin and Ethereum. Although many of its competitors have excellent security and decentralization, Polkadot believes they fail in five key areas: (33)

1. Scalability: Many previous cryptocurrencies failed to modern transaction needs. For example, Bitcoin is only capable of 7 transactions per second, which cannot meet the demands of modern society.
2. Isotability: Many cryptocurrencies serve a niche market, or a specific use-case. Not many cryptocurrencies are malleable enough to be able to meet the demands of all worldwide users.
3. Developability: Many cryptocurrencies lack the ability to build upon itself, leading to very unintuitive user interfaces
4. Governance: Networks need to remain malleable and open to change, both in society and within its community. Blockchains such as Bitcoin have no governance, which can lead to community friction and resistance to change.
5. Applicability: The blockchain itself needs to serve a purpose. It must not serve simply as a "middleware" to other applications.

Thus, Polkadot must address these issues while adhering to a similar level of security and decentralization as its predecessors. Polkadot resolves the issue of scalability through the use of Parachains, which are independent blockchains connected to the main Relay Chain. These blockchains can either be connected indefinitely to the main Chain, or only when they need to be. This allows specific transaction types to go through separate channels, allowing for greater transaction speed and volume. Parachains are also able to address the issue of Isotability, as they allow the blockchain to cater to a wide variety of use cases, not limited to those of DOT. Polkadot is also highly developer friendly, with its own testnet Kusama and a high degree of support from the Web3 Foundation, Parity Technologies, as well as the Polkadot Council itself. Polkadot

also stands out in terms of governance, imposing its own pseudo-democratic ruleset onto chain, allowing for seamless and versatile democratic elections and referenda to occur. Finally, the Polkadot currency, DOT, is not only useful as a transaction currency, but it also holds value within the Polkadot network. Although Polkadot at times acts as a middleware, its utility as a currency trumps all else. Polkadot's marketing strategy should focus on these key areas in which it thrives, while also constantly improving its system through its stake-based democracy.

Issues and Roadblocks

Despite Polkadots impressive improvements over existing blockchain technologies, there exist many design flaws: (34)

1. Inflation: Polkadot's consensus mechanism is NPOS, which means that it relies upon its users to offer a stake in exchange for trust in managing the validation protocol of the network. The stake acts as mechanism to deter malicious groups from taking advantage of the validation for personal benefit. However, users require a strong incentive to place at risk a large amount of assets, so there are rewards associated with the stake. This leads to inflation in the network due to the constant generation of new DOT. At present, the inflation rate stands at around 10%, which is comparable to the inflation rates of countries such as Brazil and Turkey which have rapid cost increases. Further, this puts at a disadvantage any passive user who opts not to place their DOT at stake (approximately 50% of the total market capitalization of Polkadot), as they will be losing 10% of their wealth per annum. This is especially problematic when considering that there is a limit to the total number of active users. If Polkadot hopes to be more widely used, it will need to re-evaluate its strategy regarding inflation and Stakeholder rewards.

2. Staking: Because there is such a large risk associated with passive holding of DOT, any large stakeholder is likely to be an active DOT holder. The only way to become an active holder is to become involved in the consensus mechanism, which is to say to assume the role of either a Nominator or Validator. Because there is a minimum DOT stake amount, and because there is a hard cap on the maximum number of validators, only the largest stakeholders are likely to be active holders. There are two main problems that arise from this. One, due to the governance structure of Polkadot, users of the network holding more DOT have more influence on the decisions made by the community and through referenda and elections. This results in the Validators and Nominators having more control and influence over the network, placing passive holders at risk. In the long term, this is problematic, as the passive holders essentially represent the liquid token supply. If the stakeholder minority have more influence on the network than the passive holder majority, then it may lead to undesirable consequences such as high fees and oppression through governance. Second, each Validator may only pay out to a maximum of 256 Nominators (35). Given that the average Staking per Validator is 2 MDOT and each Validator pays out to its maximum number of Nominators, the average stake per Nominator will be around 8000 DOT. (28) This equates to around $230,000 USD, which is likely to be far outside the reasonable investment potential of the average investor. Further, at that price range, the only entities who can afford to place that much DOT at stake are corporations. Thus, there is a high potential for the Validation of the network to be overtaken by a single corporation in the long term. Although in theory, there should be no negative consequence to this – the Validators and Nominators all have invested a stake in the network and are unlikely to act maliciously, as it will mean a total loss of stake. However, it should also be noted that this is antithetical to the goal of Polkadot – a completely decentralized network. Thus, it is highly undesirable for this to occur, even if the network remains honest.

3. Governance: There are currently 12 electable council members in Polkadot. The thirteenth, unelectable member is known as the prime member, who holds the power to cast votes on behalf of the other Council members in the event of an abstained vote. This prime member is none other than Dr. Gavin Wood, the creator of Polkadot. (36) (34) By having a permanent seat on the most powerful position on the Council, Gavin holds the most power in the Polkadot network, akin to a CEO or President. This makes sense, as every democratic system in the past has had a leader, why should Polkadot be any different?

   However, this may be a difficult roadblock to climb, as the stakeholders are powerless to voice their opposition to Dr. Wood in the form of voting. The primary goal of any blockchain is to give an alternative to the centralized fiat currencies which are the current world standard. Having a permanent member of the Council is far from decentralization.

Conclusion

Polkadot poses unique solutions to the problems faced by many of the modern blockchain technologies in modern society, such as a progressive on-chain governance protocol, impressive scalability through the use of Parachains, and excellent interoperability with other chains, both within its network and beyond. However, Polkadot also faces many issues due to its inflation, staking, and governance mechanisms, which may be the cause of friction in the long-term. These mechanisms may cause the blockchain to become too centralized, which is antithetical to both the idea of blockchains, as well as Polkadot's purpose. However, the silver lining is that the Governance system is both on-chain and progressive, meaning that changes can happen. If all goes well, the network will be able to avoid the coming centralization of its network, providing excellent value to its users, investors, and perhaps even society as a whole.

References

1. **What is Polkadot? (DOT).** ***KRAKEN.*** **[Online] https://www.kraken.com/learn/what-is-polkadot-dot.**

2. Solidity. ***Solidity.*** **[Online] https://docs.soliditylang.org/en/v0.8.10/.**

3. Parachains are live! ***PolkaDot.*** **[Online] https://polkadot.network/blog/parachains-are-live-polkadot-launch-is-now-complete/.**

4. Web 1.0 Web 2.0 Web 3.0 with their difference. ***Geeks for Geeks.*** **[Online] https://www.geeksforgeeks.org/web-1-0-web-2-0-and-web-3-0-with-their-difference/.**

5. Dennis Prager. Dennis Prager on YouTube's Record of Censorship. ***Wall Street Journal.*** **[Online] https://www.wsj.com/articles/youtube-censorship-prager-free-speech-big-tech-11628204348.**

6. Jay Peters. Google salvaged Robinhood's 1 star rating by deleting nearly 100,000 negative reviews. ***The Verge.*** **[Online] https://www.theverge.com/2021/1/28/22255245/google-deleting-bad-robinhood-reviews-play-store.**

7. Deltec Bank & Trust. What is Web 3.0. ***Deltec Bank.*** **[Online] https://www.deltecbank.com/2021/08/04/what-is-web-3-0/?locale=en.**

8. Cryptopedia Staff. Polkadot (DOT): Envisioning Web 3.0. ***Gemini.*** **[Online] https://www.gemini.com/cryptopedia/polkadot-crypto-dot-coin.**

9. Polkadot Network. ***The DeFi Standard.*** **[Online] https://www.thedefistandard.com/polkadot-network/.**

10. Learn Architecture. ***Polkadot.*** **[Online] https://wiki.polkadot.network/docs/learn-architecture.**

11. Learn Parachains. ***Polkadot.*** **[Online] https://wiki.polkadot.network/docs/learn-parachains.**

12. Chris Macdonald. 3 Reasons to buy Polkadot. ***Motley Fool.*** **[Online] https://www.fool.com/investing/2021/11/17/3-reasons-to-buy-polkadot/.**

13. Learn Validator. ***Polkadot.*** **[Online] https://wiki.polkadot.network/docs/learn-validator.**

14. Learn Consensus. ***Polkadot.*** **[Online] https://wiki.polkadot.network/docs/learn-consensus.**

15. Joe Petrowski. Polkafot Consensus Part 2 GRANDPA. ***Polkadot.*** **[Online] https://polkadot.network/blog/polkadot-consensus-part-2-grandpa/.**

16. Learn Staking. ***Polkadot.*** **[Online] https://wiki.polkadot.network/docs/learn-staking.**

17. Supporting Decentralization: Join the Polkadot Thousand Validators Programme. ***Polkadot.*** **[Online] https://polkadot.network/blog/supporting-decentralization-join-the-polkadot-thousand-validators-programme/.**

18. Learn Collator. ***Polkadot.*** **[Online] https://wiki.polkadot.network/docs/learn-collator.**

19. Learn Bridges. ***Polkadot.*** **[Online] https://wiki.polkadot.network/docs/learn-bridges.**

20. Join the Council. ***Polkadot.*** **[Online] https://wiki.polkadot.network/docs/maintain-guides-how-to-join-council.**

21. Participate in Democracy. *Polkadot.* [Online] https://wiki.polkadot.network/docs/maintain-guides-democracy.

22. Learn Governance. *Polkadot.* [Online] https://wiki.polkadot.network/docs/learn-governance.

23. Learn Treasury. *Polkadot.* [Online] https://wiki.polkadot.network/docs/learn-treasury.

24. Katelyn Peters. A History of Bitcoin hard Forks. *Investopedia.* [Online] https://www.investopedia.com/tech/history-bitcoin-hard-forks/.

25. What are Bitcoin Forks? *The Balance.* [Online] https://www.thebalance.com/what-is-a-bitcoin-fork-4684459.

26. James Wo. No More Forks: A Case for the Polkadot Approach to Blockchain Upgrades. *NASDAQ.* [Online] https://www.nasdaq.com/articles/no-more-forks%3A-a-case-for-the-polkadot-approach-to-blockchain-upgrades-2021-09-09.

27. DOT. *Polkadot.* [Online] https://wiki.polkadot.network/docs/learn-DOT.

28. Staking. *Polkadot JS.* [Online] https://polkadot.js.org/apps/#/staking/targets.

29. Transaction Fees. *Polkadot.* [Online] https://wiki.polkadot.network/docs/learn-transaction-fees.

30. Jake Frankenfield. Initial Coin Offering (ICO). *Investopedia.* [Online] https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp.

31. Polkadot. *ICODrops.* [Online] https://icodrops.com/polkadot/.

32. The Story Of Polkadot Starts With The 2017 ICO: 2,000% ROI For Early Investors. *CryptoPotato.* [Online] https://cryptopotato.com/the-story-of-polkadot-starts-with-the-2017-ico-2000-roi-for-early-investors/.

33. Wood, Gavin. *POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK.* 2016.

34. Here's Why Polkadot Will Fail? *ProVsCons.* [Online] https://provscons.com/heres-why-polkadot-will-fail/.

35. Nominator. *Polkadot.* [Online] https://wiki.polkadot.network/docs/learn-nominator.

36. Council. *Polkadot JS.* [Online] https://polkadot.js.org/apps/#/council.

37. What is Kusama. *KRAKEN.* [Online] https://www.kraken.com/learn/what-is-kusama-ksm.