POLKADOT FOR BEGINNERS

A non-technical guide to decentralization, blockchains, and Polkadot

gbaci

Polkadot for Beginners: A non-technical guide to decentralization, blockchains, and Polkadot by gbaci

Published by gbaci

Lagos, Nigeria

Edited by AnaelleLTD

First Edition

Acknowledgements

This book was made possible thanks to Polkadot's on-chain treasury, a mechanism that allows the Polkadot community to fund projects and ideas that help foster greater adoption of Polkadot technologies.

First, I would like to thank Raul Romanutti for his help and guidance during the drafting of my treasury proposal.

Thanks are also due to Polkadot Council members who have the thankless task of overseeing and steering the network towards long-lasting stability and growth. Without their dedication, the ecosystem would not have made the progress that has helped it flourish over the past two years.

I would also like to extend my appreciation to Emre Surmeli for his immensely helpful guidance during the technical review of this book's content. Bill Laboon, Head of Education at the Web3 Foundation, was also instrumental in making this book come to life.

I feel indebted to Anaelle LTD for her expert editing skills and insights into blockchain technologies which have made this book so much easier to read.

Finally, I want to thank the Polkadot community members who participated in the making of this book by responding to tweets, polls, and calls for draft reviews. A community is only as strong as the dedication of its members and I'm grateful to be part of an ecosystem filled with committed people who are eager to help each other thrive.

Book Outline

Foreword

Up until the 15th century, European commerce was dominated by the Venetians and Genovese who controlled Mediterranean trade. These traders bought goods from merchants at the port of Alexandria in Egypt–goods which originated mostly from India and were then acquired by Arab merchants who moved them via the Red Sea to Egypt. These goods were then sold in Cairo where they were heavily taxed by the Sultan before reaching the merchants in Alexandria. From there, the Venetians and Genovese distributed said goods all over Europe at very expensive prices. Yet, as in any inefficient system where some benefit at the expense of others, there would be some to challenge this status quo.

At the end of the 15th century, the Portuguese discovered a direct route to India, which allowed them to bypass all these intermediaries in time and enabled them to transport their products at a fraction of what continental Europeans were required to pay. This led to a radical change in how the old world operated, and within a few years, Venezia and Genoa were no longer relevant players in trading with the East.

Think of blockchain technology as "the Portuguese discovery of the direct route to India". The main idea being that, in order to disrupt the "old world", certain infrastructure needs to be in place. In the above example, not much could be done in the first years of the discovery until ports were secured, contacts were made, and suppliers were established. The implementation of this infrastructure was the final blow that destroyed the Venetians and set up a whole new way of doing commerce and trade.

Today, the infrastructure that is needed for blockchain to take off and cement disruption has been built. Different industries have started to converge – gaming and crypto, identity and crypto, finance and crypto, just to name just a few. When this intertwining of industries occurs, magic happens, and we can only speculate on the kind of innovations

it will birth. The future is exciting, and it is becoming clear that blockchain projects will need to communicate and interoperate with other projects as well as with other actors outside the crypto world.

As it stands, the world is no longer dominated by a single blockchain. We have entered the multi-chain era, and this is where Polkadot will play a major role, as you will learn throughout this book.

In traditional finance, there has been a somewhat arrogant attitude towards Bitcoin and all its ramifications which prevented many (including me) from seeing the benefits of blockchain technology in its earliest stages. Luckily, this attitude is changing. Traditional finance has many challenges that it has yet to surmount, despite having a persistently negative impact on the global financial and economic system. Banking, within traditional finance, for example, runs a system of incentives that is not aligned with other market participants. Bankers, having been one of them, are short-sighted, focused on end-of-year bonuses, and are not accountable for their actions. This setup has led to less-than-acceptable banking practices, as the world saw during the Great Financial Crisis where greed drove the sale of investment products that were priced as safe but were in fact extremely risky. Investment recommendations are not made based on what benefits investors, but on the amount of fees that are generated and on the data stored within centralized entities.

When I started studying blockchain technology, I began to discover that decentralized and “permissionless” networks address the problems of trust and security in such a way that we no longer have to rely on corporations alone. I learned that the incentives incorporated into blockchain protocols ensure that economic interests are aligned and that participants can be held accountable. Those who want to use a network, make proposals on governance, or earn by helping secure a network must own tokens of said projects. This ultimately leads to good behavior and compliance, as otherwise, participants would risk losing their capital.

It took me a while to understand Bitcoin and its unique characteristics as a new member of the monetary world, and appreciate how its emergence complements the way we transact with money. First, I learned about the Bitcoin blockchain, a protocol whose function is to record transactions of bitcoins. Then I learned about Ethereum, a "programmable" blockchain whose protocol enables building applications and smart contracts on top of it to record transactions on-chain. Think of Ethereum as a smart phone where you can download and run applications, while the Bitcoin blockchain is a landline phone exclusively used to make and receive calls.

Ethereum opened Pandora's Box in terms of what could be done with blockchain technology. As traffic on the Ethereum blockchain exploded, its drawbacks started to emerge. Some of them are well known: high gas fees and slow transactions; however, some are not that intuitive. The Ethereum blockchain was not designed to be updated too frequently, so, when upgrades are needed, they are extremely difficult and lengthy to implement. Another drawback is that the Ethereum blockchain was not built to communicate with other chains, as its original design did not consider the question of interoperability. It is those problems that gave birth to Polkadot.

Polkadot enables independent blockchains called "parachains" to connect to it, essentially handling the connectivity and security for them. Polkadot can change its own design over time and allows interoperability among different chains. Polkadot makes the entire blockchain space much more scalable and enhances network effects, it is essentially like a railway connecting cities and enabling economic activity to flourish.

Due to the speed of innovation in the blockchain space, and owing to the fact that I am not a computer scientist or developer myself, it's been difficult to identify which blockchain projects will make a difference. In the Portuguese example we saw earlier on, if you were in Lisbon and learned about the discovery, you could have invested in a single ship and brought spices for your own personal business. That

would have been extremely risky, as not many ships made it back safely in those days. Imagine a better investment such as a ship factory, where you benefit not only through the sale of the ships you build, but also through potential royalties from successful expeditions.

I think of Polkadot exactly like that. Polkadot requires independent blockchains to win an auction and lease a slot, so that they can be connected to the Polkadot infrastructure and become a parachain. This means that projects can focus on their use cases and let Polkadot take care of the security and connectivity. Supporters of those parachain candidates can lend DOTs–the native token of Polkadot–to projects and get rewarded in the projects 'own cryptocurrency if a parachain slot is won. This system warrants projects maintaining their quality, their relevance to end users, and the support of their community in order to continue deploying on Polkadot after their slot leases end. This extraordinary set-up will ensure that the Polkadot ecosystem always gets the best projects and remains at the vanguard of innovation. This is why I think Polkadot will play an essential role in the blockchain space.

Never before has the world had millions of incredibly smart people working simultaneously on open-source protocols, which has led to a Cambrian explosion in the uses of blockchain. We are just getting started, and it is simply a wonderful time to be alive. Maybe after reading **gbaci's** book you will agree with me that investing in Bitcoin is investing in price, investing in blockchain is investing in innovation, and investing in Polkadot is investing in the railway system that will carry a lot of that innovation forward.

Jean Philippe Tissot

Founder and Portfolio Manager of Arauca Capital

A Brief Introduction

Since its launch on 26th May 2020, Polkadot has captured the imagination of a wide variety of people who share similar values about the future of human organization. Polkadot is a blockchain whose main purpose is to connect other blockchains. Given that few people understand what a blockchain is, it is only natural that they would think Polkadot's objective idea of a blockchain that connects other blockchains is akin to gibberish. Thus, trying to understand what Polkadot is and how it works is an arduous intellectual endeavor. Or at least, it used to be.

This book was written with the sole purpose of simplifying the immense complexity of Polkadot so that the average reader can understand this ecosystem without any prior technical knowledge of blockchains or computer networks. To achieve this, a great deal of technicality has been scrubbed out of the presentation of many concepts. And so, though this book is ideal for the average reader, it may not be so for a technically savvy person. That said, there is still a lot to learn about Polkadot that doesn't fall within the scope of technicalities—governance, crowdloans, and parachain auctions to name a few.

The hope of this writer is that the reader will become as fascinated and as inspired as he was when he first read the Polkadot whitepaper, a document that laid out a bold vision for blockchain technology and the decentralized web (aka web 3.0), proposing to solve the problem of scalability (for maximum adoption), shared security (for maximum diversification), and interoperability (for maximum innovation and

useability). The Polkadot whitepaper made it clear that its goal was to enable mass adoption through digital ownership and freedom for the individual by building as many different kinds of blockchains as possible, each dedicated to a different industry in need of a revolution.

But I am putting the cart before the horse. An explanation of what Polkadot is and how it does what it does will come later. First, we shall begin with the why of it all. I have found that the easiest way to understand a new technology is to understand the philosophy that powered its creation. Thus, we'll start with the philosophy of decentralization.

The Philosophy of Decentralization

My purpose in this chapter is to explain why decentralization is necessary. Why go through this first? Because there seems to be some misunderstanding amongst people who are called to the decentralized world. Many come for profits, believing that this is all the industry is about.

Of course, there are many builders in the space who are only focused on growing their stock in life, and this isn't at all bad. I mean, everyone is free to do what they want. But let's not forget that Bitcoin, sitting at a hefty $600+ billion market capitalization, was a reaction against the tyranny and callousness of the financial elite. Vitalik Buterin, the originator of Ethereum, was driven to create Ethereum because of the tyranny of conglomerates. In a famous anecdote, he recalled crying himself to sleep when the famous World of Warcraft game unilaterally seized all his in-game possessions.

Both instances were about *freedom for the individual*. Was there money involved? Sure. Was financial profit the end goal? No. The point was always to lead humanity to a better place—greater individual freedom. If decentralization ever loses sight of this end goal, then it will spiral out of control, something closer to an undefeatable hydra.

Lessons from our Ancestors: The Necessity of Centralization

The terms centralization and decentralization refer to different ways of managing power, ownership, and authority. Power, ownership, and authority are directly related to security because:

1. He who owns is responsible for the security of what he owns.

2. He who owns has power and authority over what he owns.

In a centralized system, all three attributes (power, ownership, and authority) flow to and are issued from a center—King, Council, Government, CEO, Management, etc. In this manner, the government is a central agent organizing national affairs, while the company is a central agent organizing business affairs. This centralized mode of organization has served us well for centuries because it was the most effective method we had for coming together to build civilizations. But this was not always the case. Centralization, as we have come to know it, began with the invention of farming.

Before farming, our hunter-gatherer ancestors weren't stationed in one place, nor did they own many things; and so they naturally didn't need to bother about security the way we currently do. Their mode of governance was more decentralized, so that the tribe would collectively decide what to do and where to go. But upon finding the benefits of farming, our hunter-gatherer ancestors abandoned their nomadic lifestyle for a sedentary one.

From then on, people had farmlands, houses, and villages with clear borders drawn. With a more stable food supply came the explosion of the population, which brought new problems to light.

For one thing, our ancestors had a lot of decisions to make. How were they to share the land? Who would resolve disputes? Who would lead in times of war—for self-defence and for conquest? Imagine a band of soldiers from a rival kingdom coming to conquer a kingdom of 5,000 inhabitants. If the invaded kingdom were to rely on a decentralized model of organization, then it would need to deliberate at length before coming to a conclusion. By then, the kingdom would have certainly been captured by the invaders.

Thus, a new mode of organization was needed to match our newfound prosperity and lifestyle. Then began the popularization of centralization as our de facto organizing principle.

Centralization was largely made possible thanks to specialization—wherein all members of the tribe didn't need to become farmers anymore. Thanks to a stable food supply, people could specialize according to their talents and the available tasks. Our ancestors figured out that if some people were tasked with leading—arguing about the right way forward and making decisions—the community would become more efficient at using its resources and resolving issues.

Understand what was really happening here. The community decided to concede its power, ownership, and authority to a center (King, Council, etc.) for the sake of greater efficiency. This evolution was described by Thomas Hobbes in *Leviathan (1651)*. According to Hobbes, an almighty organization comes to life when its individual members renounce their right to live by the laws of nature (aka "each for himself"), hand all their powers over to the sovereign (central agent)—which is created as a result of this act—and promise to obey thenceforth the laws made by the sovereign.

This mode of organization has served us well for centuries: it helped bootstrap civilizations and elevated them to their current status.

Depressions, Censorship, and Protests: The Dark Side of Centralization

> The collapse of the US housing market in 2007, which no regulators had predicted, was caused by widespread illusions of safety in abstract investments, which hardly anyone understood. The system remains as complex now as it was then and a similar crisis could happen again. Maybe tomorrow.
>
> — Hans Rosling, Factfulness

As we all know, everything has a dark side. In the case of centralization, we have been exposed to its darkest aspects, assuming each time that things could never get worse. But reality has proved us wrong.

In 2008, the global economy was dragged into the Great Financial Crisis by the actions of a few bankers in America. Think about that for a second. The whole world experienced pain and heartache because of a few humans who, in the end, got paid large salaries for their greed and incompetence.

The real problem with the crisis was that the bankers had no skin in the game. They were playing with other people's money, and when they lost it, there were no major consequences for them, but the rest of the world had to pay. This was a failure of incentive design in the traditional finance world, which is also why the new Web3 movement is a welcome evolution. If decentralized finance protocols were to lose money for any reason, there would be no government to bail them out.

I have personally experienced the dark side of centralization during the EndSARS protests in Nigeria. The Nigerian government, abusing its power, forced the banks to block the accounts of people who were helping and facilitating the peaceful protests (I can testify that these were peaceful protests because I followed it all). It took Bitcoin and Ethereum to sustain the movement for an extra week, before the government repressed the demonstrations in the most depressing way imaginable. It sent the army to the Lekki Tollgate in Lagos where soldiers shot live rounds at the protesters, injuring and killing citizens who only wanted a better life. Till today, thinking about this brings tears to my eyes. That a government can unleash the army on innocent citizens is the highest abuse of centralized power. The bitter irony here is that the protests were aimed at ending police brutality being dished out to young Nigerians by the rogue police unit called SARS. Here is a CNN report on the tragedy.

I could also take the case of Facebook, Google, and other web products and services we use as examples of centralization gone wrong. The current web is structured in a way that encourages greater levels of centralization over time. Google is so valuable to advertisers because of the data that Google can access but doesn't actually own.

Same goes for Instagram and other social media apps we use. Without user data, they would be worth far less than they currently are. These companies have specialized in taking our data to grow billion dollar empires without ever paying a dime to us, the actual owners. Even worse, they can (and do) censor us whenever they want. This is the reality we live in and have grown to accept because we did not have any real alternative until Bitcoin came along. But we will get to Bitcoin in a moment.

To further understand the dark side of centralization, we need to explore the trinity—ownership, power, and authority.

Ownership refers to who owns an item. In the case of a country, the land belongs to the government, except in cases where citizens have acquired these lands. But even in those cases, governments still reserves the right to confiscate said lands.

Power refers to the ability to take action. Again, in a country, power is distributed across the society, with the larger share belonging to the government (split into hierarchies). Thus, the president has more power than the Vice President because he has the ability to do more than the Vice President. The citizens have power because they can vote and protest.

Authority refers to the ability to control. Naturally, one who has ownership and power also has authority by default. In the current social media space, you don't own anything, not even your account. This is why you can be blocked or suspended. You also don't have much power over anything other than to leave if you don't like how things are going. And finally, you have no authority to tell the company what to do, except in a case where a large number of community members agree with you (because companies like to bend to the will of the majority). This is the present state of affairs even with your bank account. Banks can freeze your accounts for any reason, especially if the government asks them to.

This isn't to say that it is bad for the government or banks to have these powers because the truth is that sometimes this power is put to good use. But more often than not, power is abused. It is just the nature of power– ifif it is too great, it will corrupt. This is one major problem with centralization. It encourages the accumulation of a great deal of power in the hands of a few people. Naturally, this creates god complexes in some individuals, turning them into tyrants (where 'tyrant 'isn't reserved for only rogue heads of state).

Thus, the imperative to abandon centralization is manifold:

1. History has proven to some degree that too much power corrupts.
2. Centralization creates single points of failure, making it easy to take over a system. A perfect illustration of this is the story of Atahuallpa.

> Atahuallpa was absolute monarch of the largest and most advanced state in the New World, while Pizarro represented the Holy Roman Emperor Charles V (also known as King Charles I of Spain), monarch of the most powerful state in Europe. Pizarro, leading a ragtag group of 168 Spanish soldiers, was in unfamiliar terrain, ignorant of the local inhabitants, completely out of touch with the nearest Spaniards (1,000 miles to the north in Panama) and far beyond the reach of timely reinforcements.
> Atahuallpa was in the middle of his own empire of millions of subjects and immediately surrounded by his army of 80,000 soldiers, recently victorious in a war with other Indians. Nevertheless, Pizarro captured Atahuallpa within a few minutes after the two leaders first set eyes on each other. Pizarro proceeded to hold his prisoner for eight months, while extracting history ́s largest ransom in return for a promise to free him. After the ransom—enough gold to fill a room 22 feet long by 17 feet wide to a height of over 8 feet—was delivered, Pizarro reneged on his promise and executed Atahuallpa.
> Atahuallpa ́s capture was decisive for the European conquest of the Inca Empire.
> Although the Spaniards ́superior weapons would have assured an ultimate Spanish victory in any case, the capture made the conquest quicker and infinitely easier. Atahuallpa was revered by the Incas as a sun god and exercised absolute authority over his subjects, who

> obeyed even the orders he issued from captivity. The months until his death gave Pizarro time to dispatch exploring parties unmolested to other parts of the Inca Empire, and to send for reinforcements from Panama. When fighting between Spaniards and Incas finally did commence after Atahuallpa´s execution, the Spanish forces were more formidable.
>
> — Jared Diamond; Guns, Germs, and Steel

3. Centralization encourages people to abdicate their power and responsibility, inevitably leading to decision-making that marginalizes many in the community.
4. Centralization creates asymmetries in ownership, power, and authority, putting the fates of the many in the hands of the few.

The Only Solution?

One solution to the pitfalls of centralization is decentralization. Perhaps not the only solution, but it is the best option we currently have. Decentralization, at its core, is concerned with the redistribution of power and authority from a few in the center to the community at large. In such a system, not one person or group rules over the system: risks, responsibilities, and rewards are shared by everyone. Thus, decentralization's greatest appeal is fairness. It is far better to know that we went down because of our collective action rather than the actions of a few. It is better to know that no one can be silenced for speaking out against injustice, cruelty, corruption, bigotry, etc. It is better to know that everyone is financially free to transact with whoever, wherever, and whenever.

The philosophy of decentralization is the breakup of centralized power structures. The natural consequence of such a philosophy is greater freedom. The nature and kind of freedom, however, is dependent on which decentralized system we are talking about. Bitcoin was created with the goal of financial freedom, to give people the option to free themselves from an economic machine they were deeply unsatisfied with. Ethereum wanted to offer developers the

freedom to build apps that could change the world—going on to spur the rise of decentralized finance (which has given many people the freedom to do what bankers do) and NFTs (which has given creators a path to artistic freedom unlike anything the art industry has seen in decades). These are just the first two flagship use-cases. It is fully expected that within the next ten years, more decentralized products will make it to market, offering alternatives to current systems.

In summary, the advantages of decentralization are:

1. Greater security because the system cannot be hijacked from the center. For example, if Google is hacked, the hacker will gain access to all the information Google has. If the president's mind has been hijacked by dark agents (or aliens), the nation won't fall to his newfound foolishness because the system has many heads.
2. Greater fairness because more people are involved in decision-making. A community that only acts of on key issues when a majority approves such action is more in line with the ideal that everyone is equal. If only a few people make decisions for the community, it won't be long before the few decide to favor their own interests and take advantage of the community.
3. Better distribution of ownership. A few people should not own everything because that runs counter to the design of life. The lion doesn't own the jungle even though it could kill almost every animal in it. If ownership isn't shared, then growth and progress only benefit a few, and that is a sad state of affairs that fosters greater inequality.

In the next chapter, we will explore how we can achieve decentralization.

The How of Decentralization

> We lose thousands of nerve cells every hour, but it has virtually no effect because of the highly distributed nature of all of our mental processes. None of our individual brain cells is all that important—there is no Chief Executive Officer neuron.
>
> — Ray Kurzweil; The Age of Spiritual Machines

Having understood the necessity, purpose, and advantages of decentralization, we will now explore how we can achieve decentralization in practice.

In the past, it was relatively impossible to get many human beings to work together towards a greater goal in a decentralized manner. As previously explained, each attempt at organization towards a great goal was facilitated by centralization. But why is it so?

Well, the biggest problem we face when trying to get many people to work together is the question of trust. This is why centralization has been the dominant organizational model over the past centuries. Centralization circumvented the issue of trust by giving everyone a central party to trust. This is how banks work: their primary purpose is to help us keep track of who has what and who can send what. This is also partly why governments exist: to help us determine who can and should do what. We trust banks to keep our money safe, governments to keep us safe and facilitate prosperity, and social media companies to provide us a service. Thus, when it comes to decentralization, the question becomes: how can you get as many people as possible to trust each other?

The short answer is: you can't. Trust is about keeping track of information in a secure way so that no one can question its validity. The centralized solution has been to delegate trust to one entity, either via power, authority, or ownership. But this poses a few risks:

1. Centralization creates an asymmetry of information that some centralized controllers use to their advantage at the expenses of many stakeholders. This is the case, for example, when a businessman gets to hear of a government decision before everyone else because he is friends with a few senators and can take advantage of his position. Bankers and businesses collude all the time, the same way governments and banks work together. In short, individuals in positions of power are incentivized to scheme and put their own interests ahead of the collective good.
2. Centralized information gathering and verification presents a single point of failure. This can manifest in different ways. On the one hand, the centralized servers (computers where the information is stored—bank records, government records, user data, etc.) can be hacked. Because the hacker only has to focus on one attack vector, there is an incentive to break in and steal data. On the other hand, if anything were to ever happen to this one source of information, then it would be lost forever.

So how do we overcome our trust issues and achieve decentralization?

Skin in the Game

First, we need to recognize that the real problem is in the misalignment of risk and incentives between participants. Our current systems, democracy included, allow people with no skin in the game to make decisions that benefit themselves and harm others. Thus, when the 2008 banking crisis occurred, it wasn't because the banking elite were intentionally cruel; rather, the system allowed their

callousness and greed to affect the global economy. However, if their mistakes had yielded negative consequences for their own money, then maybe they would have done their due diligence before entering a stinky housing market. "Skin in the Game" means responsibility for one's own actions and their consequences: if you mishandle and lose your money, you will have to pay for this loss. Furthermore, you should not have the opportunity to play with and wipe out other people's funds through bad decision making yet earn support from government bailouts. That is unfair on multiple accounts.

So, how do we achieve some semblance of skin in the game at scale? Enter the blockchain and all its adjacent technologies.

What is a Blockchain?

A blockchain is a database (an organized collection of data). But it is different from the databases we are accustomed to with Web2 applications (Facebook, Instagram, and Google to name a few), most of which are permissioned, centralized databases controlled by a single authority. The data on the blockchain has some unique properties that makes it different from those traditional databases:

1. It is hosted by a public, decentralized, peer-to-peer network of computers.
2. It is secured by cryptography and a consensus protocol that is designed to make it difficult to take over but easy for the computers to stay synchronized.
3. It is immutable, meaning that you cannot update or delete existing data records without getting majority approval from the nodes on the network. Thus, although it is possible to delete and manipulate data on a blockchain, it is only possible when the majority agree to do so.

With these unique properties, the blockchain database becomes super useful for applications that require social consensus to be valid, like governance and currencies.

Another way to think of a blockchain is as a network of nodes (computers, servers, etc.) that work together with no central authority recording and verifying data. This data can be anything–transactions, account balances, and network states–stored on a ledger that every member of the network is free to access.

To build this decentralized database called blockchain, different pseudonymous stakeholders must work together. But how do you get people who don't know each other to trust each other without the supervision of a central authority? Well, you take trust out of the equation. Phrased another way, you automate trust in such a way that network participants don't need to trust each other but rather, the protocol.

What is a Protocol?

A protocol is simply a set of instructions from which a computer software operates. Think HTTP, or TCP/UDP and IP. Think the *Ten Commandments* or the *Hammurabi code*.

A protocol sets the rules of engagement for all participants in a network such that new entrants can freely choose to be a part of or leave the network. Most importantly, the protocol cannot be altered by any single participant or group of participants. Any updates can only be carried out when a majority of the network participants agree to this change. Notice that this is distinctly different from a country or company where changes are made in a top-down manner.

Thus, blockchains give every network participant the freedom of choice to join or leave the network and also the responsibility to manage the network. Collective ownership and leadership is the name of the game. However, not all blockchains follow this ethos.

It is possible to trust a protocol because its rules are clear from the beginning. In the case of Bitcoin for example, the protocol states that a block (more on this in a bit) will only be produced when a cryptographic puzzle has been solved and verified by a majority of

nodes (computers) on the network. In simpler terms, no new transaction will be added to the ledger unless a majority of nodes agree that the transactions are valid. At the creation of this new block, new BTC will be created (minted) as a reward. In summary, that is what the Bitcoin protocol is.

So how do Blockchains actually Work?

Blockchains are constantly referred to as a global ledger, and this is true. But saying the blockchain is a ledger can be sometimes misleading in an imaginative sense because there is no ledger-like table for any non-technical person to look at. The term ledger is used only to draw a similarity between a computer process and a human process. Thus, the blockchain is a ledger because it stores information, not because it's an actual ledger for bookkeeping. However, it's helpful to keep this comparison because it perfectly describes what a blockchain does. From now on, I will focus on proposing a better explanation of how this ledger is constructed.

To understand a blockchain, we need to break the word blockchain into its possible constituents.

Blockchain = blocks on a chain

OR

Blockchain = blocks + chain.

But what is a Block?

A block is a collection of verified information packaged together and ready to be added to the global ledger. A block is rarely made of a single transaction, but consists of many transactions bundled together. To create a block, valid transactions that have taken place on the network (i.e sending tokens, changing names on a decentralized social media site, swapping tokens or posting a comment) are compiled and locked together using cryptography. Cryptography is a discipline (just like biology, chemistry, physics, etc.)

that is focused on creating strong security by using difficult-to-crack puzzles based on provable mathematics. The purpose of sealing blocks using cryptography is to avoid future tampering.

You can imagine a block as a bucket. Every block starts out as an empty bucket, then end-users make use of the network, filling the bucket with their transactions. When the bucket is full, it is sealed and kept away for future reference. Now, it's important to realize that the sealing of the block is only possible when many people (nodes) agree that the transactions in the block are valid. As in, when it is confirmed that no one has tried to send tokens they are are not in possession of or other fraudulent actions. Once sealed, a block can't be opened to change any transaction, but it can be used as a reference to verify data records.

So when does the Chain Come In?

Well, there are bound to be multiple blocks, right? Since each block can only contain a finite number of transactions. Thus, chaining the blocks becomes necessary in order to decipher and track the sequence of transactions—i.e. which blocks come first. The process of chaining isn't so different from block creation itself. I only artificially split my explanation so that you could get a better understanding of the process. In reality, each new block grows the chain and, in the case of a Proof-of-Work blockchain, makes it more secure.

But, on a deeper level, how does a blockchain achieve this level of decentralized security? Different blockchains go about it differently. But despite their differences, there are really two main issues to consider in analyzing blockchains.

For a blockchain to do what it does, it needs many computers talking to each other constantly. This is called networking, or if you prefer the more human term, gossiping. This is how data is transmitted across the network. In short, data is copied from one computer to another until all the computers on the network have this data. Without networking, there would be no blockchains as we know it.

The second main component of a blockchain is its consensus mechanism—aka, how the different network participants (nodes, computers, servers) come to a conclusion on which data is valid and which is false. A consensus mechanism has two main aspects to it:

- Consensus - the process of copying and verifying data (blocks) from one node to another.
- Finality - the process of adding the new block to the chain. The difference between the two will be made much clearer below.

Naturally, every blockchain has its unique consensus mechanism, unless a new blockchain was created using the code (protocol) of another blockchain. However, all the different consensus systems can be classified into three main categories.

Proof-of-Work (PoW)

Proof-of-Work is an algorithm that was created to avoid email spam, essentially making it difficult for computers to maliciously overload email servers. To achieve this, the email server would give the sending IP a small puzzle to solve that would take some arbitrary computational effort. When done, the computer would present the solution, which was the proof of the work that it did, along with the email body. This process was adopted by the Bitcoin client and repurposed to be used as a consensus mechanism.

With PoW, computers come to consensus only when work–in this case, solving a cryptographic puzzle–has been done. Whoever provides a solution to the cryptographic puzzle first becomes the producer of the block and gets rewarded for it. This consensus method has come under fire lately for its energy-intensive operations. In such a network, the security of a system is somewhat tied to how difficult the cryptographic puzzle is, thus requiring more energy overtime.

Proof-of-Stake (PoS)

This method of consensus was invented to overcome the shortcomings of PoW in terms of energy consumption. It trades computer work and cryptographic puzzles for economic interests, so that the security of a system is tied to how many tokens are staked in the network. This is where the whole idea of staking (more on this later) came from. The logic is simply that if a system is backed by great economic power, then it will be near impossible to hijack said system because anyone looking to do so will incur even greater cost.. For example, a PoS blockchain that has only $2 million in stake is far easier to hijack than a network with $1 billion in stake.

Hybrid Consensus

Most modern blockchains use a hybrid consensus that combines proof-of-work with proof-of-stake, taking the best of both worlds to create a more secure and energy-efficient network. With hybrid consensus systems, the slight difference between consensus and finality becomes somewhat obvious.

Before a block is added to the chain, it needs to be verified by many miners (or validators). This process of ongoing verification, which includes copying the data from one node to another, is called consensus. When enough verifications have been made, as specified by the protocol rules, then the most 'supported 'block is finalized i.e. added to the blockchain. By separating the two processes, developers can better optimize the blockchain for speed, security, and scalability.

Who are Blockchain Participants?

Full Nodes: These are the people responsible for the security of the network. You can think of them as security personnel. Depending on the blockchain, they could be called different names —miners (Bitcoin and Ethereum), validators (Polkadot, Cosmos), and more. Regardless of their name, their purpose is the same—to secure the network. They

do this by recording and verifying transactions in a decentralized manner.

Builders (Decentralized Apps and Blockchains): The builders are similar to the founders in the current Web 2.0 world. They are mostly programmers who create decentralized applications or newer blockchains to work with.

Light Nodes (End Users, Wallets, and Clients): Many people in this category will never need to know about how blockchains work in order to use them. In fact, the goal of current blockchain innovation is to get the end-user to interact with blockchains without ever realizing it. These are people who use the dApps and services created by the builders.

If the concept of blockchains still seems like a concept, then worry not. We will now explore the history of blockchains, and hopefully you will get more context, and thus, better understanding.

The Evolution of Blockchains

First Came Bitcoin

In the old system, if you needed to send money to a friend, you had to go to the bank and ask the officers to send money on your behalf. If you were living in rural parts of the world, the nature of your obstacles would not only be financial but also physical.

This meant a few significant things: you didn't have full control of your money, and the bank was free to loan your money out and earn interest on it without any rewards for you. Furthermore, they could lose this money through reckless speculation and never be accountable for doing so. Crazy, right? This had been the case for a long time until Bitcoin changed the game in unexpected ways.

With Bitcoin, for the first time, people could send value digitally to anybody anywhere in the world, with no middleman asking them for documents or high fees.

With Bitcoin, all you had to pay was a little transaction fee to the protocol to make your transfer. If the transfer failed, you would receive a refund. There was no longer any need for middlemen. This network could grow and replace the traditional banking system.

There are three ways to think of Bitcoin:

1. A system/protocol for transferring digital value.
2. Digital gold.
3. As an investment.

Since Bitcoin has become one of the highest performing assets of recent times, most people prefer to see it as an investment rather than "digital cash", as it was originally intended.

Then Along Came Ethereum

In a bid to expand the functionalities of the network over the years, the Bitcoin community tried to create 'colored coins', which were tokens built on, around, or as a copy of Bitcoin to represent different assets and ideas. However, the platforms were not working as intended and couldn't get past the limitations of the Bitcoin code.

Vitalik Buterin studied Bitcoin for a few years and thought, "What if we made this technology more generalized?"

Spurred by this idea, Vitalik wrote the Ethereum whitepaper in 2014, laying the framework for a general-purpose blockchain on which developers could build and design custom tokens. To pay for the computation that would be necessary to run their code, developers would use a native token called Ether (ETH).

Essentially, Ethereum was conceptualized as a global supercomputer running on a blockchain as its database. Taking the basic structure of a blockchain, Ethereum built a platform that allowed for more flexibility of use cases. Think of Ethereum as an open internet platform that allows any kind of website/app to be created, while Bitcoin is an open-internet platform entirely populated with a single website/app.

Thus, from Ethereum's rise sprung a new component of the blockchain ecosystem: decentralized applications (dApps).

Before we move on to the cross-chains, it is crucial that we explore smart contracts for a bit.

A Little Bit About Smart Contracts

Although they became popular through Ethereum, Smart Contracts were invented in 1994 by Nick Szabo. Just like blockchains give various network participants the tools they need to work together without the need to trust each other, smart contracts provide a mechanism for facilitating trust amongst different economic actors. How is that different from a blockchain? A blockchain is a set of rules on how a network will operate, while a smart contract is a set of rules on how transactions will be executed.

To better understand smart contracts, let's look into insurance policies. In a typical insurance contract setup, the claimant needs to provide proof to the insurer that their claim is valid, which can create friction. Say you took a car insurance and your car was totalled through no fault of yours. The insurance company can either pay out the insurance as agreed or delay under the pretence of investigating the matter. Sometimes, these investigations take months, during which you have to resort to public transportion. This is not to say that investigations aren't necessary; but to drive the point of smart contracts across, we are assuming that the insurance company is acting in bad faith. With a smart contract, this won't be the case.

A smart contract is a self-executing program that runs whenever a set of predefined parameters are met. Thus, in our insurance example, here's how things could proceed under a smart contract-based agreement. First, when your car gets totalled, a sensor in the car sends this information to the smart contract. Once the smart contract confirms the data, perhaps by mapping the data to news reports from the area, it will automatically pay out your insurance claim without waiting on any further permissions from the insurance company.

Let's apply this process to financial operations. It is possible to single-handedly run a decentralized lending and borrowing platform through the power of smart contracts because participants can trust the contract without trusting other participants. Thus, a liquidity provider–someone who provides money for others to borrow–is encouraged to deposit his tokens for other users to borrow because he is guaranteed that whenever he chooses to withdraw his liquidity (tokens), the smart contract will release it along with all rewards that are due him. Similarly, the borrower can trust that the smart contract will not change the terms of the transaction (interest rates and/or penalty fees), and that his collateral will be returned to him once he repays the loan.

Now there's one big caveat. A smart contract is only as secure as the code that makes it. Many hacks leading to loss of funds have been carried out in the Web 3.0 space due to faulty smart contracts. Thus, before interacting with a smart contract, it is advisable that you review the code, if you're technically knowledgeable, or check that the smart contract's code has been audited.

One more thing to keep in mind is that a smart contract can be used in a variety of industries and for a variety of purposes so long as the end goal remains to facilitate trust amongst different economic actors through uninterrupted execution. For example, a smart contract between a supplier and a retailer would pay out funds to the supplier only when it confirms that goods have been supplied to the retailer's warehouse/store.

In the long run, smart contracts development will increasingly rely on well-written code (developers), well-incentivized economics (economists), and law abiding functionalities (lawyers). Hence, to develop smart contracts and make them smarter, we will need to take a multidisciplinary approach.

With this matter examined, we can now turn our sights to the cross-chains.

Rise of the Cross-chains

Following the smashing success of Ethereum–where success means adoption by more people–multiple layer-1 blockchains were created. But what does it mean to be a layer-1 protocol? Until now, it wasn't important to make this distinction clear, but as we are inching closer to presenting Polkadot, it's important to understand what layers represent.

A layer-1 blockchain is similar to a country with sealed borders. Within this country, information can flow between all participants without the need for trust. Why? Because it already operates with a constitution that's not open to misinterpretation but instantly executed. With Ethereum's introduction of smart contracts, a layer-1 (country) can have multiple sub-protocols (states), each communicating with each other seamlessly. But because of its sealed borders, this layer-1 cannot have direct connection to the outside world.

A common misconception amongst some early blockchain adopters is that a single layer-1 blockchain will be all that is ever needed for the blockchain industry to fulfil its mission. This view of the industry is often perpetuated by those who have a maximalist approach to blockchain adoption. Therefore, it won't be uncommon to find people who are of the opinion that anything asides Bitcoin is a scam that is not truly decentralized. Others will sing the praises of Ethereum, claiming that it is far better than Bitcoin, and that other blockchains are redundant. Most of these people are either misinformed or are solely concerned with making money on whichever tokens they are holding.

The truth is that the blockchain industry is poised for a multi-chain future, and each new blockchain will bring something new to the table that can be leveraged by existing blockchains. Thus, if there's a blockchain focused on decentralizing finance, and another focused on decentralizing identity, they would be more effective while working together than a general-purpose blockchain. Explaining this concept

in detail would require diving into technical explanations, and so I will skip it for now. The point is that there is no such thing as one blockchain to rule them all, which would be like implying that there is an online company that rules the internet.

If the reality is a multi-chain universe, and layer-1s are insulated countries, how do we connect these sealed-off countries? There are many possible solutions to this problem.

The first, pursued by Cosmos, is to give every layer-1 the same networking constitution, so that exchanging information between chains is made easier via a specialized bridge. In this context, a bridge literally means a gateway to another country. This approach definitely solves the problem of connecting chains, but it is not the most optimal setup even when compared to Ethereum.

On Ethereum, smart contracts can interact with each other in two distinct ways:

1. Send and receive tokens - Smart contracts can exchange tokens without any formal verification.
2. Give instructions - A smart contract can ask another smart contract to carry out a transaction. This is the real magic of composability, whereby different smart contracts

can be used in a single transaction or application and communicate without human intervention.

Within Cosmos's inter-chain communication protocol, the only information that can be transferred are tokens. Thus, blockchains can't instruct each other to take certain actions. As such, you can think of this level of communication as somewhat primitive (low-level composability). To reach higher levels of composability, similar to what smart contracts enjoy, a lower layer is required. Enter Polkadot.

Polkadot is a Layer-0 protocol that seeks to connect multiple layer-1 blockchains without breaking high-level composability. In this setup,

blockchains are able to connect with each other to send tokens and change each other's state.

Polkadot respects the unique state transition functions of Layer 1s, and does not require them to adhere to the Relay Chain's state change function. It just requires proof of validity of the state change that a Layer 1 might be implementing. Said differently, Polkadot the layer-0 (planet) takes into account the laws of any layer-1 (country) that connects to it. All it requires is the proof that these laws or changes are valid. This is the setup that gives parachains the freedom to develop their own consensus and finality mechanisms.

What does "state change" actually mean? Let's take a look at an example. A layer-1 blockchain focused on decentralizing finance can change the state of another layer-1 focused on decentralizing identity by requesting for the user information stored on the identity chain. The state is changed because the identity chain needs to carry out a new transaction to fulfil this request. Although no tokens were exchanged, greater value has been provided because the information provided by the identity chain can potentially be used by the finance chain to make payments to the user. This is just one example out of many which lay at the core of the disruption brought by blockchain technologies.

But before I address the disruptive nature of blockchains, let's go over one more layer in our multi-chain world: layer-2. Layer-2 blockchains were created to scale layer-1 blockchains i.e. increase the speed or expand the capacity of said blockchains. Ethereum, for instance, has at least three layer-2 protocols working on helping it scale—Polygon, Arbitrum, and Optimism. The mechanism through which this is made possible isn't exactly relevant to your primary understanding of blockchains. What is important is to know that layer-2s operate on layer-1s.

A Mini Digression on Tokens

Why're tokens necessary for blockchains, and how many types are there?

For starters, not all blockchain projects require tokens. Most private blockchains owned by businesses and corporations don't have tokens and work just fine. That said, tokens are a necessity for public blockchains because they are used to initiate transactions and pay transaction fees on-chain; otherwise, the chain would be brought to a halt by spam transactions. For these reasons, you pay BTC to use the Bitcoin blockchain, ETH to use Ethereum, and DOT to use the Polkadot network. For proof-of-stake networks, tokens are also needed for security purposes—more on this in chapter 3.

It is important to note that not all tokens are utility tokens (i.e. tokens that are used for network-related transactions). Some tokens are governance tokens that only give a user the ability to vote on decisions that will impact the future of the project. Most dApps hosted on layer-1s have issued governance tokens that have no utility, however some governance tokens can be used to obtain dividends, though the exact mechanisms vary from project to project.

All the earlier mentioned tokens above are fungible tokens. A group of items is fungible when every item in this group is identical to the other, such that no member possesses any individuality. This means that they can always be traded for one another without any friction. But not all tokens in blockchain technology are fungible. Some are non-fungible.

If fungibility is the quality of being interchangeable with something of similar properties, then non-fungibility is the ability to have an identity, to be unique. That is all there is to it. Thus, a non-fungible token (NFT) is a token that is unique, as long as a single item/object was minted (created) when it was added to the blockchain. So when you hear of NFT collections today, it usually means that they are a group of unique tokens/pieces.

This settled, let's focus on the disruptive nature of blockchain technology.

Blockchains and Web 3.0: Disrupting the Web 2.0 Landscape

Like most technologies that came before them, blockchains want to challenge the status quo. Unlike earlier technologies that went about their disruption in a covert manner, blockchains are deliberately and openly revolutionary, seeking to change our perception of trust and automate it. Ask yourself: which human-centered industry doesn't require trust? Everywhere there is a middleman, there is an issue of trust. Thus, many fields are ripe for disruption through the use of blockchains. Below are some of our industries that are currently being reshaped by blockchains:

- Finance
- Governance
- Property
- Identity
- Data
- Supply Chain

At the core of this disruption is a difference in ethos between the existing digital world and the new digital world, between Web 2.0 and Web 3.0. First, there was Web 1.0, the phase of the internet during which end users could **only read data**. This was dominated by emails, newsletters, static websites, etc.

Then came Web 2.0, the phase during which end users could **read and write data**. Web 2.0 enabled a lot of good in the world, by enlarging our social networks and allowing us to become more connected. However, a lot of unintentional exploitation was allowed to run rampant until it grew into a monster that is brewing more inequality and abuse of end-users. It is marked by data leaks, user censorship, and user data exploitation to name a few.

Web 3.0 was born from the shortcomings of Web 2.0 and has brought a phase where end-users can **read, write, and own data**. With digital ownership comes a whole new paradigm that will take a few decades to fully define itself. Ideally, the user experience of Web 2.0 and Web 3.0 will remain very similar for the end-user, while the builders and project founders will have to work on catching up with new trends. For the end-user, the real challenge is understanding the ideals that underpin the revolution, as well as the advantages and disadvantages of self-custody of digital assets. More on this later.

What is important to note is the scale of disruption that is possible. In theory, any Web 2.0 company you can think of can be reorganized from a Web 3.0 perspective. Remember that the main differences between Web 2.0 and Web 3.0 are actual ownership and freedom. Ask yourself: is there an industry that can't be reshaped to promote more fairness and inclusion? It would be near impossible to find one that is optimized as is, and this is the reason why blockchain disruption will keep speeding up. For now, this forward movement is limited in scope because every blockchain is an island.

Thankfully, Polkadot offers a path to maximum disruption, and the rest of this book is dedicated to explaining what it is and how it plans to achieve its end goal.

Chapter 1

Into the Dot

Polkadot, at first glance, can be difficult to understand. Some are instantly put-off by the unfamiliar concept of a blockchain with no smart contracts connecting other blockchains. The few that make it past the initial confusion have to contend with other layers of complexity: on-chain governance, forkless upgrades, parachains, crowdloans, auctions, cross-chain messaging, and more. Some determined few make it past this point, aided by videos of Gavin Wood explaining the ecosystem design on Youtube, the whitepaper, Polkadot wiki, and other helpful resources. What they all find at the end of this intellectual expedition is that Polkadot is much more than a simple blockchain.

Every blockchain network inherently seeks security, but this is not an easy task at all. Since security refers both to network security and economic security, it is expected that:

- The blockchain is heavily decentralized with few or no high-value attack vectors (like central computers that store sensitive information). This translates into getting many miners or validators to verify transactions on the network. If there are too few, they may collude and harm the network.
- The blockchain has a market capitalization large enough to make attacking the network economically difficult. For example, if a blockchain has a market capitalization (the price

per token multiplied by the total number of tokens in circulation) of $15 million, anybody who can afford to gamble $15 million could potentially take control of the network. Also, if one person owns a lot of tokens, they could crash the price of said token by selling all of theirs at once and then buying them back when they are cheap. This manipulates the market capitalization of the network. In a PoS network where the total value of tokens staked on the network equals the cost of attacking that network, such manipulation might be difficult. This is because although you might have $15 million, it will most likely be very difficult to find enough people to sell you $15 million worth of tokens.

In summary, launching a new blockchain is not easy. How can we run a variety of blockchains and still have the same level of security across the board? That is the first problem that Polkadot aims to solve. By creating a heterogeneous multi-chain environment that other blockchains can plug into, and therefore benefit from its already established security. In other words, Polkadot creates a solar system where all planets (blockchains) benefit from the energy (security) of the sun (Polkadot's relay chain).

The second problem concerns interoperability. As I explained in chapter 0.5, DeFi (decentralized finance) grew exponentially ($50 billion in total value locked in under 15 months) because Ethereum enabled seamless interactions between smart contracts, leading to fascinating new use-cases and a "bull market cycle". Think of it this way: each smart contract is a house that can be accessed by all the servants of other houses in the country (blockchain). Thus, if a baker needs butter, his servant can run into the cook's house and get the butter without seeking permission. In the real world, this would be called theft; but because the house itself is a smart and connected device, it knows that the butter is being borrowed by the baker's servant and that it will eventually be returned. This is an overly simplistic illustration of what happens, but it does explain the basic processes.

Things and people work better together, and blockchain networks are no exception to this rule. If you think of each blockchain as an Internet Service Provider, then it becomes easier to understand why one blockchain might want to deal with identity, another with content, and others with banking, gaming, privacy, and so on. The possibilities become endless, like it used to be with Web 1.0. It is irresponsible, given the potential of blockchains, not to take advantage of the opportunity to create richer interactions between different specialized blockchains, and this is where Polkadot comes in. Similar to how TCP/IP connected different nodes to create the internet, Polkadot is connecting blockchain networks, essentially becoming a network of blockchain networks.

So what is Polkadot?

At its core, Polkadot is a proof-of-stake layer-0 blockchain that connects other blockchains. Polkadot's goal is to optimize **scalability**, **interoperability**, and **shared security** for all its connected networks.

We will consider each feature in turn to explain what the core problems are and how Polkadot solves them by design.

Shared Security

To address the issue of multiple isolated chains and splintered security, Polkadot provides a framework where various chains can share security operations. Instead of relying on each layer-1 blockchain to provide its set of validators to secure its network and a token with a large enough market capitalization, these chains can all leverage the security of Polkadot, the layer-0 protocol. In practice, if Polkadot is sitting at a $10 billion market cap, then each new layer-1 blockchain that deploys on Polkadot is economically secured by this same $10 billion. On top of economic security, the chain will also gain network security from Polkadot's large set of validators. This is a first in blockchain technology, a feat never seen before.

Interoperability

This is the highlight of Polkadot's layer-0 protocol. We have previously seen what dApps can do when they communicate with each other freely, now we are talking about what will happen when different blockchains effectively integrate each other into their daily operations. It may be hard to picture at this point in time, but it will surely become easier once we get to chapter 5 and Parachains. For now, just remember that a large part of Polkadot's design is about ensuring interoperability between heterogeneous layer-1 blockchains.

Scalability

Blockchains will never be able to bring greater fairness and inclusion if they don't scale on a global level. Polkadot's solution to this issue is to use "sharding", which allows the network to run different transactions in parallel. For example, Ethereum, as it exists in 2021, is a single-shard network where transactions are processed one after the other and every node needs to store data from the entire blockchain. In a single-shard network, all transactions, although very different in nature, will be carried out in the same shard. Whereas, in a multi-sharded network, transactions will be executed in parallel, within their respective shards. In this case, each shard corresponds to a different blockchain, such that DeFi transactions are carried out on the DeFi shard, while NFT transactions are carried out on the NFT shard. Again, this is an overly simplistic description of what happens, but it should help you make sense of scalability processes.

On Polkadot, each layer-1 chain is able to customize its network for different use cases, thus tackling the problem of scalability in an open-ended context with efficient parallel computation (wherein the network is processing different kinds of transactions on different nodes). In this way, a layer-1 chain focused on decentralizing identity will not need the same system design as one which is focused on decentralizing finance. Thus, the network is made more scalable by:

1. Ensuring that each network (parachain) is optimized for its use case.
2. Running different transactions in parallel.

For example, let's say you have 1,000 nodes verifying the validity of transactions on your network. In a single-shard model, all 1,000 nodes will be processing the same transactions. In a 4-shard model, the nodes will be split into four groups of 250 each. Each group of nodes would then process different types of transactions. Group A would process transactions from the identity chain, while group B will process transactions from the finance chain, group C from the governance chain, and group D for the data chain. In this way, we still have 1,000 computers, but we are doing a lot more because of how we have chosen to arrange them.

Forkless Upgradability

I lied. Chain Interoperability is a highlight of Polkadot's design, but it is not the only one.

Remember the problem between Ethereum and Ethereum Classic? Or the rift between Bitcoin and Bitcoin Cash? They happened because the original/canonical chain needed to upgrade its core protocols through a hard fork. A fork, as the name implies, offers a different path to stakeholders at a specific point in time. Forks may seem like a desirable feature in a network, but consider for a moment a country that splits every time its citizens have a big argument on the outcome of a vote. This country would get smaller as more people leave, losing a chunk of its original human capital each time. Of course, given that blockchains are analogous to digital nation states, forks aren't very ideal for long term growth. For the long term prosperity of the network, it's imperative that the community finds a way to resolve disputes and upgrade protocols without putting itself at risk. Thus, Polkadot allows for forkless updates, and we will explain how this is done in chapter 4.

For now, it is enough to have an overview of some of the key features that make Polkadot special, as we will go over the technical design of Polkadot in the next chapter. Before that, let's talk a bit about the Polkadot ecosystem's agent of chaos.

A Brief Note on Kusama – The Agent of Chaos

Although this book speaks exclusively of Polkadot with no mention of Kusama, it is important to understand that the two blockchains are deeply connected, both technologically and conceptually.

Kusama is often regarded as a live test network for Polkadot, but this is not the case. Kusama is an independent and full-fledged relay chain with its own auction schedules, parachain candidates, governance, and communities. Kusama spearheads developments in the Polkadot ecosystem: as such, every functionality deployed on Polkadot is first and foremost deployed on Kusama. Kusama is a wilder version of Polkadot that exists primarily to safeguard Polkadot from experiencing unexpected disruptions and real-life behaviors.

And so, the main differences between Polkadot and Kusama come down to speed of implementation and tokenomics, because Kusama's governance system runs four time faster than Polkadot's, and also because the genesis supply of KSM is a hundred times smaller than that of DOT. For this reason, Kusama's tagline - that the community has quickly adopted - is 'Expect Chaos 'because there's no telling what will happen in the wild and experimental world of Kusama.

While this book doesn't explicitly reference Kusama by name, it should be understood that every mention of Polkadot includes Kusama by default. The decision to focus the content of this book on Polkadot was mainly to avoid burdening the reader with too much information, but if you ever want to refer to both Polkadot and Kusama ecosystems in one word, the term *DotSama* will suffice.

Chapter 2

The Network

Polkadot is often criticized for being complicated, and that is mostly true. That said, this complexity is built upon a simple technical architecture which consists of only two main parts—relay chain and parachains. The relay chain is the central hub all parachains connect to. This short chapter will focus solely on the relay chain. Parachains will be covered in chapter 5.

Image: the Polkadot relay chain

Relay Chain

To visualize the purpose of the relay chain, imagine a circular pipe to which many other pipes connect. These connecting pipes could be of any shape and provide any functionality, so long as they use the same rules as the main pipe.

The primary function of the relay chain is to provide shared security and interoperability to all its parachains. But to do this, the relay chain itself first needs to be as secure as possible. I mean, how can you lend

your security forces if your own security is compromised? To understand how the relay chain preserves its own integrity over time, we need to consider two key aspects of blockchain networks.

A public blockchain is a sought-after environment because no one controls the flow of information (whether verification or retrieval) that is exchanged on it. This means that a majority of network nodes must agree on the validity of a new block before it is created and connected to the chain of blocks. But how do the nodes come to an agreement on which transactions (data) are valid? This happens via a process called consensus.

The full details of the relay chain's consensus mechanism would be too technical for this book, so what is offered here is an overly simplified explanation. The current implementation of the Polkadot relay chain uses a hybrid consensus mechanism, meaning that it combines proof-of-stake with proof-of-work to get the best of both worlds.

As a general rule, there are two processes to blockchain consensus, namely *block production* and *finality*. Block production refers to the process of creating new blocks, while finality refers to the process of verifying and sealing blocks onto the chain. The Polkadot relay chain, like all decentralized blockchain networks, attempts to solve a few problems through its consensus:

- Robustness in the face of collusion by bad actors, such that all it takes is a few good actors to preserve the integrity of the chain. This means that if there are only a few honest nodes, less than 50%, the integrity of the chain will still be preserved despite tampering by corrupt nodes.
- Speed of transaction inclusion and verification for scalability.
- Network resilience such that it doesn't go down frequently or at all.
- Higher degree of decentralization, so that no group of network participants has full control over the network.

To ensure the successful implementation of these solutions across the board, the relay chain uses a BABE and a GRANDPA. A detailed explanation of both protocols is not necessary for our presentation on Polkadot and has been relegated to the technical appendix.

Next, we consider how the relay chain gains its security from validators, nominators, and collators.

Chapter 3

Securing the Network

Having understood the technical design that facilitates technological security, we can now turn to security. How does Polkadot guarantee its economic security? To answer this question, we will dive into staking and the various roles available within the network.

The Philosophy of Staking

Decentralized networks achieve collaboration between many individuals by using the concept of game theory to design a system where there are roles, responsibilities, and incentives to align the actions of all network participants. This is one of the primary reasons why tokens are necessary for many decentralized systems—economic rewards are the ultimate incentive mechanism. For Bitcoin, it is BTC, and for Ethereum, it is ETH. Thus, the strength of a blockchain's security isn't solely determined by the quality of its code. It is also defined by the quality of its incentive and token design which, at the core, is game theory. For example, all miners on Bitcoin create and verify blocks for a reward in BTC. In a proof-of-work system like Bitcoin, the network roles are few and limited to miners. This is because the network only needs nodes, Bitcoins, and users.

In a proof-of-stake system, in addition to nodes, the network needs users who will put down some stake to secure the network. Remember that proof-of-stake blockchains rely on both technological

security and economic security so that the environmental impact is offset by economics. A proof-of-work blockchain's security is only as strong as the number of nodes securing it, whereas a proof-of-stake blockchain's security depends on its number of nodes and the value of its stake, with stake being its economic value. Thus, the process of securing the network in a PoS blockchain is called staking. There are two key advantages of PoS over PoW:

- PoS has far less energy consumption compared to PoW. This is a crucial point because our technologies are having a greater impact on climate change. For example, data on record has shown that the seven warmest years in the 1880-2020 period have all occurred after 2014.
- PoS offers greater involvement of the community in network security, thus achieving greater decentralization. This is because PoW shifts the responsibility of network security towards technically savvy people with the means and the skills to run a node. Over time, this inevitably results in increasing levels of centralization.

There are three types of participants working on securing the Polkadot network—validators, nominators, and collators.

Validators

Validators in Polkadot are like miners in Bitcoin. They run nodes that process and verify transactions, create blocks, and store the history of the blockchain. Without them, there would be no network. The key points to note are:

- They provide the physical infrastructure on which the network runs
- They have to ensure that they are always online when they need to be (particularly when they are the ones to create a new block).

The process is as straightforward as acquiring the relevant computer equipment and running Polkadot's code. Once a node is deployed, most routine operations can be automated, while validators can focus on troubleshooting and maintenance of connectivity. For their efforts, economic and physical, validators are rewarded in DOT tokens. The total number of validators on the network is a parameter that can be adjusted based on network demand, starting with a few and now reaching 297 (as of January 2022). The goal is to reach 1,000 validators.

One may look at this number and wonder if it is enough to support decentralization, especially when one considers that Bitcoin has over 20,000 miners and Ethereum 1.0 has over 10,000 miners. To understand why 1,000 validators is sufficient, we need to keep in mind how Polkadot's consensus works. By selecting validators at random through the block production module BABE and keeping the information about block validation separate, Polkadot limits the possibility of collusion between validators. This procedure is also secured by the premise that all validators must compete at once to validate individual blocks

When it is said that Polkadot targets 1,000 validators, it doesn't mean that there can only be 1,000 people qualified to become validators. Rather, it means that block production and verification will be handled by 1,000 validators at the same time, while every other validator will act as a validator candidate. In the end, a low number of validators is useful not only for reducing our carbon footprint but also to achieve scalability. If there are 13,000 validators and 2/3 validators in the active set (those currently participating in network consensus) must agree, then each transaction will need to wait on roughly 7,500 validators before being processed, which would inevitably slow the network.

The goal of decentralization isn't to have as many validators as possible, but rather, as many network participants as possible. It is all about ownership, power, and authority. This is why proof-of-stake is a much more desirable system, because many people don't have the

means nor the skills to run nodes. If the security of the network is only provided by validators or miners, then a large portion of the community will be left out. With proof-of-stake, the average Joe who knows nothing about computers or coding can play a central role in securing the network and also earn rewards; by contrast, proof-of-work blockchains tend to lead to the centralization of ownership, power, and authority around techies and mining gear operators. The main objective for a proof-of-stake system is ensuring that the staking mechanisms in place foster greater decentralization. To understand how Polkadot achieves this objective, we will explore the role of nominators.

Nominators

If you're reading this book, then it is more than likely that you are or are looking to become a nominator. A nominator's role in securing the network is much less technical than a validator's. This is because nominators are only asked to lock their tokens in support of validators who will do the heavy lifting of running the nodes. Because the bond required to become a validator is high (currently 1.4 million DOTs), validators need to secure ongoing support from a large number of nominators 'tokens to qualify for their role. When rewards are paid to the validator, a portion of those rewards go to the nominators; the exact amount is ultimately based on the total number of tokens staked and the commission percentage set by the validator.

Unlike many PoS systems which force nominators to bond all their tokens with a single validator, Polkadot uses an advanced mechanism that allows every nominator to choose up to 16 validators. From these, only a few validators will manage to get admitted into the active set during elections that take place every era (which is roughly a day on Polkadot). By choosing 16 validators, nominators give themselves higher chances to obtain maximum rewards. This is because the relay chain on which you stake your tokens has a protocol that optimizes the staking process for all nominators and validators to ensure

maximum security. The details of this action are too technical, so I will offer only a basic summary of its core functionalities:

Maximize Nominator Participation - The algorithm (protocol) maximizes a nominator's participation in consensus by selecting at least one of the nominator's validators for every era. An era is a measure of time in blockchains–a bit like how we humans have days–that is denominated in the number of blocks produced: 6 hours on Kusama and 24 hours on Polkadot. When a nominator selects 16 validators, this mechanism ensures that at least one of those sixteen will be in the active set.

Minimize Risk of Centralization - This is achieved through game theory. It is natural that humans seek that which is most certain, which often is the most popular of all available options. For example, if many nominators choose one validator, other nominators will be inclined to choose the same validator. And this is how centralization occurs, since the validator ends up with more power over the network than originally sought. To mitigate this risk, the staking protocol pays out equal rewards to all validators, regardless of the weight of their stake or the number of nominators backing them. But validators with many nominators will pay out less rewards per DOT staked overall. In the end, only nominators that are staking the most DOTs with these popular validators will get the biggest share of the rewards, while nominators who haven't staked a lot of DOTs will get much less (or not at all, depending on how oversubscribed the validator is). The number of nominators who get rewards in such a situation is dynamic and will vary over time. This is intended as a mechanism to force every nominator to constantly review their nominations and ensure that they are getting maximum rewards for their network participation.

How to Nominate

The first step to nominating is to get your DOT tokens, for which you need an account and a wallet. You can use wallets like Polkadot-JS, Fearless, Talisman, Nova, Polkawallet, and many other ecosystem wallets. One thing to remember is that, after you bond your funds for

staking, you will fall under a mandatory “unbonding” period of 28 days. Meaning that from the moment you choose to unstake and withdraw your tokens, it will take you 28 days to get your tokens back.

To avoid this inconvenience, you can stake with a third-party that will give you more freedom, as some centralized exchanges allow you to instantly withdraw your stake. A more preferable solution would be to use decentralized platforms that give you a derivative token when you stake your DOT. For example, you can stake your DOT using Acala (more on them later) and receive LDOT which is short for “liquid DOT”. The difference between DOT and the derivative token LDOT is that LDOT earns staking rewards while remaining available for use on DeFi protocols across the ecosystem. Such that when you go to swap your LDOTs back to DOTs, you will have more DOTs than you did before. LDOT isn’t the only token that serves this function. There are other parachains that offer the same liquid staking service, but with different names for their tokens (Bifrost's vDOT and Parallel Finance's xDOT to name a few).

The real work of nominating comes down to selecting your 16 validators. If you are staking via a third party platform, then you don’t need to go through this process. However, if you are staking on your own, then you will need to learn how to select the right validators.

Selecting the Right Validators

Selecting the right validator is a crucial process because of the reality of slashing. If you choose a validator who acts maliciously, then you are at risk of losing your hard earned tokens, which would be a tragedy. Another reason you want to select the right validators is to maximize your staking rewards. Some validators will allow you to earn more than others and it is your job to maximize your own rewards. When selecting the right validators, there are a couple of things that you will need to consider.

Validator's Skin in the Game - It's hard for someone to act maliciously or carelessly when they have something to lose. This is also referred to as having "skin in the game". If a validator doesn't have any tokens in his own stash, then it means that he has nothing to lose if he gets slashed; but his nominators will be bearing the consequences of his actions. If he gets rewarded however, he will get to keep some chunky rewards. Thus, it is not advisable to put your stake on a validator with no or low self-stake, unless you trust that they won't act maliciously or carelessly.

Validator's Identity - It is hard for someone to act maliciously when their identity is known by everyone on the network. Of course, this isn't going to save you from every validator's mistake, but it is a reliable rule of thumb to use. People who display their identity on-chain are more trustworthy than those who don't because their reputation is on the line. In the case of someone with an on-chain identity, you can reach out to them to find out what is going on in the event that you have concerns about transactions.. However, some shady validators can get slashed and decide to spin up a new validator account with a new identity, which would probably be the same as the original, only with a few details changed.

Validator's Commission - For greater profitability, it is wiser to choose validators with the lowest commissions. A validator with a 50% commission will take 50% of all staking rewards, leaving only 50% to be shared between nominators. One with a 10% commission will take only 10% of all rewards, which certainly makes the latter much more profitable.

Validator's Slashing History - It is natural to make a decision about a person or entity based on past performance. In the case of validators, you don't want to nominate validators that have had multiple slashes in the past. However, sometimes validators can be at the receiving end of slashing events that are not entirely their fault. The network can sometimes run into problems that cause honest and diligent validators to get penalized.

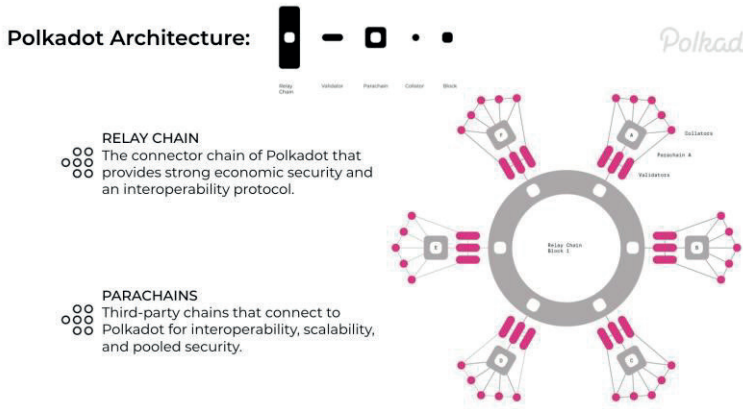
For more information on the safest way to nominate validators, check out this guide.

Collators

While validators create and confirm blocks for the relay chain, the collators create and confirm blocks for the parachains. Keep in mind that the same mechanisms (BABE and GRANDPA) are at play on parachains. You can think of collators as parachain validators, because they have to run a full node of the parachain as well as the relay chain. When Collators on a parachain agree on new parachain blocks, they forward these blocks to relay chain validators for inclusion into the relay chain. This way, verified transaction blocks submitted by collators are further verified by validators and added to the relay chain; with relay chain validators assigned to parachains at random.

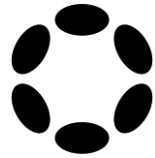
For example, in the first era, which lasts x number of blocks, validators V1, V2, and V3 are assigned to parachain A. This means that the collators of parachain A will forward their transactions to V1, V2, and V3, leaving all the other validators free to verify transactions from other parachains. When these validators are done verifying, they propose their verified transactions to the rest of the validators on the relay chain for further verification before the transactions are added to the relay chain. Remember that most of this is fairly automatic. The validators don't know beforehand on which parachain they will be working. At the end of the era, validators V1, V2, and V3 will be rotated away from parachain A, so that a new set of validators will be verifying transactions on parachain A for the duration of the second era.

This process strengthens network security by minimizing and containing the risk of collusion between collators and validators. For example, if there was an attack during an era, this attack would be countered by honest validators at the beginning of the following era.



Architectural diagram of validators, nominators, and collators

1. National Oceanic and Atmospheric Administration. (2021, January). 2020 was Earth's 2nd-hottest year, just behind 2016. *https://www.noaa.gov/news/2020-was-earth-s-2nd-hottest-year-just-behind-2016.* Accessed: 2021-08-31.



Chapter 4

Governing the Network

When a Classic Left with the Cash

In 2016, $60 million in ETH was stolen in what is now called the "DAO hack". This is a brief summary of how it happened.

In April 2016, a large number of people pooled their Ethereum tokens in a smart contract to fund the very first Decentralized Autonomous Organization (DAO) of the crypto ecosystem. $150 million was raised during this crowdfunding. However, less than three months later, the smart contract was hacked and a bad actor began draining the funds. The community was thrown into panic mode. Soon enough, a group of white hat hackers emerged, collaboratively trying to stop the offender. The details of how the hack occurred would be too technical for this book, but it was clear that the black hat hacker had taken advantage of a flaw in the smart contract code. Since the attacker could only withdraw the tokens very slowly the collective of white hat hackers ultimately found a way to stop the exploit. But the rescuers made a blunder that would eventually allow the thief to go scot-free with the money: the only solution left was to revert the chain and cancel this event.

Given that the theft happened right under the nose of the Ethereum community, you would think that deciding on the right course of action would be an easy conclusion to reach. But that wasn't the case. First, the community had to figure out a way to poll the users of the

Ethereum network on what they thought should happen next. This is because, at the time, it was generally accepted that blockchain data was immutable, sealed by cryptography, and that whatever happened on-chain could never be reverted. But, in this case, since $60 million had been stolen, ideals had to contend with reality. And the reality of the situation was that it was possible to change the information stored on the Ethereum blockchain.

Two camps emerged as a result of this discovery. On the one hand, the majority wanted to erase the history of the theft by reverting the chain to the block preceding the attack. On the other hand, decentralization purists were against tampering with the immutability of the Ethereum blockchain. In the end, a vote was carried out and 80% of the community voted to erase the hack from the Ethereum blockchain's history. To do this, a fork had to be created to update the blockchain and rewrite the original code. But for a fork to go ahead, all the nodes on the network needed to accept the update so that the network could enter a new state and proceed in a new direction. Thus, when the update was carried out, it erased all traces of the hack and most community members were happy that morality had won and that the thief would be left with nothing. Or would he?

It soon became apparent that, although the Ethereum network had forked into a new chain and was writing a new history, there were some nodes thatdidn't follow the path of the new upgrade. Basically, they had chosen to stay on the old Ethereum canonical chain, with records of the theft still in place. Soon, a new kind of panic set in: were the node operators doing this intentionally? Could it be the hacker? Attempts were made to reach out to the miners and, in the end, it was clear that it was a deliberate act, though the reasons still remained unknown. The old chain that refused the fork became known as Ethereum Classic. You can learn more about this story in *Out of the Ether,* a book by Matthew Leising released in August 2020*.* It became necessary to delve into this bit of history to highlight the importance of Polkadot's on-chain governance design and forkless upgrades.

You may then wonder: what is the big deal with Ethereum forking into Ethereum Classic? From the perspective of decentralization, it makes sense to give every network participant the freedom to choose whether a fork is suitable or not, thus preserving the integrity of the chain. But it also poses other important risks for the community: when a few miners broke off their consensus with the Ethereum network and chose to stay on the old chain, the security of Ethereum was compromised on three levels:

1. The network was left with fewer miners to mine transactions.
2. The value of ETH was affected as its price went into free fall.
3. The faith of the community was shaken by the hack and the unexpected fork.

Sadly, this isn't the only contentious fork to have happened in the history of blockchain networks. It also happened with Bitcoin. It started when the Bitcoin community got into an argument about the Bitcoin blockchain's speed, proposing different ways to scale the network and increase the number of transactions that can fit into a block. One camp wanted to increase block size by 8x to process 8x more transactions per second. But this would also increase the block validation time beyond 10 minutes as the network waits for the now larger blocks to fill up. Others thought that tampering with the Bitcoin protocol was heresy.

There was no vote and no consultation; a portion of the Bitcoin network forked into a new network called Bitcoin Cash which saw them update the existing code to allow an increase in their block size. Over the years, Bitcoin has been forked into many other networks, however, the mining power that secures these forks is more and more concentrated into the hands of a few large mining pools.

So, these forked networks can easily be attacked because they don't offer the same value as Bitcoin and can't attract enough network participants. This is because the power of any decentralized network lies in the strength–numbers and participation levels–of its community.

When we look at Bitcoin and Ethereum today, it seems that these forks have had no impact on the networks, but that would be a naive view of the situation. The fact that both networks have made it this far in spite of these contentious episodes isn't proof that their design is optimal. Rather, it points to a problem inherent to all blockchain networks: if the code is available for everyone to see and copy, then it is easy to fork. And if you fork a network enough times, you can damage its security for good. Because each fork results in a loss of network value and consensus power by drawing miners or community members away.

So how can you avoid weakening a network and its community? Polkadot's answer is to offer an on-chain governance process that every participant can trust. Coupled with forkless upgrades, you then get a blockchain that is easily upgradeable without enforcing breaking changes. To understand how, let's dive into Polkadot's governance mechanism. This section will follow a Q&A format.

Governance on Polkadot

1. What is governance for?

The main purpose of governance in any system is to modify the system parameters. In the case of countries, these would be new bills and revisions to the constitution. In the case of Polkadot, these would be on-chain data. Some examples include:

- Updating user balances (in the case of theft or lost keys for instance)
- Updating the runtime
- Connecting or disconnecting parachains and parathreads

2. What is the governance structure?

Polkadot's on-chain governance structure has 3 arms: the Council, the Technical committee, and the community (also called the "referendum chamber" or the number of DOT holders available to vote). Let's examine each of them in detail.

Council - This is a group of 6-24 members who represent all DOT holders**.** Their primary purpose is to examine proposals that aim to give new directions to the Polkadot network.

What can they do?

- Elect Technical committee members
- Vote on Council motions - All proposals (Referendum, Treasury, Bounty, Tips) need to be explicitly passed/rejected by the Council before moving to the next stage. The only exceptions are community-led proposals.
- Veto referenda in the case that a proposal is deemed harmful to the ecosystem. That said, their veto can be overridden via another public vote.
- Fast-track referenda in the case of a technical emergency.

Who can join the Council?

Any DOT holder.

How are they selected?

A DOT holder who wishes to join the Council only needs to nominate him/herself and gather enough votes to get into the elected set. DOT holders can elect Council members to govern the network on their behalf by bonding their tokens, the same way they chose their validators. As such, any DOT holder willing to become a Council member should be willing to campaign for nominators because Council members are selected based on the backing and preference that voters gave them.

Every two weeks, an election is held to reshuffle the composition of the council so as to prevent nepotism. This is designed to encourage community participation in governance as it invites passive holders to delegate the power of their DOTS to other members willing to govern the network. But this is only an ideal scenario. In reality, the same Council members often remain in their seat for months because there aren't enough Council candidates and because voters rarely change their list of their preferred candidates.

What is the voting mechanism?

The selection of Council members is carried out using the same mechanism implemented in staking. However, since the selection relies on token-weight, there is the chance that, over time, the network will favor users with a large number of DOT called "whales". There is no perfect solution to this problem as of now, but the Phragmén method that is used in Polkadot offers an interesting solution. This is because its algorithm takes into account the token-weight behind each candidate but doesn't make decisions solely based on that information. Instead, the method optimizes outcomes for the following ideal scenarios:

1. Maximize the total amount at stake so that maximum economic security is guaranteed.
2. Maximize the stake behind the minimally staked validator so that all candidates keep competing to obtain backers that will allow them access to the active set.
3. Minimize the variance of the stake in the set so that there isn't too much of a difference between the highest and lowest staked validators.

All in all, the Phragmén method does a decent job of creating a certain degree of fairness, all things being considered. To understand its inner workings, take the time to read through this wiki article.

Technical Committee - The TC is composed of developers who have contributed to the Polkadot codebase. They are tasked with ensuring that the network runs smoothly.

What can they do?

- Make proposals to the Council
- Fast-track proposals—usually in the case of a technical emergency
- Veto referenda through a recommendation to the Council—if a referendum poses a security risk to the Polkadot relay chain

Who can join the Technical committee?

Teams are added or removed from the Technical committee via simple majority vote of the Council.

Community - It is composed of any DOT holders who can and are willing to participate in the following activities:

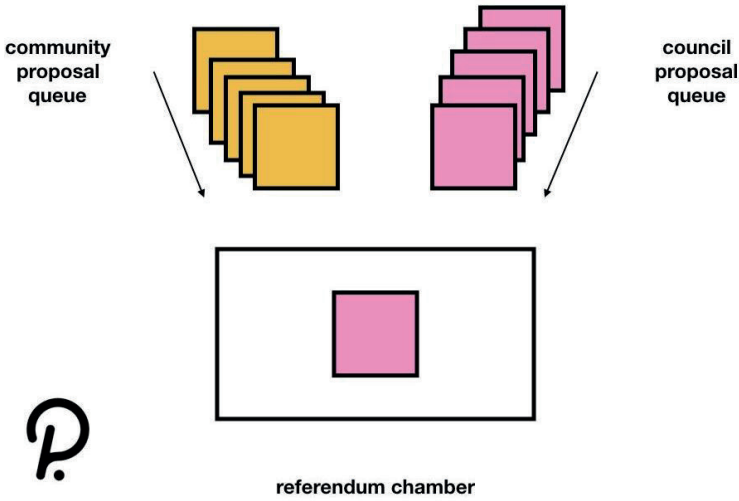
1. Nominate Council members
2. Make proposals
3. Vote on referenda

3. How are decisions made?

Every decision made about the direction of Polkadot begins with a proposal. A proposal can be initiated by any of the three governance arms, though all Technical Committee proposals are submitted to the Council who then vote on it. If the proposal is successful, then it becomes a public referendum. As such, there are two main proposal queues: one for community-led proposals and the other for Council-led proposals.

Every "voting cycle" (28 days on Polkadot), the proposal backed by the highest number of tokens becomes a public referendum. There can only be one proposal per referendum, except in emergency situations when the technical committee needs to fast-track one or more supplementary proposals.

If a proposal from the community queue was voted on in the last voting cycle, then the top proposal from the Council queue will be featured in the new voting cycle. This turn-taking approach helps ensure that the community, Council, and technical committee can actively participate in timely decision-making.



The referendum process: two queues.

4. What is the life cycle of a proposal?

Every proposal submitted via on-chain governance can fall under any of the following status:

Seconded - When a community-member makes a proposal, he or she must bond some DOTs. If the proposal is valuable to other community members, they can second it by locking more DOTs into the original bond. The more DOTs get bonded in support of a proposal, the faster this proposal reaches the top of the queue, at which point it will change status. A similar process is in place for Council-led proposals.

Pending - When a proposal has reached the top of the queue, it will soon be converted into an official public referendum. It is important to note that once the proposal is timetabled, bonded DOTs are returned to the proposers/supporters.

Canceled - If a proposal is considered dangerous for the Polkadot relay chain, it can be cancelled by the Technical committee. If such a proposal reaches referendum status before the nature of its threat is identified, then a two-thirds majority of the Council can cancel the referendum. If the cancellation of a referendum is contentious, then the decision making will be passed onto the community. When a proposal or referendum is cancelled, all the tokens deposited as part of its bond are burnt.

Blacklisted - A proposal that poses a significant risk to the system, for example, a coding error, can be blacklisted by the protocol. A blacklisted proposal can't be added back to the queue unless it has been amended.

5. How are votes calculated?

To calculate the results of a referendum, there are two main mechanisms that are worth considering.

Conviction Multiplier - This is a key area of governance that makes the most of game theory. This is because a system that relies heavily on proof-of-stake needs to have effective processes in place to level the playing field for token holders. In Polkadot, this practice is supported by the conviction multiplier.

Let's say, for example, that there are only two voters in a referendum: voter G and voter B.

G votes with 20 DOTS

B votes with 90 DOTS

Naturally, we would expect voter B's opinion to win. This isn't the case when you introduce the conviction multiplier because both the number of tokens bonded and the bonding duration are factored in the final outcome.

Let's have a more in-depth look at the conviction set up by voter G and voter B.

G votes with 20 DOTS for a lock period of 6 voting cycles

B votes with 90 DOTS for a lock period of 1 voting cycle

According to the Polkadot blockchain specifications, a voting cycle is 4 weeks and each cycle increases the conviction multiplier by a factor of 1. Thus, in the above example, here's what the result will look like.

G = 20 x 6 = 120 DOTS

B = 90 x 1 = 90 DOTS

As you can see, voter G's opinion will be of greater consequence because she had a greater conviction multiplier. To learn more about this interesting mechanism, you can read this wiki article.

We do not yet know to what extent the conviction multiplier rebalances voting power between community members with a few DOTs and those with much bigger portfolios, so this solution might require further adjustments in the future.

One last thing to note is that tokens that are used for voting in referenda or nominating Council members are temporarily locked and cannot be transferred to another account, which makes any attempt to game the system costly. However, these DOTs can still be staked to earn block production rewards.

Adjusted Quorum Biasing - This is another important area of on-chain governance that makes extensive use of game theory in its design. There are three different ways to determine the outcome of a public referendum depending on which governance body initiated the proposal.

Simple Majority

If a proposal is submitted with a majority approval from the Council, then it needs a simple majority of 'aye 'or 'nay 'to pass or fail. Regardless of voter turnout, the majority will determine the final outcome of the vote.

Positive Turnout Bias

For referenda sourced from community-led proposals, things are a bit different.. In this case, the voting mechanism has a built-in bias against the proposed changes that can only be offset if there is overwhelming positive support from the community. If few voters turn up, then the amount of 'ayes 'required to proceed with the upgrades increases considerably. For example, where 19% of community members cast their vote, it could take as little as 20% of 'nays 'to overthrow 80% of 'ayes'.

This setup is designed to protect the ecosystem from bad actors who submit controversial proposals in the hope that a low referendum turnout will favor their desired outcomes.

Negative Turnout Bias

This mechanism is used when tallying the votes of a referendum sourced from a Council-led proposal. In this scenario, the mechanism is positioned against a rejection of the proposal, so that with a low number of voters, the percentage of 'ayes 'needed to pass the proposal will be low. For example, with a turnout of 30%, only 30% of 'ayes 'will be needed to overthrow 70% of 'nays'. The main goal here is to speed up the technical updates on the network. If the council and technical community unanimously agree on the merits of a proposal, then it is also safe to assume that the proposed changes will add value to the ecosystem.

6. What happens after a referendum?

If a referendum fails, then nothing happens on-chain. If the referendum passes, on-chain changes will be automatically implemented by the system after a waiting period of 28 days. This is one of the advantages of on-chain governance as coded on Polkadot, which also highlights why it is important to have the option to cancel or blacklist proposals.

With all these major parameters considered, I feel the need to add one more section.

Criticisms of Polkadot's Governance Mechanism

Polkadot's on-chain governance processes has drawn a lot of criticism. Most times, these negative comments are born from ignorance rather than strong opinions about specific issues. This section will address the most common criticisms and propose a rebuttal.

1. It is another form of centralization/it will become centralized

Some people believe that a visible and active governance process is just another form of centralization waiting to happen. Truthfully speaking, I also have this fear. That said, a governance process doesn't really instigate centralization, it is the users who do. Presently, many people believe that Ethereum is fully decentralized when it comes to decision-making, which is not completely true. But what does the Ethereum foundation do with its budget? How exactly is spending governed or tracked by the community? This isn't to suggest that anything shady is going on behind the scenes. Far from it. My main point is that no one in the Ethereum community knows the full details of how funds are being spent and who is saying yes to these spending proposals. This is not meant as a criticism of Ethereum's process, but rather to draw attention to the fact that information on some of its workings remains rather vague. Thus, how can anyone really have a problem with having a more transparent method of doing the same

thing? I'm only pointing out some aspects that we might overlook or take for granted.

When it comes to network-related developments, it is widely accepted that Vitalik Buterin's ideas are driving the Ethereum ecosystem's roadmap. Other participants often champion his ideas into new projects, while a minority of critics point out flaws before the changes are eventually implemented by the miners. This is a good process in practice, but it can be very slow and is lacking in transparency. While the same would have been said about Polkadot at the beginning, we can now verify all changes because everything is on-chain.

If there's a treasury, then the community needs to know how it is being spent. And if there is none, wouldn't the community benefit from having one? As of now, there is no official Ethereum or Bitcoin treasury that can provide funding to community members in an open and verifiable manner the way an on-chain treasury is available to support ecosystem developments. Beyond funding, it is obvious that decision-making processes are currently centralized in the hands of a foundation. Personally, I find no fault in this as it is hard to imagine that the people who built a system would scheme to destroy it; this is also why we implicitly trust project founders. But I'm still in favor of on-chain processes as a way to make sustainable decentralized network-related decisions.

In the end, if we want a better society, one that will still reflect the present one but with fairer rules, we need blockchain. This is because blockchain is a tool we can use to fix or better our governance systems. Many mistakes will be made and many lessons will be learnt, but overall, experimenting is far better than doing nothing.

2. It gives bad actors (or novices) an opportunity to cause harm to the network

This is a legitimate concern, and thankfully, it has been considered in the design of Polkadot's governance. For one thing, any bad actor who wishes to destroy the network via governance must be willing to

spend a lot of money denominated in DOT. This means that anyone wishing to sway votes towards a negative outcome would have to:

1. Convince a large number of DOT holders to make a bad decision with their DOT.
   OR
2. Fund their bad decision themselves

Either scenario would be extremely costly in terms of funds and resources. But if a novice were to submit a dangerous proposal by error, there will always be checkpoints in the governance system that allow for corrections or cancellations.

3. It is too complex for the average Joe

I can fully empathize with people on this. Traditional governance is already so complicated that there are special academic fields to teach us about it. And so it is expected that a governance process that aims to become fully decentralized has to incorporate many lessons learnt from political science, history, and game theory into its design, thus making it complex.. That being said, you cannot gain a solid understanding of your country's constitution by reading a series of blog posts. Just as that requires some effort, this requires just as much.

And in the case of Polkadot, all you need to know is that there are specific roles and processes in place, information on which is much less than a 300 page document. As with any technology, understanding something simply means being able to use and make the most of it. Just as the average human can learn about an ordinary town council, understanding what an on-chain Council might do would not be too much of an ask. Admittedly, a bit more could be done to try and simplify the explanations of governance processes and the interfaces that are currently available.

4. Decentralization means no governance—Ethereum and Bitcoin are doing just fine

This criticism is far from being valid because technologies are meant to evolve in different directions, in the same way Ethereum Classic and Bitcoin Cash forked away from their original chains. At present, on-chain governance offers a way to resolve conflict without going to extremes and by providing verifiable means to an end. With the exception of Bitcoin, most decentralized projects have a parent Foundation. But what is a Foundation in this context, if not a group of people that we trust when it comes to managing the long-term success of the network? We don't really get to witness how decisions are made and the steps that are taken in applying these decisions. We get a blog post here and there with some vague explanations, but we don't see a vote count. Now, this is not to say that a vote is necessary for the validity of a decision, but only to show that we put a lot of trust in decisions that are made on our behalf without any real data to attest their legitimacy. Whereas, in decentralized blockchain systems, trust is only as good as the verifiable data that is recorded on-chain.

5. There is too much reliance on DOT and so the network is always at the mercy of large holders

This is another legitimate concern that I have had to think hard about in the past. First, there are a few aspects that we need to consider:

1. Whoever holds more DOTs has a lot more to lose if governance decisions negatively impact the ecosystem. Thus, this holder is incentivized to support changes that are best for the ecosystem.
2. Polkadot has recognised the limitations of token-based governance and is proposing a solution to work around these issues. It has introduced the conviction multiplier mechanism which allows small holders to give more weight to their votes.
3. If the network isn't evolving in a direction that you find desirable, you are always free to opt out of the ecosystem.

The over reliance on DOT is needed to secure the future of the network. Proof-of-stake is **proof-of-stake**. If we are fine with securing the network by using proof-of-stake mechanisms, why should we worry about adapting it to governance? The real question is: is there a better way to come to a consensus on governance decisions while maintaining operations on-chain? It is also possible that our reliance on tokens will eventually shift if the community later deems this step necessary. And that's the beauty of Polkadot's governance processes.

6. Something will go wrong, one way or another

We tend to have a negative bias towards things that are new or unknown. I myself can imagine the worst outcomes in nearly every situation so it is only natural for me to consider the possibility of something unforeseen happening in the course of governance on Polkadot. However, the presence of ***a governance process*** still gives me reasons to stay positive, because whatever happens, DOT holders can collectively decide on the preferable course of action for the network. And if a proposed upgrade splits the community in two and we reach a stalemate, then we will have a true test of the resilience of the network.

All in all, Polkadot's on-chain governance is one of the most robust in the space because it incorporates political science, human psychology, and economic theory into its design and implementation. One major caveat is that everything I have written so far is subject to change because things move really fast in the Polkadot ecosystem and pretty much every system parameter can be adjusted by participants. This is a good thing because if the wrong assumptions have been made at the design stage, these can be corrected in the next version of the system. Only time can reveal what our mistakes have been, and so it makes sense to give ourselves the opportunity to observe and reflect in the meantime.

A New Kind of Treasury

One of the advantages of an on-chain governance process is that the community can make the most of the protocol's treasury. In Polkadot, the on-chain treasury is managed by the Council and its sole purpose is to foster the maintenance and growth of the ecosystem. It achieves this goal through various components:

Bounties

There are practical limits to the curation capabilities of Council members when it comes to treasury proposals. It is highly unlikely that Council members will always have the expertise to make proper assessments of the activities described in all proposals, so there needs to be a way for Council to delegate the supervision of proposals to experts.

A Bounty is a reward for a specified body of work - or specified set of objectives - that needs to be executed for a predefined treasury amount to be paid out. It can be initiated by any DOT holder, who is called a proposer. Once the proposer has proposed a bounty, then the burden of project execution and verification will rest on a bounty Curator. The bounty curator can be defined as a person or group of people with agency over a limited portion of the Treasury to be used for a specific purpose. This can be for fixing a bug or vulnerability, developing a strategy, or monitoring a set of tasks that benefit the Polkadot ecosystem.

Curators are selected by the Council after the bounty proposal is passed. Before they are approved, curators need to make a deposit to accept their new role, so that the funds can be withheld to punish them if they act maliciously. However, if they are successful in their task of getting someone to complete the bounty, they will receive their deposit back as well as the bounty reward.

((INSERT IMAGE)) of the bounty process

Spending Proposals

Whereas bounties define specific tasks to be completed, the spending proposal is more open-ended. A proposal can be geared towards building infrastructure, educating the community, building a new project, creating tools, or marketing the ecosystem. To date, over 100 independent proposals have been funded by the Polkadot Treasury, including the creation of this book. The primary difference between a spending proposal and a bounty is that the proposal in question will be executed by its proposer.

Tips

This is a way for community members to reward other community members for their efforts towards maintaining and growing the ecosystem. Any DOT holder can request a tip for any member who has done something worthy to be relayed. For example, I was once nominated by a community member for an article I wrote on Polkadot governance

Funding the Treasury

The Treasury's funds come from different sources:

1. **Slashing:** When a validator is slashed for any reason, the slashed amount is sent to the Treasury with a reward going to the entity that reported the validator, often another validator. The reward is taken from the slash amount and will vary depending on the nature of the offence and the number of reporters.
2. **Transaction Fees:** A portion of each block's transaction fees goes to the Treasury, with the remainder going to the block author.

3. **Staking Inefficiency:** Inflation is designed to be 10% in the first year, and the ideal staking rate is set at 50% of the total supply. This means that half of all tokens in existence should ideally be locked in staking for the inflation to go entirely to validators as a reward. If the staking rate falls below 50%, then the validators will receive a lesser amount, with the remainder going to the Treasury.

4. **Parathreads:** Parathreads participate in a per-block auction for block inclusion. Part of their bid amount goes to the validator that accepts the block and the remainder goes to the Treasury.

   For more details on the Treasury, you can read this Polkadot wiki article.

Chapter 5

Expanding the Network

Having seen how the network is structured, we are now going to look at how the network is expanding through parachains, the ultimate value-proposition of Polkadot. Without parachains, the relay chain is just a skeleton network limited to staking and governance functionalities. By contrast, parachains can be designed however the building teams want: with or without transaction fees, bigger or smaller blocks. In short, each parachain is a country of its own. And you can think of the relay chain as the network that maintains the roads and sea routes that connect each of these various countries.

Each parachain is also a very customisable layer-1 blockchain that can fall into the following categories:

- Public Layer-1 Network
- Private Layer-1 Network
- Layer-2 Scaling Solution
- Bridge

This is possible because the relay chain makes no assumptions about the entities that connect to it. It accepts them as they are, so long as they are built using programming languages supported by Substrate. Substrate is a framework for building modern blockchains created by Parity Technologies, the company that was commissioned to build Polkadot by the W3F. Thus any blockchain or network built with Substrate is compatible with the Polkadot relay chain.

But really, what is a parachain? What does it mean to be one? Parachains are like children of a relay chain in that they are secured by the economic power of their parent relay chain and are also able to use the computing resources of relay chain validators for cross-chain operations. The advantages of parachains over standard layer-1 blockchains are two-fold:

- Shared security
- Interoperability

The concept of shared security should be understood by now, so we can now focus on interoperability, which is seen as the holy grail of blockchain technology.

Parachain Interoperability

I believe that interoperability is Polkadot's killer feature. If you are unfamiliar with blockchain, then this might not make much sense to you, but I'll try to explain why parachain interoperability is the key to unlimited innovation within the blockchain space.

Decentralized finance and decentralized digital ownership (via NFTs) became the powerhouses that they are today thanks to interoperability, the trustless communication between different automated systems/networks. Usually, blockchain platforms are said to be interoperable, when tokens from one platform can be moved onto another, and vice versa, through a bridge.

For example, if I want to send Bitcoin to Ethereum, all I need do is go to the bridge's application and make the transfer. This is now a pretty straightforward operation that can be completed in a few clicks. What I don't see is that the tokens I moved from Bitcoin to Ethereum are technically still on the Bitcoin network. This is because the bridge's method of transfer is tofreeze my BTC tokens by sending them to a special-purpose address on the Bitcoin network, mint a new set of derivative tokens called "wrapped BTC" on the Ethereum network,and send the wrapped BTC tokens to my Ethereum account.

Like I said, this is a straightforward process, but it isn't interoperability as implemented on Polkadot.

There are two aspects to interoperability:

1. Sending tokens and messages
2. Calling functions

Nowadays, the first aspect is pretty trivial, but the second is relatively unheard of. For blockchain

A to call a function of blockchain B, we would need to automate operations between blockchain A and blockchain B, thus eliminating the need for human intermediaries. In such a setup, blockchain A would call a smart contract on blockchain B, which will in turn respond to blockchain A, giving it whatever information or running whatever computation was requested. Inter-operability!

Let's use another practical example to make sense of this concept.

A user requests to use his valuable NFT stored on chain B as collateral on chain A, a

DeFi-focused chain, to take a loan. But before chain A can accept this loan request, it needs to confirm a few things:

1. Is the user who he says he is?
2. Does the user own the NFT?
3. What's the true value of the NFT?

Apart from these questions, chain A also needs to:

1. Mint an NFT to represent the loan position
2. Send tokens to Chain B

To gather all this data, Chain A will need to talk to other chains.

- To know the real identity of the user, Chain A talks to identity Chain C, which verifies that the user is truly who he says he is and that he's eligible for the loan.

- To confirm that this user has no outstanding loans, CChain A does cross-checks with two other DeFi chains that are its partners.
- To check that the user actually owns this NFT, Chain A moves on to verify the information with Chain B.
- To assess the value of this NFT and confirm if the collateralisation ratios are suitable, Chain A initiates a smart contract on Chain D, a prediction chain. This prediction chain incentivizes its set of predictors and assessors to analyze the true value of the NFT.
- Having confirmed that all is well, Chain A proceeds to collect the NFT and lock it in its NFT vault on Chain B, while it gives the user the tokens requested and starts collecting interest rate repayments.

Note that I've added more steps than are necessary for such a transaction for descriptive purposes only.

Thus, we see that there are two kinds of interoperability—strong and weak. With weak interoperability, the user has to do all of these operations in isolation, signing multiple transactions on different chains. With strong interoperability, one chain can leverage cross-chain features—identity, prediction, and vaults from other chains to secure its operations and provide a better user experience.

Now, given the strong advantages that parachains have over other layer-1 blockchains, we can now begin to understand why there is going to be intense competition for parachain slots. Since the relay chain can't have an infinite number of parachains–its resources are finite–it will support around 100 parachains within the next decade or so, according to the Polkadot whitepaper. But this presents a new challenge: how do we determine who gets a parachain slot?

Parachain Slot Auctions & Crowdloans

In a situation where a few valuable items are available for sale but there is a great demand from buyers, the most sensible way to distribute these is through auctions, because this guarantees that those who value them the most will be final takers. For Polkadot, a decentralized system with technological and economic security, finding the best way to distribute its precious network resources is paramount. This is when the parachain slot auctions (PSA) come in. The PSAs are a robust mechanism that help allocate parachain slots to the highest bidder amongst different projects. The full details of how it achieves this are summarized below.

Every parachain slot auction lasts 1 week on Polkadot. During this week, parachain teams make their bids. At the expiration of the auction period, a winner is determined. However, the actual procedures are a bit more complex.

Each week of parachain slot auctions is divided into 2 phases: an opening phase and a closing phase. The two phases are necessary because Polkadot uses a novel on-chain mechanism inspired by "candle auctions". Traditionally, running an auction involves setting a timer and allowing the highest bidder to emerge once time runs out: this is similar to what you can see on Ebay. However, since Polkadot works to maximize the economic security of its own network, this style of auction presents a major problem because it doesn't incentivize bidders to make their best bids early, leaving the system exposed to auction sniping.

For example, Bob wants to bid for a painting with $40,000 but decides to start out at $15,000 to feel the market. When his bid is overtaken, he adds an extra $500 and bids again. But his bid is overtaken once again, so he has to keep bidding up, on and on, until the timer reaches the last 3 seconds, with Bob winning at $28,000. Unfortunately, at the last second, Alice snips Bob's bid with her own $28,500 bid and Bob loses out on the auction. But the real tragedy is that the artist loses out on a larger valuation for the painting, given that $28,500 is much

lower than Bob's actual budget of $40,000. To discourage such actions, the "candle auction" was invented around the 17-18th century. It introduced some randomness and uncertainty in the final stage of an auction: participants were encouraged to place their best bids early because, although they could tell the starting point of the auction, i.e. when the candle is lit, they could never guess when the candle will die out signalling the end of the auction.

Now, implementing the candle auction on a blockchain is not a trivial affair because blockchains are not built for randomness. Polkadot's solution is to introduce two-phase auctions and a "retroactive random end time" which comes into play during the second phase of the auctions.

In the opening phase, which lasts 2 days, projects place bids that are registered on-chain and will run until the end of the auction. They are free to bid as much as they think is needed to win, but must also be careful not to break their own treasuries. In the ending phase, which lasts 5 days, all bids from the final day(s) can potentially be invalidated because the relay chain will use a verifiable random function to retroactively choose the moment when the auction ended. Therefore, it is the parachain candidate that has the highest bid at the exact time when the auction ends that will be the winner. So it is possible for the relay chain to decide that the auction ended on the 3rd day on block #123456. This means that a parachain candidate which made the highest bid after block #123456 will definitely lose the auction. This is why the opening phase is important because the relay chain will always consider all bids placed in the opening phase.

A parachain slot can range from 3 months to 2 years on Polkadot (1 year on Kusama), depending on the number of slot periods that the team chooses for its project. This introduces another interesting dynamic to the auctions because the relay chain now needs to consider the following requirements when selecting a winner:

- Maximize economic revenue (get the teams to bid as many DOTs or KSM as possible)
- Maximize slot duration (get the teams to bid for as many slot periods as possible)

This means that a parachain candidate that has the highest overall bid but for the shortest available slot duration will be less favorable in the eyes of the relay chain compared to the parachain candidate that has the second highest overall bid for the longest available slot durations. However, note that a slot duration is also dependent on the slot periods that are available at the time the project needs them; and so this ideal scenario may not always play out.

Getting a parachain slot can be a very costly affair. The first parachain slot on Kusama went for 500,000KSM (~$90 million), which isn't ideal for decentralization because very few teams can realistically afford to spend that much in digital rent. To level the playing field, Polkadot has put in place a crowdloan module that enables parachain teams to source DOTs from their communities. This is akin to a funding round, with a few notable differences:

- The tokens bonded by the community aren't given to the parachain teams. Instead, they are held by the relay chain. Think of it as staking without earning staking rewards.
- If the team doesn't win the auction, the tokens are refunded to the contributors.
- If the team wins the auction, the tokens are bonded on the relay chain for the duration of the rent. At the end of this rent period, the tokens are returned to the crowdloan contributors.

To encourage community members to contribute to their crowdloan during parachain slot auctions, parachain candidate teams often offer contributors a share of the supply of their native token, along with other perks like NFTs, derivative tokens, bonus staking rates, and special community roles. For community members, this becomes a win-win scenario, with the only loss incurred being staking rewards,

as tokens used for parachain crowdloans and auctions aren't eligible for staking rewards.

When we put the candle auction mechanism and the crowdloan module together, we begin to see that Polkadot is poised for an unprecedented spur of innovation and expansion. I say this for the following reasons:

1. Parachain slots have to be won with the help of the community, which guarantees that the "best teams" will rise to the top first. By "best teams", I mean the teams that can deliver on both technology and community engagement. Because it is possible for the best tech teams to be overshadowed by weaker tech teams who have a firmer grasp of community building.

2. Parachain slots have to be renewed eventually, which guarantees that teams will focus on delivering better services to their community and growing their treasuries to overcome the reliance on crowdloans. Naturally, some projects will be unable to renew their parachain slot, and this is both good and bad. Bad for the parachain that reduces or stops its services; good for the ecosystem because it will ensure that no parachains have a permanent slot unless they generate the value needed to keep them going.

Another exciting aspect of this design is the diversity of parachain projects. For example, if there are 3 DeFi chains that are competing, it is unlikely that they will all be successful. Instead, only 2 might get a slot by generating enough revenue and community goodwill. In this case, the third parachain will be downgraded to a parathread, while other non-DeFi projects continue to operate on the network. Note that this is only theoretical speculation: the point I'm driving at is that this design encourages diversification among parachain candidates.

A Short Take on Parathreads

Given that parachain slots are finite, not every candidate will successfully attain the parachain status. Also, becoming a parachain may not necessarily be suitable for some projects. Seeing as parachains are desirable because they have uninterrupted access to the relay chain and are able to submit blocks whenever they want, projects that do not require such resources are better off becoming a parathread. You can think of parachains as a subscription service while parathreads are pay-as-you-go.

In the context of Polkadot, this model is ideal for two reasons:

- It is easy for projects to wind down their parachain operations since they don't have to completely lose their connection to the relay chain.
- It is possible for projects that are unable to acquire a parachain slot to still benefit from Polkadot's shared security.

How Parathreads will Operate

Some of the parachain slots on the relay chain will be reserved for parathread execution. These special slots called "parathread pools" will host projects that wish to become parathreads. To add a block onto the relay chain, these parathreads will send their block candidate and a transaction fee to a collator located within the parathread pool who will, in turn, relay it along with a bid designated in DOT.

A relay chain validator will review the bids, and decide which block to include in the relay chain. The primary incentive for relay chain validators is to accept block candidates submitted with the highest bids, generating the most profit for themselves. According to the Polkadot Wiki, "*the tokens from the parathread bids will likely be split 80-20, meaning that 80% goes into Polkadot treasury and 20% goes to the block author. This is the same split that applies also to transaction fees and, like many other parameters in Polkadot, can be changed through a governance mechanism.*"

A Brief Overview of Interesting Parachain Candidates (Sept., 2021)

1. Acala - DeFi

Acala is a first-of-its-kind decentralized finance consortium with a vision to create cross-chain open finance infrastructure for the Polkadot ecosystem. Its mission is to become the DeFi hub of Polkadot to make it easy to use or build financial applications, improve trading efficiency, and save valuable time. This means that Acala has the same mission as Ethereum, the only difference being that it was built specifically for DeFi use cases, making it far more convenient for DeFi services. The platform offers a suite of core protocols that make it a worthy destination for any DeFi dApp developer and user.

a) Honzon Protocol (aUSD)

This is the protocol behind Acala's aUSD, which is a decentralized, multi-collateralized stablecoin that is backed by cross-chain assets. By contrast, USDT, the biggest stablecoin by market capitalization, is a centralized stablecoin that is under the control of a single agent. The widely-adopted DAI, a decentralized stablecoin, is currently limited by the fact that there's only one type of collateral that can be used to mint it i.e. ETH. This explains why DAI has a much lower market capitalization in comparison to USDT. Thus, aUSD seeks to offer the best of both worlds and avoid the limitations of popular stablecoins. Furthermore, it can be minted from a variety of collaterals which include DOT, ETH, BTC, KSM, and any other token whitelisted through Acala's governance.

b) Homa Protocol (LDOT)

The Homa protocol is a decentralized staking protocol that enables users to get the benefits of staking their DOT without losing their access to their liquidity. So instead of staking their DOTs on the Polkadot relay chain, users can use the homa protocol on the Acala dApp and receive LDOTs in return,

although not necessarily at a one-to-one ratio. LDOT stands for liquid DOT, which users are free to use as collateral to take out stablecoin loans, for transfers, or swaps. When users want to redeem their staked DOTs, they can simply return the LDOT to the protocol and get their DOT plus their staking rewards refunded into their wallet immediately, thus avoiding the relay chain's 28-day unbonding period.

c) Decentralized Exchange

This is a protocol similar to Uniswap, Sushiswap, and other decentralized exchanges that enable users to swap tokens, provide liquidity, and earn rewards.

Acala's goal is to make DeFi accessible to everyone without all the complexities that come with decentralized protocols. Already, they have a partnership with *Current*, an American fintech company, which will help create a new type of finance called "Hybrid Finance" (a blend of decentralized and centralized finance). Meaning it will be possible for users who don't have a crypto wallet to earn yields in DeFi from their traditional bank accounts.

2. HydraDX - DeFi

HydraDX, another DeFi-focused layer-1 blockchain, is very different from Acala. A core part of HydraDX's offering is the "Omnipool", a "well of liquidity" that is deep and diversified enough to withstand anything the market throws at it. Presently, most token trading is carried out in pairs, such that if I wanted to swap DOT for KSM, I would need to find an exchange that has a DOT/KSM pair. Only then would I be able to swap from DOT to KSM. If no such pool exists in the exchange, then I'd be forced to swap DOT into a token that is paired to KSM. Say, for instance, I find a DOT/USDT pair and a KSM/USDT pair, I will have to swap my DOT for USDT before swapping USDT for KSM. This is neither capital efficient nor user friendly. Even when decentralized exchanges like Uniswap propose swaps between two tokens that are not paired

in a pool, they do so by automatically swapping from one pool to the next, which causes a lot of slippage.

Thanks to Substrate's power and flexibility, HydraDX is overcoming this limitation by building a single pool (Omnipool) for every asset. The details of this execution are quite technical, both in terms of finance and technology, but I'll give a basic summary here. To create an Omnipool, HydraDX uses the LRNA token as the base token against which all other tokens will trade, so that the LRNA token can act as a price oracle. Given that HydraDX is a layer-1, its Omnipool is not all it has to offer: rather, it is the building block upon which many more financial applications will be stacked.

3. KILT - Identity

For a long time, our data, particularly data which identifies us, has been used to entrap, manipulate, and take advantage of us. KILT is looking to challenge this state of things by decentralizing the process of attesting and verifying users 'credentials.

KILT is an open-source blockchain identity protocol for issuing self-sovereign, anonymous and verifiable credentials. KILT enables innovative business models around identity and privacy, addressing the need for reliable identity solutions in the digital world. It allows users to claim personal attributes, have them attested by trusted entities, and store the claims as self-sovereign credentials.

At the core of their model is the idea that users should have full ownership and rights over their credentials, so that only they can make use of their identity information when interacting with another party. Within their protocol, there are those who need credentials issued (like job applicants), and those who need to verify credentials (like hiring companies).

Once the KILT blockchain is fully set and running, it will be possible to prove to a company that wants to hire you that you are who you claim to be. This will be possible because the company will only need to

check the information you provide them on the KILT blockchain. If they need further verification, they can then pay an attestor to verify your credentials.

Again, this is the basic idea. But remember that this is a layer-1 blockchain and that many more ID applications can be built on it.

4. Robonomics - IoT

In my opinion, this is the most interesting parachain candidate in DotSama. I say this because they are building something that no one else has proposed—robot economics. Core to their idea is the realization that with the rise of automation (autonomous robots), there comes the need for a framework to manage robot-to-robot interactions. For example, there are usually a pool of robots and machines working together to manufacture products in factories, but humans are still needed to facilitate operations between said robots.

For example, when an item has completed a cycle on one line, a human is almost always needed to move it to the next line to continue the manufacturing procedure. In this case, a human is only needed because there is no way for the robots to talk to themselves and coordinate their actions independently.

By adding an automated line of communication in robot interactions, a whole new world of possibilities is opened to us: robot economics. With Robonomics, it will be possible for a factory robot to instruct an automated vehicle, so that when the products are ready, the factory robot can ping the automated vehicle to come for pickup. To avoid robot spamming, the transportation robot will only react to the factory robot's call if the factory robot has paid some tokens to the transportation robot.

For better clarity, the word "robot" does not necessarily refer to humanoid machinery. Any automated machine is a robot: a printer, a coffee machine, a computer program sitting in a truck, a trading bot. They are robots because they are designed to perform a certain set of

actions automatically having received a certain input. Robonomics is highly interesting because the project wants to link the economics of the digital world and the real world through “robots”, just like fiat and cryptos finances are linked through “oracles”.

5. Phala - Privacy

Phala tackles the issue of trust in the computation cloud. Phala’s layer-1 blockchain is a trustless computation platform that enables massive cloud processing without sacrificing data confidentiality. In layman terms, Phala is building a decentralized and private cloud through a network of PCs brought together via blockchain consensus. Phala wants to make permissioned/Web2 cloud services like Google Drive, One Drive, Adobe Cloud, Azure, and AWS redundant. Phala is committed to providing a universal decentralized computing network that can be freely combined with smart contracts, decentralized storage protocols, and data indexing services.

One of Phala’s novel products is the *Fat Contract*, an intended upgrade on the current smart contract model made possible by the power and flexibility of Substrate, the framework used to build Polkadot and its parachains. Traditionally, smart contracts execute their code on-chain, meaning that the blockchain network is responsible for carrying out the computation of the smart contract along with consensus. But this limits the power of smart contracts because they are bound by the computational ability of the network (i.e block production, finality, etc). By decoupling the execution of a smart contract from blockchain consensus, a more powerful smart contract is created.

A Fat Contract is simply a smart contract that handles its computation off-chain. This is coupled with Phala’s privacy-preserving feature that ensures that computational data cannot be read by miners. The main appeal of Fat Contracts is that they enable a much richer and powerful use of smart contracts for a wider range of services, particularly those that require a lot of processing power and speed, like gaming, metaverse, and data analysis to name a few.

6. Crust - Data

The cloud has been a great addition to our lives: we no longer need to store all our digital files on personal devices with limited disk space. However, the data you store on centralized cloud servers doesn't fully belong to you, and you can't be certain that your data will always be safe and accessible. By contrast, a decentralized cloud has the advantage of not relying on one single cloud or hosting service.

Crust is providing a straightforward decentralized cloud storage solution for everyday users, professionals, and developers. With Crust, your data is stored on multiple nodes across the world, ensuring that you can retrieve this data anywhere and anytime. Furthermore, any data stored is fully owned and can only be accessed by you. This is because Crust makes use of advanced data encryption before sending it to its nodes. All in all, Crust is looking to challenge every centralized cloud storage service currently in operation—Google, Dropbox, Box, etc.

7. Zeitgeist - Futarchy

Zeitgeist is a layer-1 blockchain that proposes some of the most original ideas in the Polkadot ecosystem. Democracy is an ideal form of governance, but it has many drawbacks when it comes to models for decision-making.

Currently, there are vast differences in wealth among nations which cannot be attributed to differences in natural resources or human abilities. In truth, the heart of these inequalities lies in the fact that nations, many of which are democracies, often adopt ineffective policies. Futarchy presents itself as a new form of government and wants to alter the way decisions are made by using the outcomes of a prediction market.

The core argument for Futarchy is that markets tend to be more rational and can be used as a standalone form of governance. Zeitgeist provides a layer-1 blockchain that enables anyone to create

a prediction market to measure people's opinions on any topic, thus supporting policy-making for companies, governments, blockchain communities, DAOs, and other organizations. With Futarchy, decisions won't be made based on free-floating opinions, but weighted bets whereby people are forced to "put [their] money where [their] mouth is".

And so, it is expected that people will be more careful and honest with their opinions when there is a cost attached to voicing it. One can imagine a future where the members of parliament come to a decision based on how they placed their bet. Let's look at the following question: "Will reducing taxes create more economic progress?" In a democracy, all members would vote based on their or other people's opinions; meanwhile, Futarchy requires all members to take a financial position on whether lowering taxes will lead to economic progress or not. Those with the strongest conviction will likely put more money on the line and indirectly influence the outcome of the vote.

Who would you go with: the people who have enough faith in their opinion to take the risk of making a big bet or those who aren't brave enough to back their opinion with sufficient funds?

But it is not all sunshine and rainbows. There are some potential downsides to the Futarchy model. Some people will inevitably get distracted by the gaming/betting/risk-taking part of Futarchy to mint money and social influence i.e the Crypto Twitter phenomenon where 'big 'accounts use their influence to pump the price of tokens that are not worth their market cap. It is also expected that people could end up following hypes and big bets without ever forming an opinion of their own, which would be 100 times worse than democracy where apathetic individuals don't bother to vote because of a lack of "incentive". Thus, Futarchy is decentralized enough to attract a wider array of participants, but there is also a "gambling" effect that undermines the relevance of the bets. Only in implementation can we

see how it will unfold, and that is why I'm excited about the future of Zeitgeist.

8. Moonbeam - Smart Contracts

Moonbeam is an Ethereum-compatible smart contract platform on the Polkadot network that allows developers to deploy existing Solidity smart contracts and DApp frontends with minimal changes to the original code. After the successful launch of their canary network on Kusama (Moonriver), some people have dubbed the platform "Ethereum 3.0".

Asides from the appreciation in the value of MOVR tokens that'll no doubt accompany this appellation, the tag isn't entirely undeserved. For one thing, Moonbeam's smooth integration of native Ethereum tools makes it an easy destination for all Ethereum dApps; this way, developers can build richer dApps that don't suffer from the limitations of the Ethereum blockchain—unreasonable gas fees, lack of modularity, etc.

These are just a few of the many parachain candidates building on Polkadot. Below are the links to some useful resources on ecosystem projects:

- https://parachains.info/
- https://dotmarketcap.com/
- https://polkaproject.com/

An important point to note is that most of these projects are only registered as parathreads. Until a project is plugged into the relay chain after winning a parachain slot auction, it remains a parachain candidate.

At the beginning of this book, it may have been difficult for you to imagine why we would need a variety of blockchains. I hope that this section has been successful in convincing you that the future is truly multi-chain. If anything, I hope you have gained a greater appreciation for the infinite versatility of a layer-0 protocol like Polkadot that aims

to support the exponential innovation on which future layer-1 developments can thrive.

There are far too many unresolved problems for humanity and the planet as a whole, and the goal of every technology should be to make life better. Not life in the narrow sense of the word that only takes humanity into account–that's the kind of thinking that led us to the present climate crisis. Life, as I use it here, refers to plants, animals, the atmosphere, and everything we can't do without. The aspirations of decentralized networks and organizations are that people can become more receptive to global issues over time: respect life, promote freedom, peace and fairness, and bring human prosperity. If they can't do this in the long run, they are doomed to repeat the mistakes made in Web 2.0.

Chapter 6

Participating in the Network

At this point in the book, you have already learned a great deal about Polkadot. But knowledge for knowledge's sake doesn't bring any value: it is in application that knowledge gains its value. This book was written to present Polkadot in an approachable way, so that more people can become aware of the wonders and possibilities of this decentralized network. But that is only half of the story. The more pertinent reason why this book was written was to recruit new builders and ambassadors for the ecosystem, because a network is only as good as its participants.

If you are excited or inspired by the opportunities emerging in the Polkadot ecosystem, this short chapter cordially invites you to participate in the network.

Here are some reasons why you might want to participate in Polkadot:

- It is truly decentralized.
- It is future-proof thanks to forkless upgrades and on-chain governance.
- It has a vibrant and passionate community.
- It can accommodate the wildest ideas with its scalability.
- It aligns with universal values like freedom from discrimination and censorship.

- It is a portal to a boundless *Paraverse* of layer-1s, layer 2s, smart contracts, dApps, bridges, and many other novel protocols.

Thus, by building or participating in Polkadot, you are placed at the forefront and center of Web3 innovation. Now that you are sold on the idea of participating, let's consider how it works in practice.

How to Participate in the Network

In this subsection, we will go over what your options are in terms of participation.

Security

A decentralized network is only valuable as long as it remains secure, and so the most obvious way to participate in the network is to contribute to its security. Luckily, Polkadot is a nominated proof-of-stake network which gives the average person a chance to join as network maintainers.

There are four distinct roles available here:

1. **Become a validator - T**his requires some equipment and technical know-how. By becoming a validator, you will be verifying transactions and producing blocks.
2. **Become a collator - W**hile validators secure the relay chain, collators secure the parachains and parathreads. You can become a collator for your favorite parachain.
3. **Become a nominator -** If you have DOT tokens, you can simply stake them with validators to earn rewards. There are different wallets and extensions you can use for this purpose (see the recommendations below).
4. **Become a crowd loaner -** You can lock your DOT to help a parachain secure a parachain slot on the relay chain for a fixed duration. This will allow you to get native tokens from the

parachains, which is an added incentive for portfolio diversification.

All the above operations can be completed through Polkadot-js extension and Apps, the official web interfaces for the network. However, most non-technical users will need more beginner friendly alternatives.

Some Wallet Recommendations for Staking and Crowdloaning

1. Talisman wallet and extension (my personal recommendation)
2. Fearless mobile wallet
3. Nova mobile wallet
4. Polkawallet
5. Mathwallet

A Brief Note against Centralized Exchanges

Although you can stake your DOTs and participate in Polkadot crowdloans through centralized exchanges like Binance, Kraken, and Coinbase, I have intentionally left them out of my list of wallet recommendations. This is because using centralized exchanges for on-chain operations goes against the idea of decentralization: when you stake or contribute to crowdloans through these exchanges, you effectively forfeit the ownership of your tokens to the exchange. This can become a problem in the long run because:

1. A centralized exchange can use your tokens, as well as those of other users, to participate in governance and vote for proposals that you don't support.
2. A centralized exchange can get hacked and its validators can get slashed, which places a greater portion of network participants at risk.

Staking and crowdloaning through the wallets I recommended ensures that your on-chain actions are always tied to an account that is under your custody, as opposed to transferring your rights to on-chain participation to an account that is controlled by a third-party business.

Governance

Governance remains the least popular feature of decentralized networks, with most referenda failing to get a 10% voter turnout. Therefore, your participation in governance activities would be giving the network a new lease of life. Below are some ideas:

1. Run for Council
2. Vote for Council candidates and runners-up
3. Propose or second proposals
4. Vote on referenda
5. Submit tips for ecosystem builders and ambassadors
6. Join discussions on Polkassembly, Element, Discord, and Reddit

You can find more details on these processes in the Polkadot wiki.

Ecosystem Growth

If neither securing nor governing the network appeals to you, you can consider becoming a builder or an ambassador.

Builder

A builder is an individual or a group of individuals that are working on deploying parachains, runtime pallets, smart contracts, dApps, and developer tools. As a builder, you can get funding by applying for grants from the Web3 Foundation or by submitting spending proposals to the on-chain treasury. You can also get into the Substrate Builders Program, a program that identifies, supports, and mentors current and potential Substrate-related projects.

Ambassador

This role isn't to be confused with the position offered as part of the Polkadot ambassador program, which you can join by filling out an application form here. The main responsibility/duty of an ambassador is to help drive the growth and adoption of the network. This can be done in as many ways as the mind can find, the most important thing being the end goal. For example, writing a book or blog is a worthy task for this purpose, but so is recording a webinar, composing a song, hosting a meetup, creating an audio-visual explainer, etc. Again, your imagination is the limit. If you have a project that you believe the ecosystem will benefit from, you can apply for funding from the on-chain treasury through the procedure outlined here. For context, this book was an original idea made possible by the funds received from Polkadot's on-chain treasury.

Keeping Up with the Ecosystem

The first step you can take towards participating in the network is to stay up-to-date with the happenings of the ecosystem. Below are the links to some important resources that will help you keep track of ecosystem developments.

1. **DotLeap**

   This is a weekly newsletter run by me and Bruno Škvorc. It focuses on publishing the most note-worthy updates of the DotSama (Polkadot + Kusama) ecosystem, covering news from relay chains, parachains, dApps, parathreads, communities, and much more. It is a truly comprehensive overview of the ecosystem that is published on Substack and Subsocial every week. Subscribe here for updates.

2. **Parachains.info**

   This is the cleanest and most comprehensive website I have come across for all things DotSama. It presents information on crowdloans, auctions, and parachain projects—including

token supply & price, investors, roadmap progress, Web3 Foundation grant status, and more. It also has a news tab that aggregates news from official parachain projects. This is another community-led project that has been funded by the on-chain treasury.

3. **Dotmarketcap**

   This website is similar to parachains.info in the sense that it aggregates information about Polkadot ecosystem projects, parachain candidates and auctions. It provides a list of tradable projects ranked by market cap and some valuable insights. Its biggest advantage is that all information on token prices and crowdloans is updated instantaneously and that you can use the website to track a selection of projects that interest you.

4. **NFT Review**

   This is another weekly newsletter run by **gbaci** (me) and Bruno Škvorc, with a strong focus on NFTs and the metaverse. It has the benefit of covering NFT news from DotSama and the rest of the web3 space and is available for subscription here.

5. **Polkadot Blog**

   This is the official blog run and maintained by the Web3 Foundation. Updates are not frequent and so it is advised that you subscribe to the blog. Naturally, if you are subscribed to DotLeap, you'll receive an update on the newest blog articles whenever they are published.

6. **Polkadot Daily Digest**

   The daily digest is written almost every day by Bill Laboon, Director of Education and Community at Web3 Foundation. The digest includes important Polkadot and Kusama updates on the relay chain, governance, and community discussions. You can find it on r/Polkadot and Subsocial.

7. **dotTreasury**

   This is a great website for finding information on the Polkadot treasury. It gives information on treasury reserves, income, expenses, and other treasury-related information.

8. **Polkadot A to Z**

   This is an educational series by Emre Surmeli, Technical Educator at the Web3 Foundation. It provides core technical information about Polkadot and Substrate technologies one concept at a time. The content is presented in a short digestible format and currently lives on Reddit.

9. **Guide to Polkadot-JS**

   This is a very comprehensive presentation of the functionalities of Polkadot-JS Apps and Extension created by Anaelle LTD, a community member. It provides step-by-step instructions to make wallet operations accessible to beginners and is available on this website.

10. **Ser, Have ya 'Heard?**

    This is an educational series of daily videos by Jay Chrawnna, a community member. It breaks down and discusses the latest news and developments in the DotSama ecosystem in a very entertaining format for the general audience. It is currently hosted on Youtube.

And that's all, folks! Welcome to the Paraverse.

Technical Appendix

A BABE and a GRANDPA

(Kindly note that, owing to Polkadot's forkless upgradability feature, this consensus mechanism is subject to change in future).

Before I talk about BABE and GRANDPA, I need to explain something about computer protocols.

First, always remember that a blockchain is a protocol. But what is a protocol? A protocol is a set of instructions that a computer software operates with. It is possible to trust a protocol because its rules are clear from the beginning. You can think of a protocol as a set of automated actions that a computer takes.

Now, the vital thing you need to know about protocols is that a protocol can have many protocols and sub-protocols within it. Such that when we say a blockchain is a protocol, we really mean that a blockchain is a protocol of sub-protocols, with each sub-protocol equipped with the ability to have other sub-sub-protocols. Each sub-protocol and sub-sub-protocol is responsible for a specific task.

Thus, in the case of the Polkadot relay chain, which is in itself a protocol, there are various sub-protocols and sub-sub-protocols. This is why we have both BABE and GRANDPA as sub protocols of the relay chain protocol.

With this out of the way, we can now get introduced to BABE. To nerds who know how to read code, she's pretty sexy. But for us noobs, she's just a BABE, although a powerful one.

BABE - Blind Assignment for Block Extension

BABE is a sub-protocol in the relay chain that coordinates block production. To do this in a secure and decentralized manner, she uses a few cool tricks:

Blind Assignment aka Random Selection

The first trick up her sleeve is the process of blind assignment. There are two ways to determine which node gets to create the next block—randomly or deterministically. If a node knows ahead of time that it will provide x number of blocks, this node has enough time to create fake transactions for inclusion into these blocks. Thus, BABE chooses randomly. This way, the nodes do not know beforehand which blocks they will produce. The specific mechanism is too technical to explain in this book, just remember that our BABE selects nodes at random to produce blocks. Another reason why I don't want to go into more detail in this book is that a rumor has it that she is on her way out. It would be quite unfortunate to spend so much time breaking down her complexity only to have to make amendments less than a year later.

Multiple Assignments aka Creating Backups

To assure a greater level of decentralization, BABE gives different nodes the same block to produce. The purpose is to make block production competitive so that in the event conflict between different nodes about the validity of a block, all nodes can vote on which block is most likely valid according to predefined parameters—remember, it's a protocol.

Another good advantage of multiple assignments is that sometimes a node that was chosen to create a block may go offline or have other issues that prevent it from creating a block. When this happens, there will always be a secondary block produced on which the network can fall back. And so, for every block waiting to be created, there is a primary block producer as determined by BABE and several secondary block producers.

There are other sub protocols in BABE, but the ones I have listed are the most noteworthy. Any further information will only push us to dive deep into technical territory. For that, I recommend reading the following research paper on BABE.

GRANDPA - The Finality Gadget

Like BABE, GRANDPA is another sub protocol. But unlike the girl, he is focused on finality—verifying that blocks are valid and can't be reverted. In short, where BABE helps the network create blocks in a decentralized manner, GRANDPA helps to finalize blocks in a decentralized manner. It does this by running elections on all the various fork choices.

Because BABE selects different nodes to produce the same block, there is always a question of which block sequence is true. This is because BABE creates a few blocks and their associated forks before GRANDPA comes in. So GRANDPA's job is to decide which fork of the chain is the most valid.

You're probably wondering, "So Polkadot also has forks?!" Well, a more suitable term for these forks in our context would be "faux-forks" (false forks), because they are yet to be finalized. Once a fork is finalized, all the others are abandoned and every node on the network accepts GRANDPA's decision. But how does GRANDPA make his decision and how can we trust him? Well, for one thing, he's a protocol and so he only does what he has been instructed to do. I'll explain this point while avoiding as much technical details as I can.

When various forks arise on the chain, GRANDPA's decision as to which fork will become the finalized chain is guided by:

1. Its connection to the last finalized block - Any of the fork options coming from the last finalized block by GRANDPA is considered valid enough to remain an option.

2. Its number of primary blocks - Any of the fork options with the highest number of primary blocks is given a higher weight. A

primary block is one that was created by the node considered as the primary node by BABE as at the time said block was in production. Remember that BABE chooses different nodes to create the same block, and that one node is always primary while the others are dubbed secondary.

Armed with these requirements, GRANDPA can choose whichever block most matches these finality criteria.

All in all, the main purpose of BABE and GRANDPA is to offer the relay chain a decentralized way to achieve consensus and finality i.e. security. More decentralization is always favored because it ensures that the network will be operating on shared truth and not on centralized falsehood. If all bad actors were to attempt to manipulate on-chain data, they would have a near impossible task to fulfil.

About the Author

gbaci is a writer, filmmaker, and musician who is passionate about decentralization and the DotSama ecosystem.

He began his deep-dive in blockchain technologies in December 2020 and has since become a Polkadot Ambassador, the Head content writer at RMRK, and the Co-editor of NFT Review and DotLeap–a weekly newsletter on all things Polkadot and Kusama.

gbaci believes that "RMRK will be the only NFT standard used by everyone." He produces music professionally under the moniker *Gillian Baci* and has released his music on *Singular* in the form of composable multimedia collections.

When he isn't talking crypto or composing music, **gbaci** writes novels and scripts, shoots movies, reads books, and plays with novel ideas on how to create lasting impact.

As a global citizen, he believes that everything is connected and that we are all one within our societies and the universe at large.

You can find him on Twitter under the handle **@gbaciX**.