

Polkadot: The Bedrock of the New Web



Cointelegraph
Research



Welcome to the Future

The presently established ways to conceptualize and build computer systems and human networks connected by software products are imperfect, to say the least, and have led to many complex problems. Some of these problems are purely software-driven, but others go deeper into the ways we self-organize as a society and cannot be reduced to just faulty infrastructure.

A cohort of newer developments in IT — blockchain networks being only a small part of that — has developed in the last decade and is now coming to conceptual and technological maturity. Polkadot and

its emerging ecosystem can be viewed as a forefront of that innovation, offering a robust toolset to rethink and rebuild both the software and some of the social dynamics that it facilitates. This innovation is not just about software or architectural principles or a group of overly enthusiastic developers. It's about a vision of a more secure, more stable and more efficient ecosystem driven by innovators and standing on a new kind of infrastructure.

This report builds a case for Polkadot and some of the hallmark projects it enables.

Research Partners

PNYX
ventures

 Polkadex.

 Polkastarter

 Moonbeam

 PHALA
NETWORK

 Zeitgeist

 Centrifuge

 Equilibrium

 DARWINIA

 subsocial

 DEPER


ocean

 CRUST

 Math Wallet

 Bit.Country

We thank our research partners for their support of this report.

Table of Contents

Introduction: Internet Without Fail	4
Technology	6
Architectural Overview	6
Polkadot Consensus	8
Parachains and Substrate	12
Cross-parachain Communication	14
Conclusion: Plug-In Blockchains	16
Interlude: Kusama, the Canary Network	18
Tokenomics	19
Introduction: Role of Tokenomics	19
One-Page Overview: The Token	20
Security: Proof-of-Polkadot	20
Ecosystem: Slot Auctions	21
Governance	25
Ecosystem	26
Introduction	26
Infrastructural Projects	28
Application-Layer Projects	36
Closing Notes	44
Authors and Contributors	45

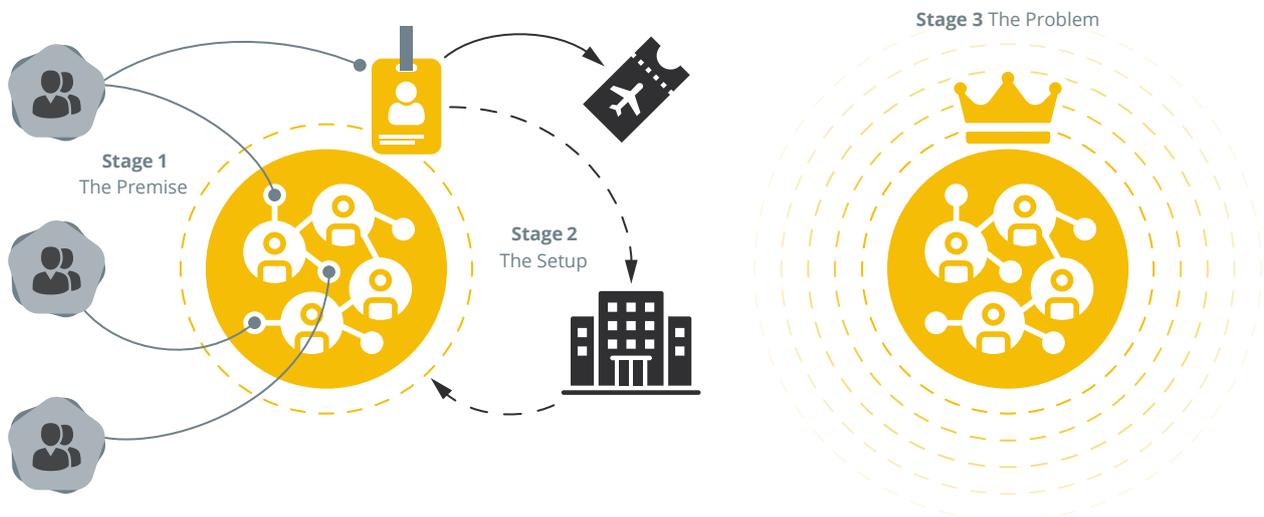
Introduction: Internet Without Fail

With the way our contemporary internet is built, power tends to accumulate in the hands of the few — not so much in the sense of a single small group having unlimited influence over everyone, but more as a “natural” emergence of local power clusters that become problematic later on. It usually has to do with a combination of two topics: *data* and *access control*.

Centralization of data. After a certain threshold, the accumulation of seemingly innocuous data by a company can lead to disproportionate knowledge about its existing or even potential customers. When enough data points are gathered, the company can employ cohort analysis at scale and also correlate disconnected anonymized observations. Together,

it allows the company to make inferences overstepping the bounds of what the user would be comfortable sharing. Furthermore, the marginal utility of additional data points is bigger at this large scale than for newcomer companies.

Centralization of access control. A company that offers electronic money accounts can become so deeply integrated with distribution platforms that it becomes irreplaceable — its clients cannot end the relationship with the company without also losing access to the distribution platforms, crippling the business. To top that off, the ability to freeze operating funds for a long time without recourse can be, and sometimes is, used disproportionately.



A new exciting social network attracts a great deal of users and becomes a central hub where “everyone” has an account.

The social network adds a Single Sign-On (SSO) service that other companies can use. It’s convenient for the user (fewer accounts), convenient for the other companies (streamlined user onboarding with much lower development costs), and is great for the social network.

In a while, several very distinct issues arise.

- The social network accumulates a lot of data about the user, potentially including usage patterns of the 3rd party companies using the SSO. The technical opportunity is tempting for the company.
- The user’s ability to access the 3rd party company via the SSO is contingent on her good standing with the social network. Losing vacation bookings and air tickets because of an unrelated (and even unwarranted) automated ban is not unheard of.
- The social network becomes too big too fail. And keeps accumulating distance with potential competitors.

These local power clusters have many ways of causing trouble — due to incentive misalignments, technological failure, institutional failure, hacker attacks — and any other number or combination of reasons. Developments across the software industry, such as mass migration to the cloud or the rise of software-as-a-service — sometimes amplify this dynamic further as control moves farther away from the user and the technological stacks get more complex, with subtle infrastructural dependencies being introduced along the way.

As an entrepreneurial developer in the existing environment, one has to encounter and successfully handle a number of challenges that could seem more of a historical artifact than anything else. A long evolution of a very complex system, which spans across hardware, software, programming languages and paradigms, finance, the legal world, etc., is bound to leave lots of redundancies and legacy components that could have turned out differently under different circumstances but are very hard to modernize or replace now.

Some of these legacy configurations are outlined below.

- **Cumbersome payment infrastructure.** Digital fiat money exists as a sequence of nested records:
 - User's balance is an IOU from their payment provider.
 - The balance the payment provider has with its bank indirectly represents the provider's IOUs to multiple users.
 - The bank itself aggregates its IOUs to its clients into an account with the central bank of the country.¹

This system is convenient in the sense that it scales rather well, but in exchange, it introduces high fees, long processing times (measured in days in some cases), and, most importantly, it gives to the banks unreasonable amounts of control over the funds of their users.

For an entrepreneur, this turns a deceptively simple use case of accepting funds in exchange for goods and services into a highly complex and nuanced endeavor.

- **Account-centered identification.** It is standard practice for an online service to ask a new user to create an account, and for the user to agree. The service requests and stores some data about the user (for instance, name and email). For the user,

this dynamic replicates with every counterparty, increasing the amount of work the user has to do. More importantly, the practice multiplies the amount of places that could leak the user's data if they get hacked. It also leads to the next point.

- **Ad-driven monetization and data hoarding.** Data has repeatedly been named the new oil in this century. While customer data can usually be leveraged in many ways to improve the quality of the goods or services being offered, the common denominator is always value for advertisement. One more random data point about a user may or may not improve the offering, but it will most likely contribute at least somewhat to ad efficiency. And thus, all market participants can get more value from their users if they *also* gather as much data as possible and use it or sell it to advertisers.
- **Service-side storage.** A flow for storing or sharing data that the user brought with them penetrates most digital encounters — email service, website hosting, photo and video sharing, items uploaded for cloud calculation, etc. The list can be long. Insofar as storage is held by the service, the data is always under threat that the company will delete it, lose it, leak it, or go out of business. Quite often, the service itself defines some kind of a new data archetype and then monopolizes not its ownership but the right to hold it. The user gets locked into the service, having part of their life held hostage without recourse.
- **Cloud services and subscription for software.** Several decades ago, most of the commercial software was treated as a good rather than a service: The customer would buy a distribution of a word processor or a graphics editor with a one-time payment and get a lifetime license for that version. Subscriptions dominated enterprise software and, sometimes, access to additional services. In 2021, the leading model for software distribution is subscription-based, and countless software startups have launched as web-first. The underlying reasons for that shift are plentiful, but it further amplifies to a great magnitude the shortcomings of three of the four previously mentioned configurations.

Polkadot is part of a bigger vision brought forward by the **Web3 Foundation**, a robust technological infrastructure powerful enough to underpin a digital environment built for decentralization.

¹ If the bank isn't registered in the country that runs that currency, this step is preceded with a similar relationship with a corresponding bank.

In the context of addressing the aforementioned legacy configurations, the driving values of the movement for decentralization, of which the Foundation is one of the central propellants, could be conceptualized as follows:

1. If a trust-sensitive system can be replaced with a mechanism that combines cryptography and strong economic incentives, it should.
2. Ownership (of both assets and data) should be direct and mediated by cryptography — not privileged third parties.
3. Behavior beneficial to the ecosystem should be rewarded economically. Harmful behavior should be defined in machine-verifiable terms and penalized on the protocol level, not by discretionary action. Systems and protocols should be designed with this principle at its core.
4. Whenever possible, human organizations and communities should be open-entry and open-exit, encouraging meritocracy and active participation while discouraging artificial power bottlenecks.
5. Infrastructure should be open and verifiable on every level. Otherwise, everything built on top of it will be poisoned with trust sensitivity, which was covered in the first principle.

At numerous technological junctions, the movement around and adjacent to the **Web3 Foundation** envisions and builds infrastructure that could be leveraged to avoid entirely having to deal with every legacy configuration mentioned above. This is a monumental effort, but the internet of old wasn't built in one day — nor will the Internet Without Fail.

Technology

Architectural Overview

Polkadot is a network of networks: Different blockchains (parachains) are anchored at the base layer (Relay Chain) to establish shared security and a means of cross-network communication.

This approach has two important advantages:

1. The network is able to break up its state into many shards and process them in parallel, gaining scalability without considerably decreasing the level of security.
2. The blockchains plugging into the network can have very different rules of operation, transaction processing, capabilities, etc., giving the whole system much greater flexibility.

However, it is also a great engineering challenge to implement correctly. If every node processed every transaction on the network, the level of scrutiny would be at its maximum. But since it's not the case — due to sharding — in order to have the same confidence, that missing attention has to be partially replaced with cryptographic guarantees and cryptoeconomic mechanism design.

Polkadot introduces two types of nodes: Collators and Validators. Collators are the nodes of the parachain: They accept and gossip parachain transactions, store the state of the parachain, and produce block candidates. Validators check block candidates submitted by Collators, sign them, and then use them to include into Relay Chain blocks.

Figure 1
Collators and Validators: Role distribution

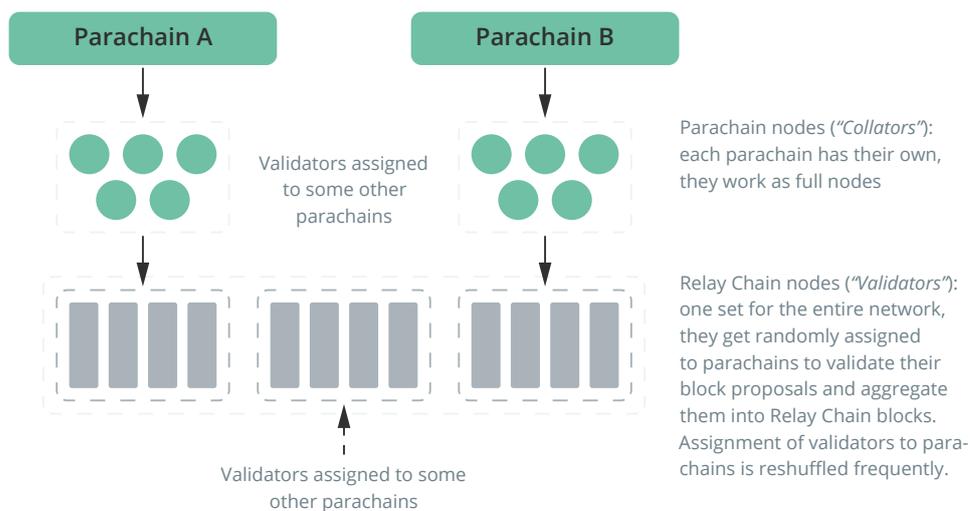
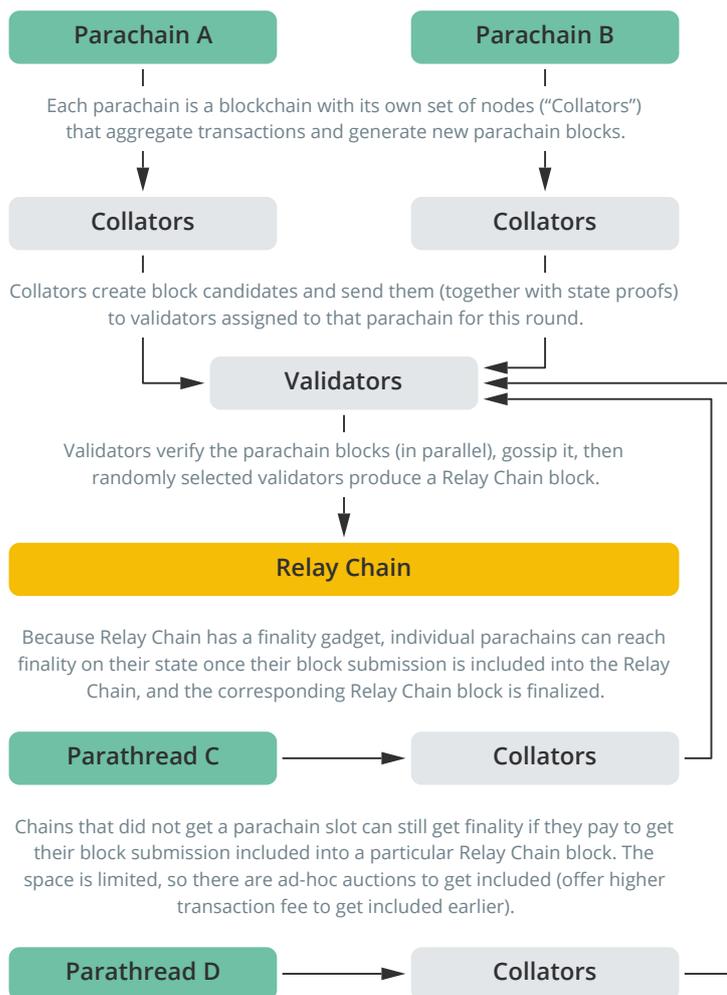


Figure 2
Architectural overview: The network



An important security consideration for sharded systems is dealing with potential collusion among nodes maintaining shards. If the shard validator set is small and static, it would be sufficient to corrupt just a few nodes to break the security of the whole network. Having broken one shard, an attacker could use cross-shard messaging, for instance, to try and steal assets on other shards by double-spending a transaction on the broken one, buying something externally over and over. Since shards do not cross-validate the state and transactions of each other (as a sharded network wants to spread computational effort), this is a viable attack vector that has to be kept in mind.

Polkadot avoids these scenarios by combining a variety of methods:

1. The base layer (Relay Chain) has very strict rules for finality: Once a block is finalized by the respective gadget² (more on that later), it is irreversible, and all of the parachains anchored before and within that block cannot roll back their state.
2. Consequently, a cross-parachain transaction is considered safe once its effects are recorded³ into a finalized block of the Relay Chain.
3. The nodes that anchor parachain blocks into the Relay Chain (Validators) are rotated randomly and regularly,

so it is highly improbable that an attacker could corrupt a sufficient number of Validators to try and anchor a broken parachain state transition.

4. Validators are heavily staked in DOT on the Relay Chain, and their stake can be slashed if proof of their Byzantine behavior is submitted.
5. Validators cross-check the work of other validators assigned to that parachain slot for the round, and there are also dedicated agents (Fishermen) whose job is to monitor block proposals and look for punishable behavior. If a Fisherman submits valid cryptographic proof of a fraudulent action, she receives a large reward from the stake of the Validator being slashed.

In summary, the Relay Chain's consensus provides a secure anchoring and message passing environment for parachains, using a large set of validators with regular reassignment to parachains. In the next sections, we will look at the three components at the center of the design: Polkadot Consensus, Structure of a Parachain and Substrate, the framework for building parachains. The topics of cross-parachain messaging and more general cross-chain communication are covered in the Ecosystem section.

Polkadot Consensus

Context

Broadly speaking, the core properties of a blockchain can be boiled down to two properties:

1. The ability to receive new transactions and include them into the state (by generating new blocks containing these transactions).
2. High certainty that a particular block or transaction is accepted into the blockchain for good and will not be removed later.

These two points correspond to the two topics relevant to blockchain design: block production and block finalization, respectively. Historically, the two properties were frequently handled by the same component, but as later research demonstrated, it is not a strict

requirement, and interesting results can be achieved by splitting them off. Let's look at how the two properties work.

A classic example, Bitcoin relies on so-called "probabilistic finality," derived from PoW mining and the Nakamoto consensus. Under the assumption that an attacker controls less than 50% of the computational power in the network, the farther a given block is in the past in terms of work committed, the smaller is the probability that the attacker can catch up and exclude this block from the canonical chain (the chain that is accepted by the absolute majority of the network participants).⁴ Since this process is exponential, the subjective level of one's certainty that a particular block is final grows quickly, as work accumulates.

² GRANDPA — covered in the section [Polkadot Consensus](#)

³ Technically, the transaction is recorded in a parachain block, which is anchored as part of the parachain state transition in the Relay Chain block.

⁴ A good walkthrough can be found in the paper that originally presented Bitcoin. Satoshi Nakamoto (2008). [Bitcoin: A Peer-to-Peer Electronic Cash System](#), pp.6–8.

In contrast (as just one example), Algorand's consensus offers immediate (and deterministic) finality: If a block is accepted into the chain, it is final, as can be known with certainty by calculating the total amount of stake voting for that block. The tradeoff is that, in theory, it is possible that under a network partition — as a result of a connectivity loss, or of inconsistency of rule interpretation between different software versions during an upgrade — segments of the Algorand network would lose their ability to produce blocks.

In the same scenario, disconnected branches of the Bitcoin network would have very different consensus chains⁵, and as soon as connectivity is restored, all but one version will be discarded by every protocol-compliant participant.

This comparison illustrates a potential tradeoff between consistency (the entire network having the same idea about the “real” state of the network) and availability (every computer in the network being able to interact with the protocol). It could be argued that Algorand

prefers consistency, while Bitcoin prefers availability.

The inclination toward one of the two properties is generally inherent to most existing blockchain designs. Additional requirements and functional considerations, such as cryptoeconomic security or the potential to adjust the scope of applicability of the properties, make this discussion even more nuanced. Polkadot takes its own place in this discussion.

In times of uncertainty, different designs tend to make different tradeoffs, accepting either network stalling or a risk of rollbacks. While by no means common, these crisis scenarios have to be accounted for in order to build a resilient public blockchain network with sufficient decentralization. Polkadot develops a design that splits off block production from block finalization, eventually offering the choice to the user: If the network experiences uncertainty, is it worth it to make a transaction that relies on the state that will be potentially rolled back? The design is explored in the next section.

Hybrid Consensus

As was mentioned above, two of the possible concessions to a faulty environment that protocol architects could make are losing the ability to produce blocks or letting go of deterministic finality. There is also a whole other direction: hybrid consensus.

The idea of breaking up block production and block finalization into two separate processes executed in parallel was first introduced in 2017⁶ in the context of Ethereum. The proposal at the time was to retain a network with probabilistic finality, but augment it with a finality gadget: a background process that would monitor blocks produced by the network and rule unequivocally on the chain, which should be considered final.

Hybrid consensus built in this way pursues both of the desirable properties of the previous section:

1. Ability to produce blocks under tolerable failure levels.
2. Deterministic finality (ability to definitively declare blocks as final).

These properties are achieved simultaneously, and without inheriting the drawbacks — potential network

reorganizations and potential deadlocks of the network, respectively. For Polkadot, there is also an additional complexity of managing the rotation of validators among parachain slots.

To tackle all that, Polkadot employs two gadgets.

BABE (Blind Assignment for Blockchain Extension) is a process for distributing work among validators for the next round. It uses Verifiable Random Functions (VRF) and stake amounts to assign slots to validators. BABE is probabilistic in the sense that if there are multiple competing chains stemming from the last finalized block, BABE employs its own fork choice rule, which does not guarantee finality. This way, new blocks can always be produced.

GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement)⁷ is a clever finality gadget: Under GRANDPA, nodes tell one another which chains (not blocks) they consider canonical, and the last common ancestor that can accumulate two-thirds of the stake implicitly voting for it is considered finalized. An example calculation is shown on the diagram below.

⁵ Assuming each branch retains sufficient computational capacity to continue mining under the same difficulty level.

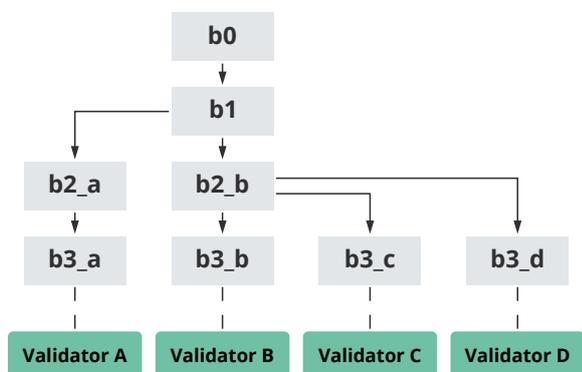
⁶ Vitalik Buterin, Virgil Griffith (2017). — Casper the Friendly Finality Gadget ([arXiv](#))

⁷ Good references are Polkadot Wiki and the formal paper: Alistair Stewart, Eleftherios Kokoris-Kogia (2020). — GRANDPA: a Byzantine Finality Gadget ([arXiv](#))

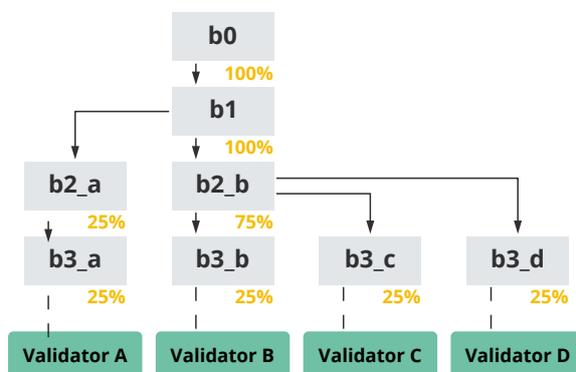
Figure 3

GRANDPA calculation for finalized blocks

There are 4 groups of validators, each speaking for 25% of the stake (hypothetically). Each group has their own chain they think is canonical



GRANDPA looks at all candidate chains. For each block separately, let's write down the % of stake that considers this block part of the chain they think is canonical



Blocks **b0** and **b1** are finalized. Block **b2_b** is also finalized, since it has more than 2/3rd of the stake behind it. No blocks at height b3 are finalized yet.

Stable block production and reliable block finalization are nontrivial properties to maintain at the same time. Many consensus designs — including most of the pre-2018 ones — usually favor one over the other to a limited

degree. Polkadot's hybrid consensus utilizes two gadgets that, in conjunction, aim to tackle both of these properties reasonably well.

Role Distribution in Block Production

As we discussed previously⁸, there are two types of nodes in Polkadot: Collators (parachain nodes) and Validators (Relay Chain nodes). A new Relay Chain block needs to include block candidates from each

parachain. These candidates are proposed by Collators, then verified by Validators assigned to their respective parachain slots for this round, and then they make it into the Relay Chain block.

Figure 4

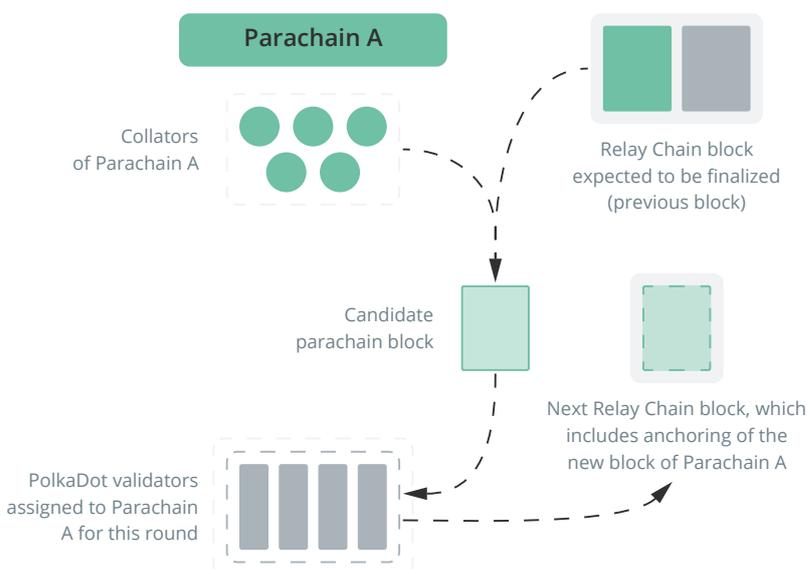
Collators and Validators: Block Production and Inclusion (high-level)

Collators use transactions sent to them to form a new parachain block.

They build on top of the last Relay chain block that they think will be finalized.

Then the candidate parachain block is sent (with state proofs) to the validators assigned to that parachain in the current round.

Validators check the candidate, sign it, then include it into the next Relay Chain block (among block candidates from other parachains).



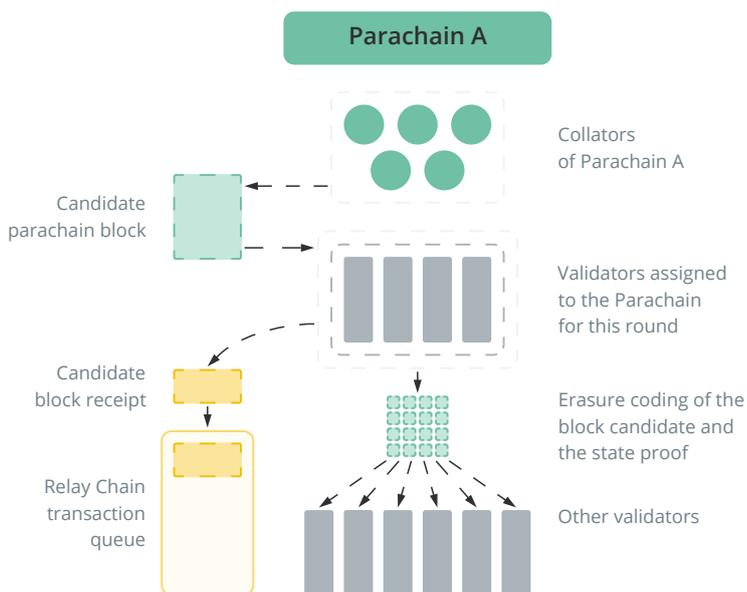
⁸ See section [Architectural Overview](#).

Block production can be conceptually broken up into five stages:⁹

- | | | | | |
|--|---|---|--|---|
| <p>1 →
Validators are selected for parachain slots, using BABE.</p> | <p>2 →
Collators produce block candidates and submit them to the validators.</p> | <p>3 →
Validators verify and distribute (via erasure coding) the block candidates they received, then submit candidate receipts.</p> | <p>4 →
A selected validator produces a new Relay Chain block, including the parachain block candidates that it could find and validate.</p> | <p>5 ◆
Additional validators and fishermen run further checks of validity and data availability, then vote on GRANDPA to finalize the block.</p> |
|--|---|---|--|---|

Figure 5
Block production pipeline

- 1** Collators produce a block candidate: (1) A list of state transitions (2) State proof (see below)
- 2** Block candidate is sent to the validators selected by BABE to validate the slot of this parachain.
- 3** Validators
 - (1) verify the state transition and the proof,
 - (2) make sure the parent of the block was included into an earlier Relay Chain block
 - (3) produce an erasure coding of the parachain block and distribute it among other validators (not limited to this slot).
- 4** Validators produce a candidate receipt and submit it to the Relay Chain queue as a regular transaction.



State proofs are a part of a very important concept in the Polkadot architecture. The Relay Chain does not concern itself with the actual state of the parachains; it only ensures that all of the state transitions are correct. This technique allows the network to considerably reduce processing and storage loads borne by Validators, trading off their ability to look inside the parachains.

The reason why it is important lies in its subtlety: If Validators had to look into the state of the parachains, they would not be able to be reassigned between validating different parachains so quickly. With that, corrupting validators to break a parachain would become simpler, as the time windows to attack could grow (not to mention expected reduction in performance of the validators). Additionally, the current design affords much greater flexibility to the parachains themselves: There are no expectations for their internal complexity or even the instruments they

use, as these parameters do not affect the Relay Chain nor its validators. It's just about making sure the state transitions are correct.

When a parachain acquires its slot to get anchored on the Relay Chain, it submits a State Transition Function, which is just a piece of arbitrary WASM¹⁰ code that looks at the state transition and determine whether it is correct or not. Validators tasked with checking a parachain block candidate do three things:¹¹

- 1.** Check that the block is attached to a block previously included into the Relay Chain.
- 2.** Validate the state proof (diagram below).
- 3.** Apply the State Transition Function to the block (list of state transitions in this case), check that it considers the transition to be correct, and outputs a matching new Merkle root.

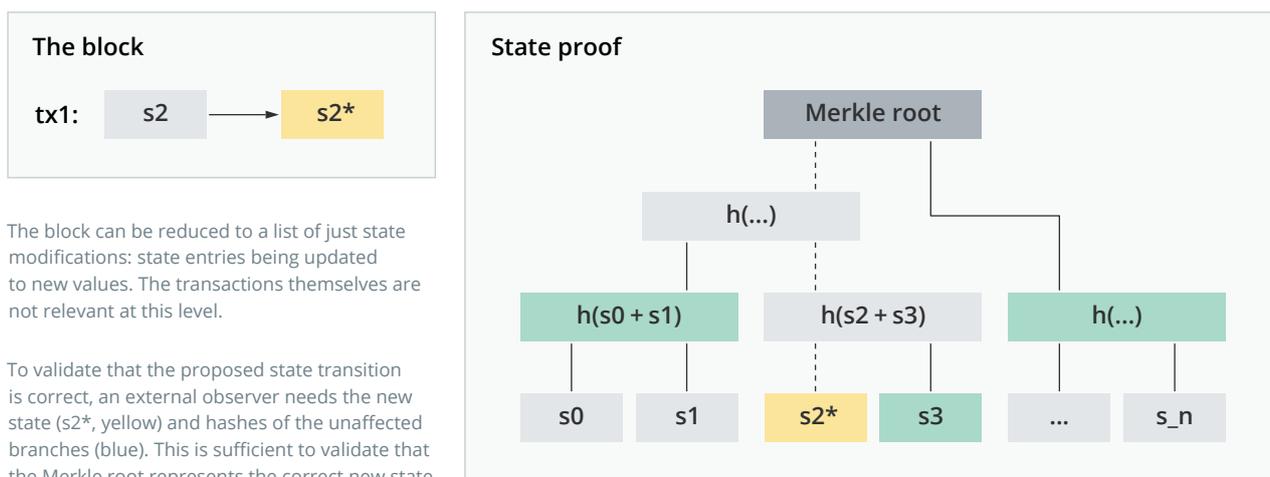
⁹ This is not entirely accurate since parts are parallelized and overlap in several ways. For instance, during what is called Stage 1 here, Stage 5 can still be running for the previous blocks.

¹⁰ Web Assembly, it can be thought of as a virtual machine (VM) designed to be very fast and very safe, sufficiently so to run in a web browser. It is a good representation of a generic platform-agnostic VM with wide usage, which are all qualities an infrastructure blockchain designer could look for.

¹¹ A good reference can be found here: Joe Petrowski, (2020). The Path of a Parachain Block (Polkadot)

Figure 6

State proofs for parachain blocks



Polkadot offers a design that connects block proposers of the anchored chain (Collators) with the block producers of the Relay Chain (Validators). This separation of concerns allows blockchain networks to come and go as parachains/parathreads without losing integrity and liveness of either side — the anchored chain

and the Relay Chain are loosely coupled and can disconnect at will. Yet the block production pipeline has strong security guarantees and connects the anchored chain to Polkadot's finalization and cross-chain message passing.

Parachains and Substrate

While the Relay Chain and its Validators are not really interested in the internal structure of a Parachain (as long as it complies with the basic rules and provides a State Transition Function), Polkadot has built a whole framework for building blockchains, called Substrate.¹²

There is a lot of work usually associated with building a blockchain: networking, gossip, consensus, cryptography, database and storage management, account management, wrapping RPC¹³ calls, transaction processing, etc. All of these have to be present and can affect the security (among other considerations) in critical ways. One of the initial goals of Substrate is to provide a variety of solid components for different layers organized into a framework that would allow

building a working blockchain in a few hours.

In the same spirit of minimal coercion and maximal modularity, which helped remove the excess load from the Validators, Substrate is very flexible and provides options for customization at basically every level. Consequently, developers can choose their own level of customization depending on their goals and resources.

For runtime, Substrate includes Core primitives (what the runtime must implement, as it is expected by other components) and FRAME primitives (enabling a modular framework for plug-in modules with out-of-the-box functionality, called pallets).

¹² It is worth noting that using Substrate is not required to be anchored as a Parachain to the Polkadot Mainnet, and, conversely, building on Substrate does not require locking in a Parachain slot or auctioning for Parathread inclusions. But it may be convenient to use Substrate to build parachains.

¹³ Remote Procedure Call (RPC) — a request-response protocol used, among other things, to describe the interaction model with a blockchain node. RPC is how an external client (such as a DApp frontend running out of a client's browser) would interact with a blockchain node or node service (like MetaMask).

Figure 7
Substrate Architecture¹⁴

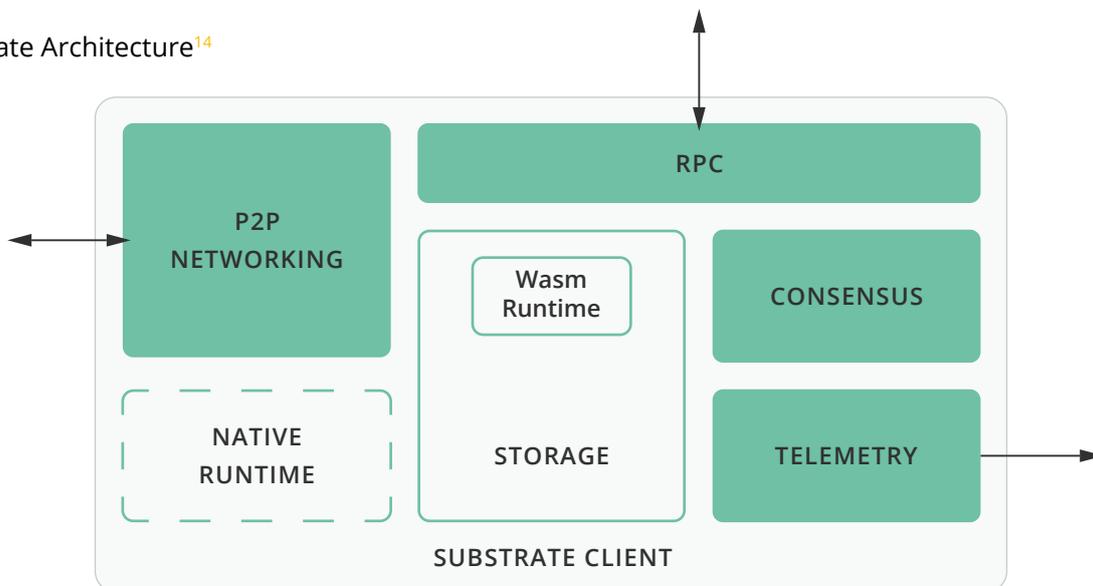
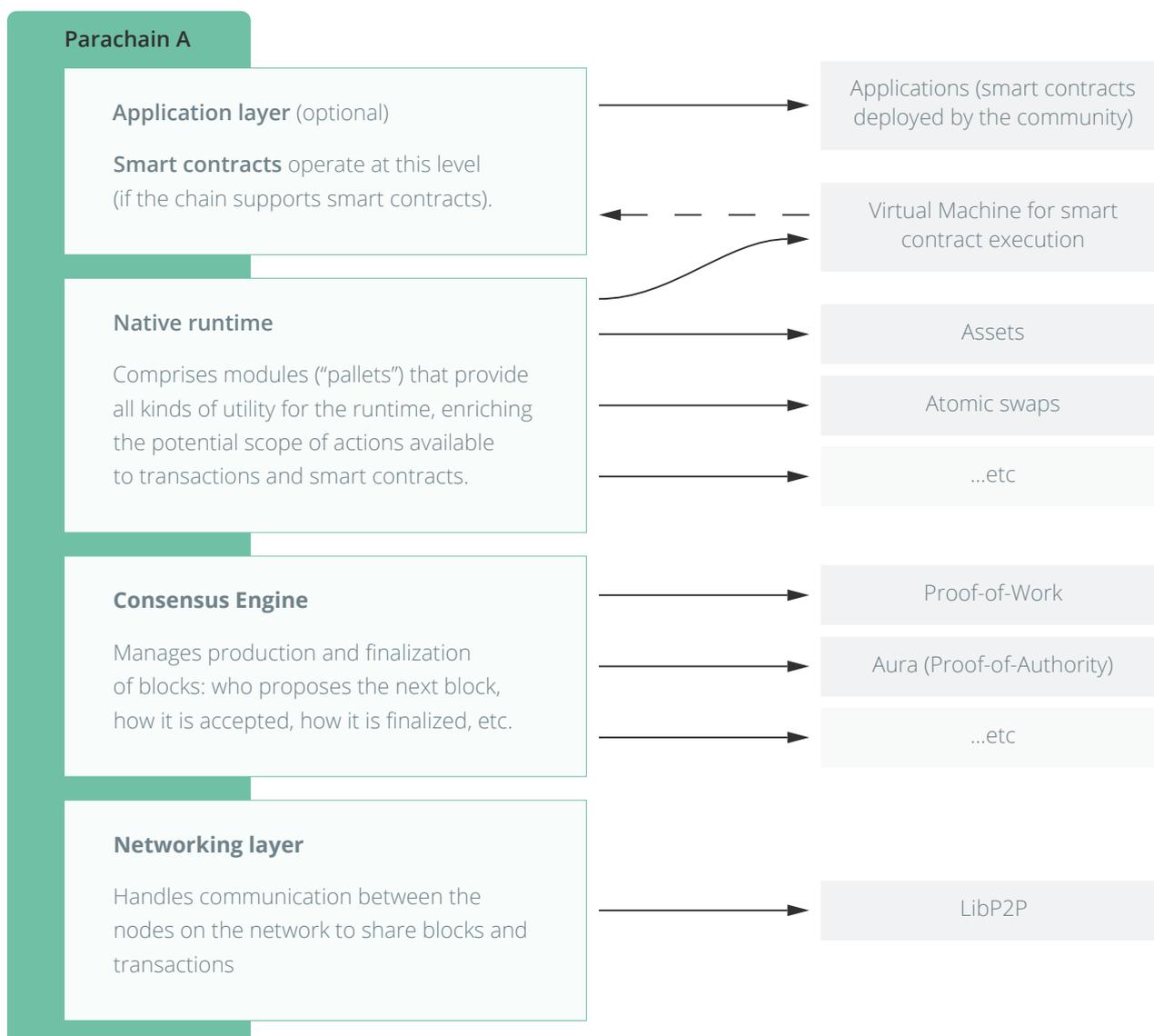


Figure 8
Architectural Overview: A Substrate chain



¹⁴ Official diagram from Substrate documentation ([Substrate Developer Hub](#))

The diagram above informally outlines the layers of a blockchain written in Substrate with some options for modules. There are available choices for every layer, excluding smart contracts but including FRAME pallets that enable smart contract execution.

Building an open network of blockchains, which is Polkadot, requires an active developer community willing to produce and maintain said blockchains.

In addition, it takes a good balance of standardization and flexibility, as, on the one hand, the anchored chains need to communicate in commonly understood ways, but, on the other hand, the tools need to be flexible enough to introduce the absolute minimal constraints. Substrate aims to be the framework that illustrates that balance, empowering developers with a strong core and a multi-layer framework with flexible component choices.

Cross-parachain Communication

Trustless interoperability among parachains and the Relay Chain is at the center of the value proposition of the Polkadot ecosystem for developers. Without native bridges, it would be misleading to think of Polkadot as a sharded environment or a scalability solution since each application would be confined to its own state space and execution space, which would be quite close to running standalone blockchains.¹⁵

Components implementing these systems are hard to get right. There have been many revisions

to the protocol gadgets that Polkadot runs for this purpose, and the final production specifications still aren't locked in at the time of writing. However, there are current implementations, and the development pace remains inspiring.

There are two topics pertaining to cross-parachain communication on Polkadot: passing messages (including contract calls) and running cross-parachain contracts. We will look at them in sequence.

Message passing: HRMP and XCMP

The general outline of passing messages works as follows. Cross-chain messages are created as a result of transaction execution on a parachain and are placed into the “egress” (outgoing) message queue for the parachain. It is the job of Collators to route outgoing messages and process incoming ones. Validators assigned to a particular parachain slot also check that message processing is performed by the Collators.

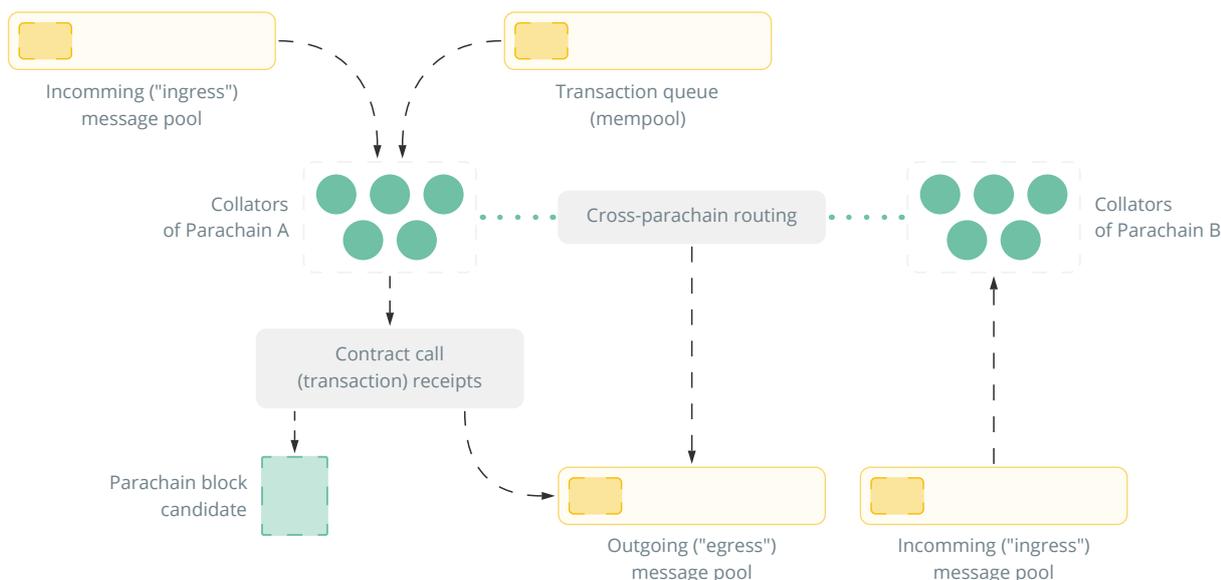
While specific details vary highly and will evolve over time, the design principles remain the same:

1. Guaranteed message delivery is a target, so enforcing message-related logic is part of the protocol guarantees checked by Collators, Validators and other agents. As long as the destination parachain is operational and does not block messaging from the source parachain, an outgoing message directed to it will be delivered.
2. Message ordering is defined and maintained.
3. The process has to be trustless, so message passing is part of the core protocol and the responsibility of nodes running it.

¹⁵ This arrangement could still be beneficial because of the shared security, — and the power of Substrate as a development effort multiplier, which could be considered a byproduct of Polkadot development.

Figure 9

Message processing and routing



In the longer-term vision, messages between parachains will not be passing through the Relay Chain, as that would introduce a severe scalability bottleneck. **XCMP** (cross-chain message passing) is defined as a protocol for cross-parachain transactions that do not go through

the Relay Chain. In the early stages, however, while XCMP undergoes iterative revisions, **HRMP** (horizontal Relay-routed message passing) takes its place instead. HRMP will eventually be obsoleted by a workable implementation of XCMP.

Execution enclaves: SPREE

While XCMP guarantees routing and processing of messages, what happens with the message after it is received on the destination parachain is ultimately up to the processing rules and contracts defined there. While this design offers maximal flexibility, it is not always convenient.

A simple example would be token transfers for a non-standard token contract. There is no automated way for a source parachain to ascertain whether the destination parachain supports a correct token implementation. The destination parachain could potentially not have a deployment of the token at all or have its own broken or malicious implementation. Handling these cases would be an additional workload for maintainers of the

source parachain, and since a destination parachain could change its implementation of the contract later¹⁶, just making sure it is properly deployed once is insufficient.

Shared protected runtime execution enclaves (SPREE) are self-contained entities¹⁷ on the Relay Chain that can receive and send cross-chain messages and maintain their own state. These modules can be deployed to the Relay Chain by its governance or by parachains and remain there, guaranteeing the same interaction model for all parties. In the example above, a safe approach would be to deploy the custom token as a SPREE module and have it track token ownership and the custom rules across parachains.¹⁸

¹⁶ In a mildly optimistic case — through a governance-driven protocol upgrade.

¹⁷ Technically, runtime logic fragments with their own isolated state. They can be thought of as smart contracts.

¹⁸ An in-depth article on SPREE can be found on Polkadot Wiki

Conclusion: Plug-In Blockchains

Technologically, one of the strongest points of Polkadot is that it can support a wide variety of chains anchored to the Relay Chain to share security and message passing. This flexibility, combined with the incentive structure of slot auctions (which will be covered in a later section), can drive innovation in a future-proof way.

If a particular chain becomes obsolete and cannot evolve, it will eventually lose its parachain slot and leave the network. If a whole new consensus family or cryptographic powerhouse emerges, someone will be able to build a parachain from it, using Substrate, and simply plug it into the network (given they can win or purchase a slot), thereby enriching the ecosystem. Moreover, because the state transition functions are generic, the Relay Chain itself can vote for an on-chain upgrade and swap its own consensus to a new one should the need arise. All of this is enabled

by decoupling functionality layers as much as possible.

The same spirit of decoupling and building ready-to-use components in a modular framework has reduced the entry barrier to building a blockchain in 2021 to almost that of launching a DApp in 2017: Developers have to write their business logic and maybe a frontend, and the rest can be taken care of by the enveloping layer.

By abstracting away many of the tedious and expensive components, Polkadot has enabled teams driven by product ideas to focus on bringing value to customers instead of needing to build their own blockchains from scratch and defend every architectural choice without direct product relevance.

As we will see shortly (in the Ecosystem section), this empowerment brought forward a plethora of innovative products.

PNYX Ventures

PNYX Ventures identified Polkadot early as an amalgamator to layer 1s and could potentially solve the issues of cost, speed and security with the framework and goals set out by WEB3 Foundation and its engineering arm, Parity Technologies. Hence, we supported a range of projects within this ecosystem across a wide spectrum of themes; particularly those of pedigree and improvements to existing dApps on existing chains. Our work brought us to close to the ground to apply our trading skillset and venture expertise to add value to projects built for longer-term adoption. With the successful launch of KSM parachains, we eagerly look towards Polkadot parachains as the significant milestone for Dot proliferation.

PolkaFoundry



PolkaFoundry endeavours to create a one-stop production hub for DeFi and NFT apps on Polkadot, ranging from DEXes and derivatives issuance to NFT marketplaces and prediction markets. The PolkaFoundry platform comprises a public blockchain and a kit of developer support tools.

PolkaFoundry provides a framework that ensures an easy start to building cross-chain and highly scalable dApps for developers. The complementary developer support services offered by PolkaFoundry tackles infrastructure issues a dApp creator could face, including managing private keys and file storage.

PolkaFoundry \$PFK tokens are used for paying for services inside the PolkaFoundry ecosystem as well as for project governance. Token holders can also stake \$PKF to participate in many high-profile play-to-earn and metaverse gaming projects on Red Kite such as Faraland, GameFi, Kaby Arena and MechMaster. The tokens are available for trading on exchanges like Uniswap and gate.io.

PolkaFoundry secured multiple partnerships with major projects in the Polkadot ecosystem and helped numerous developers to land their dApps on Polkadot. Partners integrate PolkaFoundry solutions to enhance their dApps performance.

Manta Network



Manta Network, a privacy layer for DApps, introduces a way for users to increase their on-chain anonymity when using DeFi protocols. Manta Network builds a suite of privacy-focused products, pioneering the Polkadot ecosystem with its payments solution MantaPay and MantaSwap DEX.

Built on Substrate as a Polkadot parachain for greater scalability and interoperability, Manta Network tackles privacy-related issues with zk-SNARKs technology, which allows for private transactions. To swap and transact funds privately, users deposit their tokens to the Manta Network, and the privacy-preserving tokens are minted in exchange. Sending and trading the private tokens are available for all addresses on the network.

Compatible with other projects, Manta Network has established several partnerships, including a collaboration with Math Wallet to integrate Manta's privacy-preserving layer to Math Wallet's products, which are used by 2 million people worldwide.

The team behind Manta Network is also building Calamari Network, a canary network on Kusama replicating the functionality of the parent network.

Parami Protocol



Parami Protocol aims to build a tokenized advertisement economy with its user-focused solution. The protocol serves as a beneficial layer between advertisers and users, offering users tools to monetize their engagement.

Parami Protocol enables user data sovereignty at its decentralized identity management layer and leverages this DID layer to enable personalization in advertisement users see on the platform. The protocol verifies that users meet the criteria for a reward and determines the size of the reward. The protocol plans to utilize NFTs and social coins as a form of rewards and supports yield farming for rewards.

Parami's \$AD3 token is multifaceted as it facilitates the protocol advertising system and is used to govern the Parami Protocol product ecosystem.

The Parami Protocol team received a grant from Web3 Foundation in April 2021. Parami Protocol was the part of the 9th cohort of the grant program, together with 47 more dApps on Polkadot. Parami is also a member of Substrate Builders Program.

Interlude: Kusama, the Canary Network



While Polkadot aims to empower highly stable and highly secure innovation, the spirit of its sister chain, Kusama, is in moving fast and building at a rapid pace. Kusama is a blockchain network launched in 2019 and runs largely the same code base as Polkadot. Kusama fills multiple roles in the Polkadot ecosystem at the same time.¹⁹

Staging deployment. Any upgrade to Polkadot can be battle-tested on Kusama first (given consensus of its community), as the architecture of both networks is the same.

Proving grounds. Projects that eventually target Polkadot as their potential destination could launch as a Kusama parachain or parathread first, testing out the product hypotheses on a live network before making a more serious commitment.

Iterative sandbox. Kusama has shorter governance cycles (up to four times faster), which means that decisions can be made faster, and quick adjustments are possible. As a corollary, the community needs to monitor the network much more closely in order to stay up-to-date at all times.

The same reasoning could be applied to projects deploying both on Polkadot and Kusama: Because of the faster pace and somewhat lower stakes, the Kusama deployment could be used to try out new features and integrations.

Bleeding-edge ecosystem. Due to the lower entry barriers and its general ethos, Kusama is expected to attract projects experimenting with all kinds of ideas, from feature and product to tokenomics and governance. Coming to Kusama would mean getting access to all of these projects and innovations before they make a move to Polkadot or other production deployments.

Slot auctions. One of the technologies tested early on Kusama is parachain auctions. The first auctions have already happened on Kusama, having provided stress testing and valuable data about market dynamics of how the network and the markets perform.

Multi-chain launch. A good example of a multi-chain strategy is Moonbeam, an Ethereum-like chain in the Polkadot ecosystem. Moonbeam participated in the slot auctions and has recently won a parachain slot for its Kusama deployment, called Moonriver.

While Kusama is seen as a canary network for Polkadot — and with good reason — it is an independent permissionless network. Kusama has its own token, KSM, and governance system, so while the two networks have been close so far, they can diverge (and reconverge) in the future — as the community will decide.

¹⁹ [Polkadot Wiki](#)

Tokenomics

Introduction: Role of Tokenomics

Permissionless layer-one blockchains are generally secured by the tokenomic incentive layer: an opportunity for capital holders to produce cash flows by committing their capital toward securing the network. This elegant and subtle idea was first brought to life by Satoshi Nakamoto and can be summarized as follows:

- ↓ Assuming the initial value of Bitcoin to be positive, miners run computations in order to receive newly created coins by mining blocks.
- ↓ The more computing power is committed, the more secure and censorship-resistant the network becomes (as capital commitment required to successfully run a 51% attack increases).
- ◆ The more secure and censorship-resistant an electronic cash system is, the more it is worth as a whole. If it also has a limited supply of currency, the unit of said currency will gain value, thus reinforcing the initial point.

The subtlety comes from the fact that this approach implicitly provides three important qualities of a decentralized consensus:

Sybil resistance. A mechanism preventing an attacker from increasing their power in the system by creating many accounts (or otherwise faking the weight in the system). Bitcoin does this by measuring everyone

by the computation power they use for mining; this parameter can't be faked, and reorganizing one's computational capacities among multiple addresses doesn't change anything.

Positive reinforcement. The motivation to commit resources: financial rewards. Usually, they comprise some new tokens (in the case of Bitcoin, up until the predetermined fixed supply is mined out) and fees collected from the service provided — transaction inclusion.

Negative reinforcement. A limiting factor that deals with prolonged attacks of the system. For a proof-of-work network, this is typically the expenditures and opportunity costs for performing the computations — electricity, amortization of hardware, etc.

In **proof-of-stake** networks, the above properties are usually achieved by utilizing stake commitments, inflationary rewards and stake slashing²⁰, respectively. In addition, for a sharded network with a unified level of security (such as Polkadot)²¹, a similar set of mechanisms may be sought out for the selection and adoption of shards. Polkadot approaches this through the **Slot Auctions** system. Finally, a **governance system** driven by the native token can be utilized to adjust protocol parameters and guide the overall development of the network. The following sections will cover these components in that order.

²⁰ Stake slashing — destroying or confiscating some of the collateral that a stakeholder deposited into the protocol — is a widely used design pattern for disincentivizing protocol-breaking behavior. One of its big advantages is that it can be enacted based on cryptographic proofs, so purely protocol-level means — as opposed to human discretion or market forces — are sufficient for its implementation.

²¹ See section [Polkadot Consensus](#).

One-Page Overview: The Token

Token Functions

- Providing economic security through staking (inflationary rewards, network fees, slashing). See section [Security: Proof-of-Polkadot](#).
- Bonding to acquire parachain slots. See section [Ecosystem: Slot Auctions](#).
- Governance voting. See section [Governance](#).

Supply Type

Inflationary, targeting 10% nominal inflation annually and 50% of the supply participating in staking.²²

Stats

Polkadot (DOT)

Circulating supply:²³ 986,858,626 DOT
Market cap:²⁴ \$25,585,430,984
Staked value:²⁵ \$17,075,403,500 (59.52%)



Kusama (KSM)

Circulating supply:²⁶ 8,470,098.06 KSM
Market cap:²⁷ \$2,570,366,715
Staked value:²⁸ \$1,617,006,927 (46.81%)



Security: Proof-of-Polkadot

The Relay Chain, the base layer that pulls the whole construction together, runs a staking incentive system with slashable collateral and staking delegation. The payouts consist of two parts: inflationary rewards and transaction fees.

Inflation

Polkadot targets 10% annual inflation. Rather than aiming for direct financial utility, as a means of payment (which might call for smaller inflation), the important goal of this system is to set an opportunity cost for locking DOT in slot auctions.

Staking rewards are paid by the network to validators and nominators (users who have delegated their DOT to the validators of their choice for the purpose of staking). The rewards are defined as inflation: Every year, the total supply of DOT will increase

by a percentage, which will be received, collectively, by everybody participating in staking.

Because of the target 10% rate, simply holding DOT without putting it to use is expensive.²⁹ The two main ways of investing DOT are staking (or delegating) and slot auctions. Relatively high inflation sets an opportunity cost for considering slot auction participation. This mechanism is explored in more depth in the section on [Crowdloans](#).

²² Source: Polkadot Wiki. For a deeper source, consider W3F Research on this topic.

²³ On August 17, 2021. Source: CoinMarketCap.

²⁴ Ibid.

²⁵ On August 17, 2021. Source: StakingRewards.com.

²⁶ On August 17, 2021. Source: CoinMarketCap.

²⁷ Ibid.

²⁸ On August 17, 2021. Source: StakingRewards.com.

²⁹ If the value of the network stayed the same, the total worth of non-stakers would be decreasing.

Fees and Treasury

The long-term target of the fee structure is maintainability and the performance of the Relay Chain. Important factors in this consideration are:

- Block production times (since they directly affect every parachain and parathread aside from the Relay Chain itself).
- The rate at which the storage requirements grow as data gets added to the chain.
- The ability to handle spikes in transactional volume.

- The ability to include high-priority transactions at any time without breaking any of the other targets.

Fees are calculated from the drag they exert on the system³⁰ and are adjusted for block limit utilization. Unlike many blockchain designs, transaction fees are not seen as a major Validator income driver: With the values set at launch, only 20% of a transaction fee goes to the block producer that included that transaction, with the remaining 80% going into the protocol Treasury.

Validator Rewards and Delegation

Long-term decentralization of the validator set is of particular importance to Polkadot, as it aims to be an infrastructural centerpiece of many blockchain projects. To that effect, measures are taken to avoid centralization of capital behind resourceful Validators³¹ with the ways rewards are processed and distributed.

Inflationary staking rewards are equalized among all Validators currently participating in consensus. Thus, staking rewards are not proportional to the stake. Therefore,

a Nominator who chooses a Validator to delegate to may prefer a Validator with a lower stake since that would offer a better return on DOT to the Nominator.

In addition, the Validator election gadget tries to select Validators in a way that minimizes variance in the staked amount — after maximizing the total stake, which additionally makes it more expensive for an attacker to get their Validators elected.³² Maximization of the total aggregate stake also remains vital.

Ecosystem: Slot Auctions

The Role

Being first and foremost a blockchain project, Polkadot successfully delivered a software infrastructure that brings down blockchain development times from a year to a week³³ — together with a consensus that supports [plug-in hosted chains](#). Yet, arguably, the centerpiece of the innovation Polkadot offers lies not with technology but with its tokenomic architecture.

A strong point of a public permissionless blockchain (such as Bitcoin) is that its longevity does not depend on any one group of people or a company, which is rather uncharacteristic of earlier electronic cash systems. Independent participants enter and exit the role of infrastructure providers (in Bitcoin's case, miners),

pursuing a profit and maintaining the protocol at the same time. Self-sustainability, in this sense, is a property highly desired of public good.

As we discussed in the section on [Substrate](#), the blockchain development framework provides a streamlined technological toolbox that cuts development time and effort. What remains to be built by the development team is the application logic (what the blockchain actually does) and a community to run the nodes with sufficient security guarantees. A standalone Substrate chain with a proof-of-authority consensus run by five nodes does not necessarily instill confidence.

³⁰ Mostly transaction length, processing complexity. More can be found on [Polkadot Wiki](#).

³¹ Be that owned capital or a delegating community.

³² Reducing variance in the Validator set pulls both the highs and the lows closer to the center, therefore, raising the bar to enter.

³³ This is an exaggeration to a point, but it is entirely true that the range of potential functionality combinations that one can launch into production in several days by running Substrate with multiple out-of-the-box pallets is incomparable to what can be achieved with a private PoA Ethereum deployment available to launch in a similar time frame prior to emergence of Substrate.

Parachain anchoring (connecting a chain to the Relay Chain through a parachain slot) provides highly secure finality to the hosted chain plus access to the ecosystem through [XCMP](#). But anchoring isn't free, and therefore, it sets an entry barrier to candidate chains, which is a good additional filter for confidence.

This is where the concept of parachain slots and slot auctions comes in. As was outlined in the [Technology](#) section, the Relay Chain has a limited number of slots for attaching parachains. The target number for the amount of slots is 100, but there will be just a few at launch, with the rest being gradually anchored as the network develops.

The Mechanism

Each lease period is a composition of eight equal lease slots. A parachain candidate can bid for any consecutive slot allocation within that window, setting the range and the proposed bond amount for the whole chosen duration.

Slot duration. On Polkadot, lease slots are three months each, totalling two years; on Kusama, one slot lasts six weeks, summing up to the total lease period of one year.

One candidate can have multiple bids for different ranges, but at most, one of these bids can ever be included in the winning slot allocation. In effect, there is no way for one project to win with multiple ranges at the same time. The protocol runs a candle auction to accept bids and then uses a slot allocation procedure to determine the final distribution of slots among candidates.

Candle Auctions

Equal opportunity is paramount in running an auction and especially for infrastructural allocations that affect the overall well-being of the system. To a certain extent, validators producing blocks for Polkadot could affect transaction ordering and transaction inclusion in minor ways. This is why a simple timed auction, for instance, closing at a particular pre-determined block height, would not be completely fair: Validators selected to mint

Slots are distributed through auctions: Different parachain candidates submit their proposals with DOT attached, and the parachain that wins gets its DOT locked in for two years and is granted a slot in the process. A project can bid on a slot with its own funds or apply for a crowdloan. In an economic sense, if a project uses its own funds to win an auction, this should mean it expects to make more in revenue from the parachain than the opportunity cost of using the same DOT in the staking game. Alternatively, there is a trustless mechanism for community involvement: crowdloans (covered in a [later section](#)).

the last block would have both perfect information about the auction and the power to choose what goes into the block. Therefore, said validators could “snipe” the auction by including a transaction of its own that would outbid their top competitor at the very last moment.³⁴

The way to combat this potential misalignment used by Polkadot is to run a candle auction. Historically, these auctions would run with an actual candle, running for as long as the candle was lit, and closing when it ran out. Polkadot does this using VRFs (Verifiable Random Functions). After a period of two days, for which it is guaranteed that all entered bids will be considered, there is a second period of five days, within which the auction will conclude. The bids continue to be accepted, but at a certain point, the protocol retroactively selects a bidding snapshot from the past and uses it as final. VRF cannot be tampered with by the validators, so it selects a random cut-off fairly. Since later bidders have a bigger chance of getting cut off, everyone is incentivized to bid their real value earlier rather than later.

Duration and limits. According to the current rules, each auction lasts seven days: The first two are “open” (all bids are guaranteed to be considered), and the remaining five are lit with a virtual candle, meaning that the retroactive cut-off point will fall somewhere within the range, invalidating later bids. A good illustration can be found on Moonbeam's blog.³⁵

³⁴ There are no fundamental issues there — i.e., a particular small cohort of validators cannot be censoring or frontrunning transactions for any protracted time for a number of reasons outlined in the section on [Technology](#). But within one block one particular group of validators (incorruptible, because the group composition is not known in advance) could indeed frontrun.

³⁵ [How Parachain Slot Auctions Work, Moonbeam Team, June 15, 2021.](#)

Slot Allocation

When the final snapshot of the bids is taken, the protocol needs to determine the allocation strategy: how to distribute leasing periods among the bidders. The optimization parameter Polkadot uses is total value locked throughout the total lease window: The periods get allocated in the way that maximizes the amount

of DOT that will be staked. It is worth noting that the DOT staked for a won slot auction stays locked until the lease expires, which means that there is an imbalance in the cost calculations: the same six-month slot won with the same amount of DOT could bear different opportunity costs depending on whether the lease was chosen for the first or the last six months of the range.³⁶

Example allocation

The figure below represents an auction for a single slot. For example, in Slot A, in real-time, multiple slot auctions will be taking place in parallel. Six parachains (P1,..., P6) have placed their bets for the lease period as per their business goals. It is worth noting that this is a snapshot of the final bid, not of the bidding in progress.

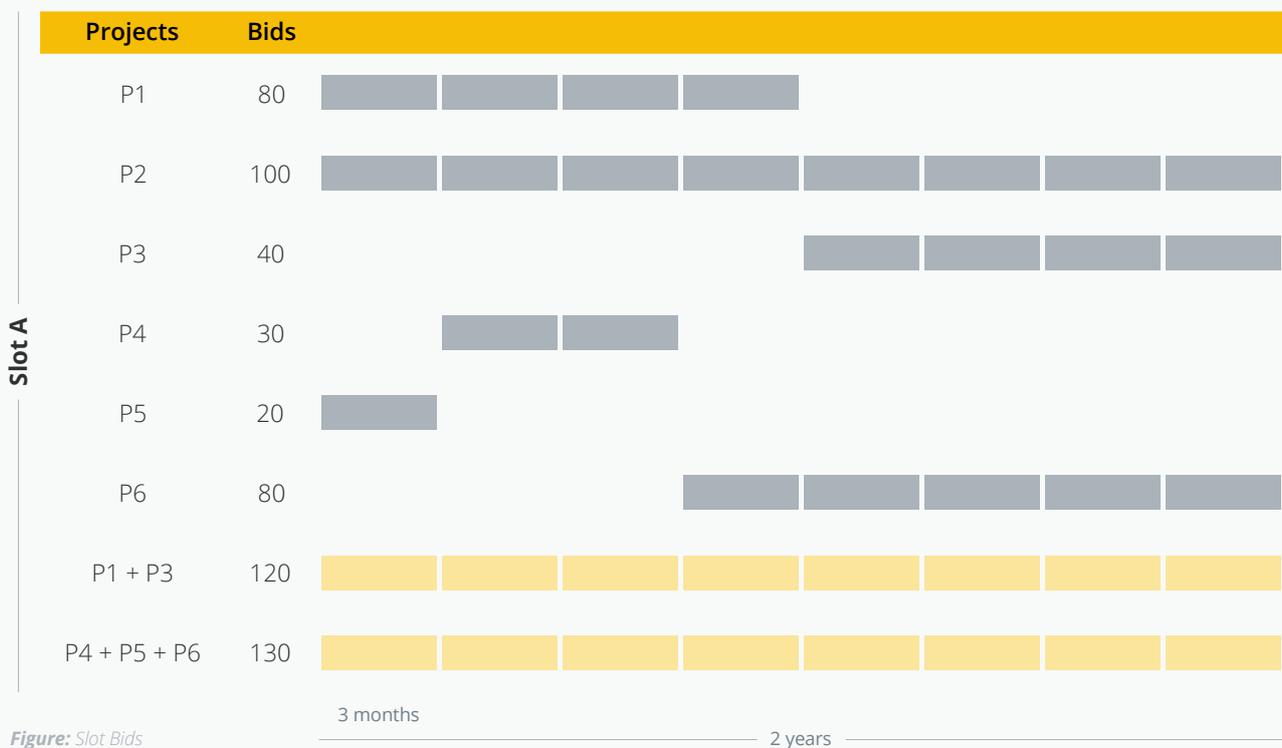


Figure: Slot Bids

Although P2 has the maximum bid of 100 DOT for eight slots, one period would be 12.5 DOT. However, if P1 and P3 are combined, the bid per period will be 15 DOT. In other words, the bids should form the combination of such projects that per period bid is highest, and at the same time, project periods do not overlap. Also, the maximum number of lease periods are occupied.

From the above example, P4, P5 and P6 will finally be allocated the lease period as per period bid is 18.75 DOT, which is the maximum of all combinations.

³⁶ Since the delivery of DOT has to be guaranteed, the former case entails a six-month lockup period, and the latter one takes a lockup for the full 24 months, while the lease itself will only last six months. This effect is not a problem since bidders control which lease slots they bid for and can account for the differences, but it is worth considering.

Crowdloans

A parachain project can offer a deal to its investors: The community supplies the DOT to stake in the auction, making a commitment for the same two-year lock of DOT with zero inflationary rewards. The parachain will then anchor itself and offer its DOT stakers rewards nominated in the native token of the parachain (or no rewards at all, which is also acceptable, although there are now precedents).

Crowdloans and Slot Auctions. A crowdloan is defined by its duration, its cap and the range of lease slots—for instance, up to 1 million KSM throughout 30 days, bidding for slots two to six (out of eight). The crowdloan will bid for the total collected amount in any auction that happens while the campaign is still open. Any new contributions update the bid in the currently ongoing slot auction. If an auction is won, the collected tokens are locked until the lease ends and then returned to their initial owners. If the auction expires, it returns the tokens immediately.

The economic rationale of this mechanism circles back to the notion of economic utility of the chain for the market. Instead of a limited group of wealthier investors, the question is posed to the wider community: How likely is it, given the entirety of data publicly available about the project, that its parachain will generate sufficient cash flows for its native tokens to outweigh the opportunity costs of locking up DOT for the duration?

There are three corollaries:

- **Distributed expertise.** Independent market agents vote with their assets based on their estimations, which on aggregate produces a better valuation than that of a single party.

- **“Holistic” assessment.** The inability to generate cash flows can come from multiple directions — technological inadequacy, lack of product/market fit, weak communication (that hinders community development) and finally, a tokenomics system that cannot convert a great project with a great community into a working token model. The market evaluates all the factors combined: the aggregate ability to produce results.
- **DOT Baseline.** The opportunity cost is staking inflation for DOT, which generates nominal APY in DOT. If the whole crypto market is bullish or bearish, DOT is affected, and some level of positive correlation with its parachain assets would not be entirely unexpected. Together, these two factors imply that crowdloans and slot auctions compare projects on their merits relative to the ecosystem first, and to broader markets only second, which adds a certain level of resilience into the system.

Common-Good Parachains

Several slots of the overall slot composition are allocated to parachains that have universal ecosystem value. The number of slots and acceptance of projects as such are decided by protocol governance, so there is a game of social coordination and social consensus to introduce a project into that role.

Furthermore, projects running for Common-Good Parachain status are not allowed to have their own native token, as that would potentially lead to incentive conflicts. These projects are rather expected to utilize DOT itself for any fees or lockups that may be needed for the parachain tokenomics, fully aligning financial incentives between the Relay Chain (and, therefore, the overreaching ecosystem) with its Common-Good projects.

One example of a (potential) Common-Good Parachain is Snowbridge, a chain hosting trustless cross-chain bridges, starting with a bridge to the Ethereum mainnet.

Governance

There are several key ideas that direct the way governance is implemented in the Polkadot ecosystem and, as part of the Substrate framework, constitutes a shared toolset along with an instance of its practical application.

First and foremost, the system should be sufficiently decentralized or at least have a path toward smooth decentralization that cannot be blocked by a central actor. Secondly, it should be verifiable and censorship-resistant. And finally, it should minimize coordination costs.

Governance on Polkadot is settled on-chain, and it can change the rules of how the chain itself

is run — made possible by modularizing the state-transition function and using WebAssembly, as per the [chain's technological layout](#).

Aside from the voting and vote settlement, another key component of governance is open discussion and social coordination. Currently, some of the good places to track coordination are the [Polkadot Governance Forum](#), [Polkasassembly](#) (a web interface for governance votes and discussions run by Parity Technologies), among other platforms. In the future, one option for the community will be to migrate to parachain-first social platforms such as **Subsocial** (covered in [its own section in Ecosystem](#)).

Governance structure

The key decision vehicle is the concept of Referendum, which is a token-weighted vote to pass or reject a proposal. The proposals themselves are pieces of code that will be executed by the protocol if the proposal passes its required threshold within allotted time. The time window for a Referendum is 28 days on Polkadot and eight days on Kusama.

In addition to the Referendum system, Polkadot governance has a Council. It is an on-chain entity that represents the silent tokenholders who do not want to actively participate in every Referendum. The council comprises a fixed number of seats, with the target size of 24 seats on Polkadot and 19 seats on Kusama.

Councilpeople control the treasury, propose referenda, are able to collectively block dangerous referenda, and elect the technical committee.

The Council is not elected directly but is rather sampled randomly each term, based on the passive endorsements of the token holders. Each token holder can endorse multiple candidates. Generally, the more endorsements a candidate receives, the greater the chance that she would be elected into the Council, but being in the top-24 list by endorsements does not automatically guarantee a Council position. The selection algorithm tries to maximize representation rather than incentivize a supermajority.³⁷

Protocol Funding

The protocol runs a Treasury that is filled from protocol-related sources, such as transaction fees, slashing, etc.³⁸ The scope of applications for which this fund can be used is not limited; it is driven entirely by the community, embodied by proposals (offered by either tokenholders or Council members) and Council votes on their resolution.

The proposer has to reserve at least 5% of the funds they plan to requisition, with this stake automatically slashable if the proposal is rejected. There are also several smaller mechanisms aimed to promote responsibility and disincentivize careless actions that waste the attention of the community.

³⁷ [More information can be found on Polkadot Wiki: Sequential Phragmén Method](#)

³⁸ [An excellent article on this topic can be found on Polkadot Wiki on Treasury](#)

Ecosystem

Introduction

In anticipation of the first Polkadot parachain launch, the ecosystem has been buzzing with projects and developers, building Substrate-based projects and advancing the Substrate framework itself. There are

many amazing communities driving innovation in the space, and we will cover some of them in this section to showcase both the variety and the maturity of the space at the same time.

Concept: Cross-Chain Bridges

Aside from the cross-parachain communication and other forms of messaging provided by the Substrate ecosystem³⁹, there is a topic of bridges to entirely different blockchains. There are several essential challenges that have to be addressed in order to build a trustless cross-chain bridge, depending on consensus, computational capabilities, and relative throughput of the two chains.

Sometimes, one of the chains is not technologically capable to run a fully trustless connectivity gadget to attach the other chain. Thus, Bitcoin's scripting language is not powerful enough to run a Polkadot light client. The Ethereum mainnet has the theoretical power (as it runs a Turing complete virtual machine), but the gas costs of processing every Relay Chain block header on Ethereum are prohibitive by several orders of magnitude compared to potential value.

There are considerable resources committed to secure Ethereum (as one example), but external parties that do not run Ethereum nodes cannot judge whether a particular block is a part of the consensus chain or not

unless they trust someone or build an economic game of their own, incentivizing correct data reporting. Such games can be highly cost efficient, but this is something that has to be separately designed and implemented.

Economic games backing the security of chains are not naturally carried over. If a particular proof-of-stake chain has extensive slashing conditions based on cryptographic fraud proofs, they could prevent a wide range of attacks against consensus on that chain. However, a naive bridge implementation between that chain and another chain could be attacked by a node of the source chain signing some messages that would get the node slashed in the consensus game, but it could fool the destination chain because of the bridge's naivety.

Furthermore, within one chain, the potential impact of a short-term consensus failure could sometimes be mitigated by a future recovery, so the losses would be limited⁴⁰. A successful attack on a bridge does not necessarily lead to a recovery and could also lead to losses of up to all of the assets bridged over from another chain.

Pattern: Parachain + Trusted Execution Environment

One of the design patterns used by multiple projects is the use of Trusted Execution Environment (TEE) enclaves. A TEE enclave is a computational instance that can be expected to run code in a secure manner, guaranteeing integrity of both the computation

it performs and the data that it holds, as well as privacy of said data.

The enclaves exist on a hardware level, enabled by technologies such as Intel SGX. The CPU encrypts

³⁹ This was covered in the Technology section: [Cross-parachain Communication](#).

⁴⁰ As an example, a short-term 51% attack on a proof-of-work chain could produce some successful double-spends, whereby a seller gives away some unrecoverable asset to the attacker, and the attacker is able to undo the payment transaction and use the same money again, which even after chain recovery would leave some of the sellers with losses. But the stability of all of most of the other assets would remain intact.

a segment of memory that is only decrypted within the CPU and only depending on the instructions stored in that encrypted memory. Each CPU is issued a unique key pair that is protected by the integrity of the device and is used to perform the encryption. The issuing entity (device manufacturer) holds an attestation service that offers an external third party to verify that it is dealing with a TEE enclave by asking the assumed TEE for a cryptographic proof of authenticity and then verifying it with the attestation service.

While TEEs offer a level of protection, they are not unbreakable. It is not impossible — although not cheap, either — to compromise a TEE instance. For that reason, the sole existence of TEEs does not make blockchain-related technologies obsolete.

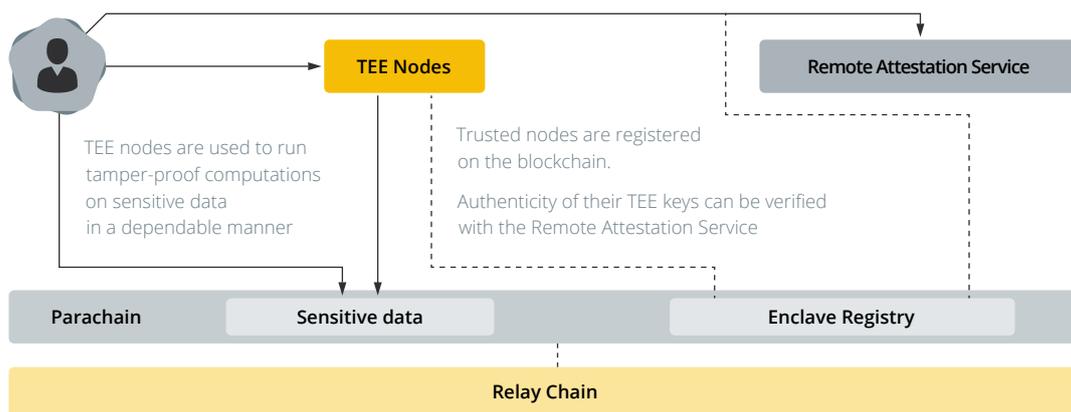
A good way to get the best of the two technologies

is to use them in conjunction. An on-chain registry is used to keep track of the TEE nodes in the system, maintain their stake, and distribute sensitive work among them. The nodes themselves are used for short-term operations, not for long-term storage of sensitive data.

If a particular computation needs to be executed, a random TEE node is selected and given the job. For the duration of that computation, it is highly unlikely that the node will be compromised. Multiple nodes could be asked to run the same computation and reach consensus on its results.

Enclave-based solutions offer good scalability and can even run private computations, but since a given node could be compromised if specifically targeted, enclaves cannot by themselves be the only critical piece of the architecture.

Figure 10
Nodes running Trusted Execution Environment (TEE) Enclaves



The Concept

Moonbeam brings a full Ethereum-like environment to Polkadot, including full compatibility with Ethereum contracts, tooling and the supporting ecosystem, and is natively integrated with the Substrate environment.

Ecosystem Value

The advantages and opportunities that Moonbeam offers cover multiple avenues, enabling a powerful Moonbeam-native ecosystem that is fully exposed to the Polkadot world and is easily connectible to other Ethereum-compatible chains.

As one example, the protocol empowers Ethereum-native projects to pursue a multi-chain approach, reusing the same code base and tooling to get exposure to the Polkadot ecosystem through Moonbeam. This opportunity is a force multiplier since launching an additional deployment on Moonbeam does not take additional engineering resources or further development — the same tools apply, users retain exactly the same interaction flows, no additional wallets are needed, etc.

Furthermore, due to the seamless integration and Ethereum account abstraction (covered below), interoperability with Substrate runtime and contracts running on other parachains through the same EVM instruments is possible and is being actively developed. While corresponding parts of the Polkadot protocol (such as [XCMP and SPREE](#)) are still evolving, the groundwork for this future flexibility is already built into Moonbeam. As a consequence, tenant projects can retain the same Ethereum-focused teams to produce the future Polkadot-focused integrations as well as the local product components.

Technology

Compatibility

All of the tooling associated with Ethereum development works with Moonbeam, including development frameworks (Truffle/Hardhat), contract bundles (OpenZeppelin), oracles, off-chain indexing tools (The Graph), etc.⁴¹

Consensus

Moonbeam will run a proof-of-stake (PoS) consensus by using an extension to Cumulus developed by the project for this specific purpose: Nimbus. The framework manages the collator set and block production rights, adding PoS consensus to the list of options for Substrate developers. The process has two steps:

1. Narrow down the list of potential collators (everybody staked in the network) to 32 candidates for the duration of one epoch (300 blocks). This is done by selecting the top 32 by owned and delegated stake.
2. Pick a few collators that are allowed to produce a block at a particular height. This part uses a randomness beacon, ideally, pulling the random seed from the Relay Chain.

Nimbus is implemented as a pallet and can be hot-swapped through governance should the need arise to update consensus rules. The framework is supported by a Web3 Foundation grant.

⁴¹ [The full list can be found in Moonbeam docs](#)

Account model

There are many intricacies to connecting worlds — per the vision pursued by Moonbeam. Cross-world interoperability needs to be smooth; ideally, users and developers should be able to interact with contracts and addresses on both sides through the same familiar interfaces abstracted away from the internal split and having to move across the gap.

Moonbeam has gone a long way to deliver exactly that kind of experience, rebuilding the entire account structure to provide a native, chain-agnostic gateway between the two address and execution spaces (EVM and Substrate). In practice, this means that the two environments interact through the same abstraction of Ethereum-looking addresses and transactions, using the same tools (e.g., MetaMask) to transact with both spaces seamlessly, with conversion logic running behind the scenes. The Unified Accounts subsystem⁴² is part of the Moonbeam codebase that is currently deployed on Moonbase Alpha testnet and Moonriver.

Parachain strategy

Moonbeam plans to launch both on Polkadot and Kusama with the help of crowdloans. The two chains — Moonbeam and Moonriver — are supported by independent native tokens and represent entirely independent deployments of the same initial code base.

Moonriver. Kusama deployment. On June 30, 2021, Moonriver Network won the second ever Kusama slot auction, becoming a Kusama parachain for one full lease period of 48 weeks. Moonriver⁴³ is a purely community-led project, and its native token, MOVR, could only be received as a crowdloan compensation or as grants and rewards for contributing to the protocol. It follows the spirit of both parent chains, positioned as a canary network for Moonbeam and a development beachhead for fast onboarding to Kusama.

⁴² [Unified Accounts — Moonbeam docs](#)

⁴³ [Moonriver page on Moonbeam website](#)

Phala Network: The Decentralized Cloud



Overview

Phala Network is a decentralized cloud computing network built on Substrate that also protects data privacy. It aims to serve both the emerging Web3 ecosystem, by providing numerous cross-chain applications to parachains on Kusama/Polkadot, and external blockchains, as well as traditional Web2 apps, enterprises, and possibly even governments.

Ecosystem Value

Phala aims to fill the role of cloud computation services, like AWS, Azure, and Alibaba Cloud, that together make up the backbone of modern digital infrastructure. The functional difference lies in that Phala's technology also inherently protects privacy of managed programs and data. Decentralized permissionless deployment of Phala also contributes to robust global coverage and censorship resistance, as the nodes do not have central coordination of any kind. A tokenomic model that avoids central overheads and can offer targeted subsidies gives Phala the opportunity to strike a balance between lower costs for the computation consumers and good financial incentives for hardware providers.

Phala aims to cater specifically to emerging technological needs. Some of the key developments that the protocol aims to serve are:

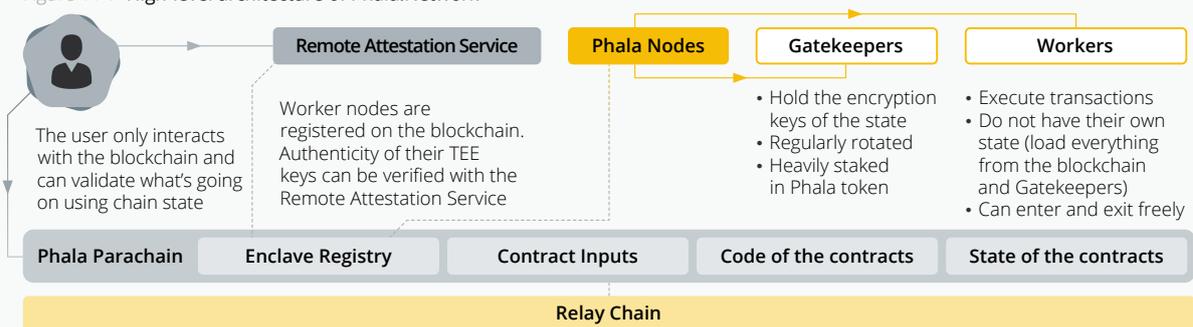
- Exponential growth in data exchange between private parties (individuals and businesses);
- Establishment of data collection and exchange rules across multiple jurisdictions (e.g. EU, China);
- Proliferation of smart devices generating and exchanging tons of data;
- Multi-industry proliferation of Machine Learning and AI implemented in businesses across all industries and verticals.

Phala can also host a full array of blockchain-native applications — including, but not limited to, DeFi products and protocols — by providing them centralized-service-level computational power while protecting the data layer. Acquiring parachain slots on Polkadot (pending) and Kusama (currently live) will give native access to Phala's services to all of the parachain and parachain-hosted products.

Technology

Phala Network makes use of the Parachain + TEE Enclave pattern. There are two kinds of nodes in Phala Network: Workers (fast stateless hardware providers with TEEs) and Gatekeepers (highly staked holders of the master keys of the network).

Figure 11 / High-level architecture of Phala.Network



Horizontal scalability comes from the fact that the set of worker nodes can get arbitrarily high, similar to renting additional instances on a cloud provider. Trustlessness and privacy from the hardware provider come from the fact that worker nodes perform computations inside their enclaves⁴⁴, and the user can establish end-to-end encryption with the enclave directly.

Parachain strategy

Phala pursues a multi-chain deployment strategy with slots on both Polkadot and Kusama. The Kusama chain, Khala, has successfully acquired a parachain slot and is now anchored to its corresponding chain. The two native tokens, Phala token (PHA) and Khala token (K-PHA) will be interchangeable 1:1, tying the security of the two networks.

⁴⁴ So, the data is hidden even from the owner of the node with physical access to it. Unless the TEE is compromised — as covered in the Pattern section referenced above.



Ocean Protocol: Sharing Data

The Concept

To kickstart decentralized data markets, multiple favorable conditions need to coincide. As a strategy, providing these conditions means bringing together data-rich and high-skill stakeholders, technological tools, a marketplace and correct incentives. Ocean Protocol is a movement that makes it all happen.

Ecosystem Value

One of the bigger contributors to monopolization in the digital space is positive feedback loops around data processing. The more data one has, the better they can generalize it, increasing efficiency on the market and getting access to even more data (through additional customers, partnerships, acquisitions, etc.).

Furthermore, a good environment for cultivating data engineers and scientists — and especially for building great artificial intelligence and machine learning models — is one with abundance of data and experience of acting on it as a business. This dynamic ingests talent from the market, further increasing the distance between small new companies and big established ones.

The vision behind Ocean Protocol creates viable instruments and market niches that drive the distribution of labor between data producers and consumers, connecting them in new ways. The scientists get streamlined access to more data and problems to solve, while the business receives wider access to talent and better tooling.

Parachain strategy

There have been no public announcements regarding plans for Ocean to acquire a parachain slot in the observable future. The protocol has partnered with Moonbeam⁴⁵, introducing webapp compatibility with Moonbeam that bridges the OCEAN token between Moonbeam and the Ethereum mainnet. The marketplace provides unified access to data on both chains.

⁴⁵ Covered in a [previous section](#)

Technology

Technologically, Ocean Protocol is first and foremost a framework for provision and consumption of data services: a toolset for decentralized access control and a marketplace. The protocol introduces datatokens, which serve both as an access control medium and a tradable asset.

Datatokens are minted by the data owners, then sold on an open market to data consumers, after which they are used to access the data, being transferred to the data owner in the process. The tokens are standard fungible tokens (ERC-20), which provides compatibility with a wide range of centralized and decentralized protocols.

Ocean Protocol provides a toolset for each type of stakeholder and a range of possible use cases. Data owners can leverage the provided libraries to go through a full cycle of publishing data, pushing it to IPFS or providing a URL to a different storage location, creating datatokens, listing the datatokens on a public or a restricted marketplace, consuming datatokens to provide access control, etc. Data consumers can get access to the marketplaces, buy and use tokens, and provide data processing services of their own.

A longer-term vision of Ocean Protocol includes the Compute-to-Data flows: full business cycles between raw collected data and insights drawn from the data with help of third parties, built in a way that preserves both the privacy of data and the trade secrets of data scientists. Compute-to-Data uses federated learning and multi-party computation schemes to run the data processing pipeline on a distributed network of arbitrary hardware providers.

Math Chain: The Mutli-Purpose Application Layer



The Concept

MathChain is an application chain with a heavy focus on utility and developer access to multiple complementary gadgets and services. As a baseline, MathChain offers an execution environment with shared security and XCMP (as a parachain of Polkadot), together with full EVM compatibility, secret storage and off-chain workers.

Ecosystem Value

One of the centerpieces of the Polkadot ecosystem is Math Wallet: a browser extension for managing private keys to Substrate (and some non-Substrate) networks. MathChain is envisioned as a parachain providing key infrastructural pieces for applications with similar requirements, which are usually nontrivial or costly to maintain for a DApp on its own.

Parachain strategy

MathChain is looking to become a parachain on the Polkadot mainnet as it becomes economically viable. The first deployment is to run as a separate Substrate chain, then being attached as a parathread, with eventual participation in a parachain slot auction. While the particulars of the strategy are not widely circulated, it is worthy to note that Math Wallet is playing an important role in ongoing Kusama auctions, as it is a key management solution that also fully supports crowdloan interactions.

At the time of writing, the project has its native token run on Ethereum, with plans to migrate to MathChain at a later time. 10% of the current supply (and roughly ~6% of the eventual supply, expected to have been mined out by the end of 2029) is allocated to lockdrop investor incentives.

Technology

The network offers access to three utility pallets and illustrates a wide range of potential applications achievable with their combinations.

Secret store

If the set of nodes running the network is relatively stable, it is possible to create a secure storage only retrievable with consensus. Each node stores the same encrypted content, and the decryption key is produced by a threshold scheme, requiring the majority of nodes to engage in a multi-party computation in order to decrypt the data⁴⁶. Because of the natural trust requirement for the committee in its entirety, the service could also process requests for storage and retrieval to external decentralized providers, such as Filecoin, without affecting the levels of centralization further.

EVM

MathChain runs a standard EVM pallet, enabling compatibility with smart contracts built for Ethereum, as well as the whole tooling stack supporting EVM chains: block explorers, web3.js, etc.

DID (decentralized identifier)

While MathChain does not offer on-chain services for verification, it enables components to link together multiple public keys and data points under one account. The account would therefore be able to hold credentials and suffice as a coordination nexus for running secure communication with a DID owner.

Off-chain workers

Computations that are unviable to run on-chain could be offloaded to specialized off-chain nodes on the network. The code remains on-chain, and it is assumed that the workers will be able to coordinate the computations they run by utilizing the on-chain code with potential for cross-validation of results between multiple workers if so required.

⁴⁶ An elaborate description of a very similar system can be found [here](#) — as a part of OpenEthereum node (formerly Parity Ethereum client).

The concept

Darwinia is building a hub of bridges and cross-chain communication gadgets. It is a separate Substrate chain that is connected to multiple external blockchains via unidirectional and bidirectional bridges. The project also hosts and builds a cross-chain metaverse game called Evolution Land.

Ecosystem Value

The Polkadot ecosystem is all about trustless interconnectivity among as many chains, layers and infrastructural components as possible. While internal messaging is covered by the native tools of the protocol (such as XCMP), interoperability with other blockchains and chain ecosystems is something to be tackled by dedicated projects.

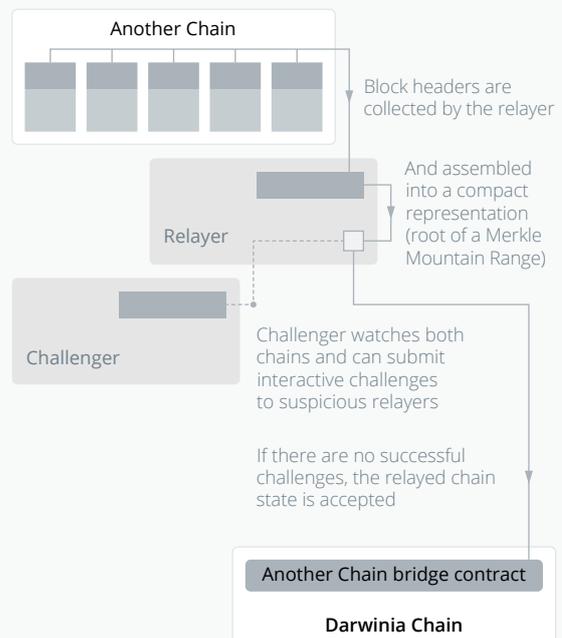
Parachain strategy

Darwinia was initially launched as a separate Substrate chain (Solo Mode of operation), with a gradual rollout of bridges to Ethereum, Tron and other chains along the way. Eventually, the plan is to have both a Polkadot parachain and a Kusama parachain (Crab Network), winning respective slot auctions through crowdloans. After securing the nodes, a network of bridges is to be established between the chains, including two-way bridges between Darwinia and Crab, and bridges to Polkadot and Kusama as necessary (and insofar as the required functionality is not covered by native tooling).

Technology

Darwinia's approach to address the bridging challenges (discussed in a [previous section](#)) utilizes a combination of techniques:

1. Light clients on each side of the bridge can validate block headers from another chain, provided someone brings the data and enacts challenges (diagram below).



2. There is a network of relayers that is incentivized to submit block headers among the chains (in condensed form).
3. The execution is optimistic, in the sense that light clients do not necessarily expend resources to validate something but rather rely on the network of incentivized challengers and challenge games.
4. Each stakeholder is incentivized both positively (with rewards) and negatively (with stake deposits, slashable for provable malicious behavior).

The Concept

A decentralized network for storage and computation, not constrained by the limitations of full blockchain consensus, could be one way to enable the next generation of web-related products. Crust aims to claim that space by leveraging TEE enclaves (described in a previous section, [here](#)) in various contexts, all anchored at the parachain running proof-of-stake consensus.

Technology

Because of the reliance on TEEs, Crust is able to support user flows in a similar way to those established in the centralized cloud computing industry. This includes automated hardware provisioning, smooth integration with off-chain APIs, etc. File uploading is maintained with IPFS, so Crust could be a natural fit for an IPFS pinning service.

Trusted execution serves four purposes:

1. Verifying resources provided and utilized by the node (*"Meaningful Proof-of-Work"*).
2. Validating that new candidate nodes can be authenticated through remote attestation and that their keys are stored on-chain.
3. Maintaining the integrity of computation and ensuring the integrity of data.
4. Managing the encryption of the sensitive data and maintaining access rights.

Consensus and token incentives

The goal of Crust's economic design is the maximization of hardware capacities available to the users without unreasonable tradeoffs in the level of security. Because of the TEE resource attestation, Crust is able to run a consensus that resembles both proof-of-work and proof-of-stake: Nodes have financial stake in the system that can be slashed for Byzantine behavior, but the rewards are partially dependent on the utilization of resources in the network.

Ecosystem Value

Keeping data intact and readily available is a prerequisite of almost any digital product and service. The same goes for running tamper-proof computations on that data. The reliance is amplified if the stakeholders relating to some data or computations are supposed to be able to enter and exit this data relationship freely.

Every application performs some data management and processing. It has been shown how powerful the concept of decentralization can be for building better products and interaction models in many areas, yet potential applications are often constrained by scalability limits: It is very hard to scale something up without compromising security or the level of trust placed into a particular service provider or managing organization.

The approach Crust Network takes is to replace global consensus with mechanisms to attest and employ nodes running TEEs. Since compatible hardware is widely available, horizontal scaling becomes much simpler: Should a user need to increase throughput, more TEE-enabled nodes could be incentivized to join the system, get attested, and start providing their hardware.

Together with the interoperability toward which Polkadot is building, Crust could become the go-to provider of decentralized cloud computing and decentralized storage.

Parachain strategy

Crust Network is planning to have both Polkadot and Kusama parachain deployments as Crust mainnet and Crust Shadow, respectively. The mainnet will launch before the Polkadot auctions happen and will be attached to the Relay Chain at a later time, using an on-chain upgrade. At the time of writing, Crust Shadow is running a crowdloan for a Kusama parachain slot. The network has distributed to the community six batches of rewards for liquidity provision in the slot auction and is looking forward to the second wave of slot auctions.

Deeper Network: VPN Everywhere



The Concept

The centerpiece of Deeper Network is its hardware solution, Deeper Connect: A device that routes all traffic through anonymous VPN channels provided by other such devices. The blockchain solution coordinates all devices and routing in a privacy-preserving way, manages the network tokens, and provides a window into the decentralized web to its users.

Ecosystem Value

Secure and private networking is becoming increasingly important as bigger portions of everyday activities move into the digital world and, in the near future, on-chain. As we mentioned in the introduction, data hoarding by the majority of digital companies sets wrong incentive structures, and predictable movement and connectivity patterns also increase threats to personal security.

Decentralized Private Network provided by Deeper aims to empower households with secure decentralized VPN and connectivity to Web 3.0. For the Polkadot ecosystem, the value of Deeper lies with potential users who could be exposed to the DeFi applications by connecting to Deeper and using its DApp store.

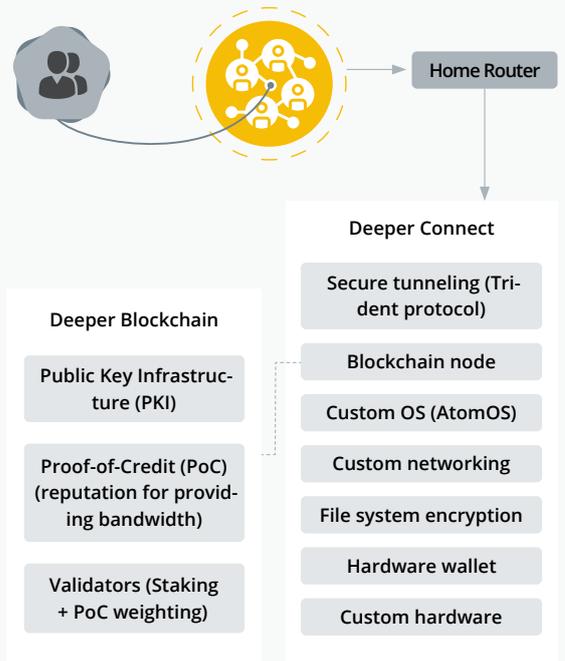
Parachain strategy

There are no publicly announced plans for parachain slot acquisition. For the time being, Deeper Network remains a Substrate chain and a member of the Substrate Builders program, selected by Parity.

Technology

Deeper Network approaches secure connectivity thoroughly, as any one security bottleneck would be sufficient to cripple the overall vision. On the other hand, in order for the VPN tunnels and bandwidth provision to be viable with random routing, the network has to have many users ready to act as bandwidth providers. This requires low barriers to adoption.

To that effect, the project starts with hardware. Deeper Connect is a hardware device that is injected between the cable coming from the ISP and the home router. In most regards, it is a 0-configuration device. Multiple levels of security are introduced into the device itself: custom hardware, encrypted file system, native hardware wallet, a special-purpose operating system and networking protocol implementations.



The blockchain component is used as a common medium of communication between the devices, holding the device registry (in the form of a public key infrastructure) and managing staking and reputation subsystems.



The Concept

Liquidity solutions in contemporary DeFi are still imperfect. Major concerns that Equilibrium raises and targets are cross-chain fragmentation (both in terms of reduced liquidity and limited interoperability), risks of liquidation failures during a flash crash, and a lack of true portfolio approach (best practice to significantly offset risks in traditional finance).

The protocol is comprised of a cross-chain lending platform and an orderbook-based DEX with spot and perpetual markets. It provides opportunities for borrowing, margin trading, and liquidity provision and plans to interoperate with networks and protocols reachable through XCMP and Polkadot bridges.

Parachain strategy

Equilibrium plans to acquire parachain slots on both Kusama (Genshiro⁴⁷ deployment) and Polkadot. As a notable construction, for Polkadot deployment, Equilibrium structured its crowdloan into two steps:

- 1. Commitment.** Up to a limited amount of DOT, investors were able to deposit DOT and receive EQ at increased rates. The DOT is held by an independent custodian and can be transferred only after consensus between Equilibrium, custodian, and a third-party gatekeeper. At their discretion, the investors can also swap their EQ back for DOT at the exact same rate as during their deposit. The project has successfully raised 250,000 DOT through this mechanics as a fraction of its bid for the parachain.
- 2. Participation.** When the auctions start, the committed investors will need to move their DOT from the custodian into a crowdloan. They will receive EQ tokens in rewards that will be partially unlocked once the parachain is launched and another fraction will be vested linearly during its lease.

Technology

The biggest contribution Equilibrium makes to the ecosystem regarding innovation lies with economic instruments rather than technology. The project introduces two new systems into the mix: bailspeople and native risk modeling.

Bailsmen

An additional layer protecting the system (and its liquidity providers) from defaults consists of bailsmen: agents willing to trade off additional risks for additional ROI by, in essence, providing insurance for the protocol.

Each individual loan is backed by its own collateral. If for some reason a default happens, a liquidation mechanism kicks in, and both borrowers' collateral and debt are redistributed among bailsmen pro rata to their participation in the pool. Since all collateral and debt are aggregated per user (as opposed to per borrowing position), this operation stabilizes the debt, as its backing grows.

Risk modeling

The protocol sets its lending fees in its native EQ tokens based on estimated borrower's portfolio risk. This allows to set more flexible rates (not necessarily based on asset utilization in one particular pool), but also introduces additional complexity. Equilibrium runs a complex risk model to correctly price debt (and set emission limits for its synthetic assets).

The initial risk model takes into consideration values of the collateral pool, debt pool, and bailout pool, accounts for upside and downside risk, as well as potential impact of stressed market conditions on the bailout pool.

Ecosystem Value

The DeFi cycle of 2020⁴⁸ demonstrated the power and potential of decentralized finance and its liquidity solutions. A stable and reliable money market can vastly improve efficiency of the on-chain economy.

⁴⁷ Genshiro Crowdloan — [Equilibrium website](#)

⁴⁸ Covered in depth in our other report — [Redefine 2020: A Primer](#)

The Concept

Centrifuge brings together real-world assets and decentralized finance. At its core is a tokenization solution that creates blockchain representations of financial assets, such as invoices, real estate and royalties, allowing owners to use them as collateral for sourcing capital on DeFi markets.

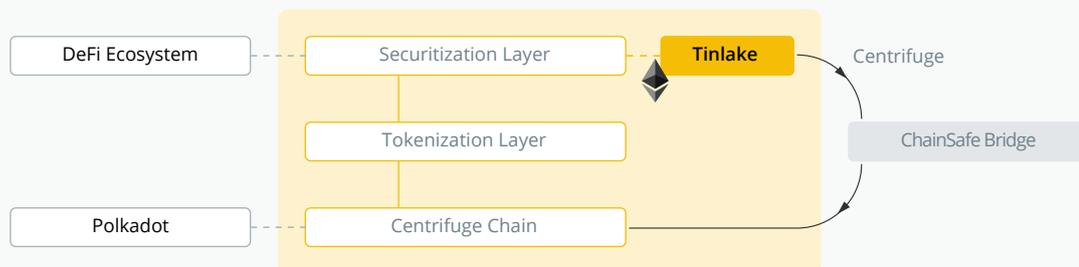
Ecosystem Value

Connecting DeFi with off-chain assets is one of the bigger challenges of the ecosystem. As long as the two worlds remain separate, most of the innovation in the field of financial products championed by the blockchain industry cannot make its way to general audiences. Self-sovereign, tamper-proof, non-custodial egalitarian products need meaningful interoperability with non-cryptocurrency assets in order for the world to benefit from them. Centrifuge is already bridging that gap.

Technology

The product connects multiple layers in order to provide clear abstractions and to offer separation of concerns for different parts of the pipeline. The tokenization layer manages the way documents connected to real assets are introduced and handled in the system. The securitization layer focuses on market mechanisms to enable liquidity provision into loans collateralized with the tokens connected to assets. Together, these layers are represented in the customer-facing product, Tinalake, which, for the time being, runs on Ethereum mainnet and connects to Centrifuge Chain via a bridge.

Figure 13 / Centrifuge architecture

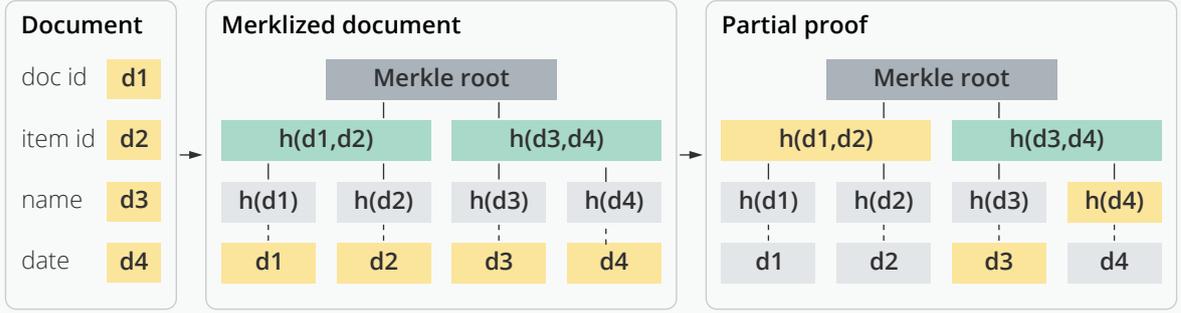


Tokenization

The tokenization layer uses privacy-oriented nonfungible tokens (NFT). The “visible” part of the NFT is its ownership and Merkle root representing the data (diagram below). Stakeholders are connected through a peer-to-peer network and are able to securely exchange information. Therefore, revealing knowledge to new parties is not problematic.

As long as all involved parties know the schema of the document, partial knowledge can be shared, supplemented with Merkle proofs. Documents can be modified by rightful parties, but modifications are incremental and refer back to the original “anchor” — the initial record of tokenization containing a state root and commitments of signing keys.

Figure 14 / Document representation



If the document's structure (schema) is known, it can be represented as a Merkle tree. This conversion is the first step.

User is able share only *some* info about the document and prove that the data indeed matches with the committed root.

Once a document is tokenized, its NFT representation can be placed into the protocol's custody.

Securitization

Tinlake captures investments through deposits into senior (DROP) and junior (TIN) tranche tokens. Every 24 hours, commitments to deposit or withdraw investments are processed depending on the current health of the debt pool, determining (a) how much liquidity can the asset originator withdraw as investment, and (b) what the redemption rate is for DROP and TIN that guarantees tranche seniority.

Parachain strategy

The project plans to run a crowdloan for a parachain slot on Polkadot, offering contributors a reward in the Centrifuge token (CFG) Centrifuge is already running a standalone Substrate chain that will be connected to Polkadot as soon as a slot can be secured.

Polkadex: The Trading Layer



The Concept

Polkadex is building a decentralized exchange based on order books. The goal is to enable a smooth experience similar to that of a centralized exchange, but without the constraints inherent to most existing blockchain-based exchanges.

Target properties of Polkadex are:

1. Classic trading experience:

- Order books;
- No gas fees;
- Integrated fiat on-ramp;
- Desktop and mobile.

2. Enabling High Frequency Trading (HFT). Low latency, high throughput.

3. Blockchain benefits:

- High security of deposited funds
- Traceable and transparent history
- Interoperability with cross-chain liquidity (through XCMP).

Ecosystem Value

Middle ground between centralized and decentralized exchanges is vital to attract larger audiences and institutional traders. An order book platform sufficiently scalable to support high-frequency trading (HFT) can go a long way toward connecting the world of traditional finance with the crypto world.

Parachain strategy

Polkadex's parachain strategy will involve both crowd loan and funding by the team. Until the project can connect to the Relay Chain, it is running as a self-contained Substrate deployment.

Technology

The project uses nodes with TEEs as a key component cementing the system. TEEs guarantee correct execution of code and can attest that its hardware is authentic and valid and prove that it runs the code that it is expected to.



The user has a smooth trading experience, like on a centralized exchange, but no third party holds custody of their funds.

Nodes running TEE (Trusted Execution Environment) with Intel SGX Enclaves are run the sensitive logic. Intel SGX guarantees that the code is tamper-proof.

TEE Nodes

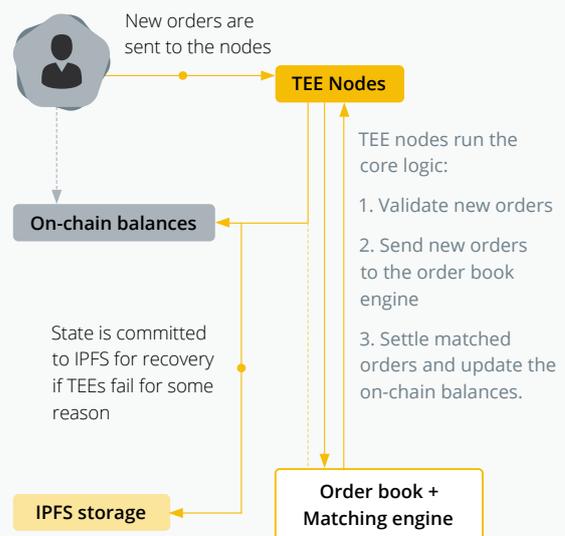
On-chain balances

All balances are kept on-chain and updated by TEE Nodes during settlement.

Order book is processed separately, but matched orders are settled with TEE nodes that check their validity.

Order book + Matching engine

Balances are kept on-chain and are updated by TEEs during order settlement. TEEs also verify new orders before sending them to a matching engine, which is a separate component in the system.



The Concept

Subsocial is a framework for creating decentralized social media platforms, realized as a collection of Substrate pallets and IPFS integrations, together with its own chain running these pallets. The project has the potential to become the communications platform behind Kusama and Polkadot governance.

Ecosystem Value

As the last few years have demonstrated, managing a social media platform requires navigating in very delicate incentive spaces. From a certain scale, the balance between private and public interests becomes unclear, and given that at times, social media becomes the only communications platform for large groups of people, setting and enforcing the rules in an optimal way become increasingly complicated.

Another big topic is privacy and management of data: Because of the chicken-and-the-egg effects, successful platforms find themselves in a position with an immense amount of private data and power over the lives of their users and hosted communities. A centralized, profit-seeking entity encounters conflicts of interests, which are partially offset by regulation and social consensus but still with leeway to sacrifice public well-being to value extraction opportunities.

Subsocial looks to decentralize this whole dynamic, getting rid of many potential incentive misalignments in the process: censorship resistance on the blockchain level (with the possibility to introduce moderation either as a pallet or on the frontend), abundant customization options, cross-social-network capabilities (as multiple deployments would be able to still communicate via common pallets and XCMP), etc.

Technology

First and foremost, Subsocial is a collection of Substrate pallets, together with community alignment toward their improvement and modernization. The framework supports decentralized communities, IPFS integration, sub-spaces, posts, comments, transferable ownership, and a large collection of quality-of-life features for the off-chain components (indexing, feed personalization, full-text search, etc.).

The network looks to host decentralized communities, starting with parachain and Substrate projects in the Polkadot and Kusama space: Each project is offered to claim its reserved name on the network, which can be governed and held in a decentralized way, leveraging whatever on-chain governance structures the project itself uses.

Parachain strategy

While Subsocial aims to eventually acquire a parachain slot, no concrete plans have been publicly announced yet. The acquisition of a parachain slot by Subsocial will enable integration of functionality from every other parachain and make Subsocial's features easily integratable across the board. This interoperability could create powerful synergies among the social component and inherent properties of other protocols. For instance:

- Connecting with DeFi protocols (such as Acala/Karura, Hydra/Basilisk, [Centrifuge](#), and others) to monetize content on Subsocial.
- Offering storage-intensive content items (such as high-quality videos) through an integration with a decentralized storage solution, such as **Crust** (covered in a [previous section](#)).
- Opening up the world of NFTs: tokenizing posts and comments, attaching NFTs from other chains and protocols, etc.
- Providing a fully integrated environment to deal with governance or exchange event analytics for prediction markets (such as **Zeitgeist**, covered in the [next section](#)).

The Concept

It can be argued that the full potential of prediction markets is still some way from realization, given the niche they currently occupy. Zeitgeist expands on prediction market protocols and wants to build a software development kit (SDK) to develop and deploy them to full fruition.

Ecosystem Value

One concept that Zeitgeist wants to develop in particular is futarchy: governance based on prediction markets. The idea is that in an efficient prediction market environment, choices between incompatible paths forward can be judged on purely market merits. After the proposals are presented, instead of some form of voting, the governance module runs a prediction market on the potential long-term benefit of each option, and the winning path will then represent the community's best guess about its viability.⁴⁹

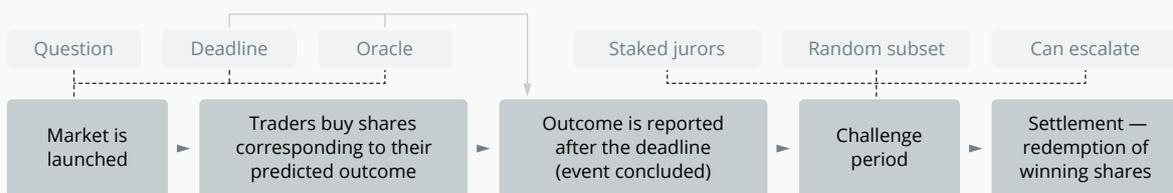
Zeitgeist intends to leverage futarchy for its own governance and also to provide tools and an SDK to enable builders to do the same: launch their own prediction markets and bigger projects leveraging prediction markets for some of the core utility.

Technology

At a high level, the construction is rather straightforward: Different outcomes on a prediction market are represented with shares that can be bought and sold by traders. Each share, therefore, represents a bet on the outcome. Once the event is "resolved", and the outcome is known, "winning" shares can be redeemed for tokens, while losing shares lose their investment.

A dispute system exists in the form of a decentralized court, whereby randomly selected jurors who had previously staked tokens in the court system are selected to vote on the "actual" outcome. If the market is unsatisfied with the result of the vote, it can be escalated by doubling-down on the deposit required for challenging, which would draw a bigger set of jurors. In the end, either the first batch of jurors will be slashed (if they rule differently from the wider committee), or the challenger will be. This process can be repeated by further increasing the deposit and drawing a wider range of jurors.

Figure 16 / Prediction market cycle



On a deeper level, building a good prediction market requires well-architected automated market makers (AMM) and adequate incentive structures, as in the optimal construction, a prediction market should represent the communal level of confidence in each outcome. An in-depth study into AMM mechanism candidates can be found on the Zeitgeist blog.⁵⁰

Parachain strategy

The network Zeitgeist is targeting to anchor at is Kusama. The project has reserved 40% of the total token supply toward a slot acquisition, with current plans to run a crowdloan and use the lease funds as continuous interest payments. It is worth noting that the entire reserve is envisioned for six years worth of slots, which represents six separate lease periods on Kusama.

⁴⁹ A much deeper and more elaborate view can be found in the original paper proposing futarchy. Robin Hanson, *Shall We Vote on Values, But Bet on Beliefs?* — 2000. Good secondary reading is an article by Vitalik Buterin, *An Introduction to Futarchy.* — 2014.

⁵⁰ Introducing Zeitgeist's Rikiddo Scoring Rule. — Zeitgeist Medium

Bit.Country: Bringing Metaverses to Substrate



The Concept

Bit.Country is bringing the nonfungible token (NFT) revolution to Polkadot. Currently, Bit.Country is the only metaverse project in the Polkadot ecosystem. Bit.Country's aims to allow anyone to start their own metaverse for their group of people. Allowing each group to create a unique metaverse means corporations could create metaverses where employees share ideas or families who are spread out across the globe can gather for birthday parties. Countries could unite for humanitarian efforts or political factions could hold town hall meetings. Metaverses are digital universes with their own map, land and buildings that can compete with Zoom calls, Slack channels, and massively multiplayer online games such as Fortnite.

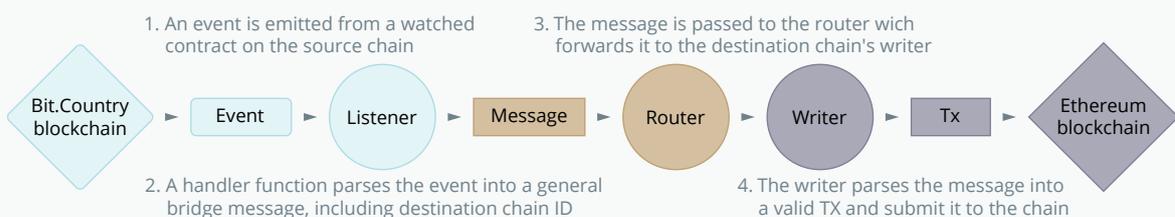
Ecosystem Value

In each Bit.Country, there is a local social token backed by our native token, NUUM, a local marketplace and a local decentralized autonomous organization that governs the community and makes decisions for issues such as the supply of assets. Bit.Country envisions users being able to earn income by performing services inside metaverses, which can make a tangible difference in their standard of living in the real world.

Technology

Bit.Country is a Substrate-based blockchain that uses the ChainBridge cross-chain communication protocol to communicate with the Ethereum Virtual Machine. This enables assets to flow among Ethereum, Polkadot, Kusama and metaverses built on Bit.Country's blockchain.

Currently, Bit.Country's utility token, NUUM, can be sent from TEWAI to Ethereum using the polkdot (.js) browser-based wallet for Substrate assets and from Ethereum to TEWAI using Meta Mask. The team is working on cross-chain transfers for its minable token, BIT, and Bit.Country NFTs such as land blocks. A land block refers to each group's unique metaverse. The main reason for the bridge is to allow assets to be traded on the most popular marketplaces on Ethereum. For example, land blocks can be traded on OpenSea or lend on Compound or swapped on Uniswap. For example, if a cryptocurrency influencer had thousands of members in their metaverse, they could sell their metaverse to a cryptocurrency exchange.

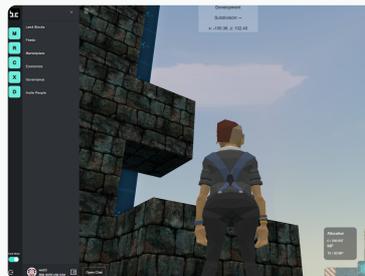


Source: Adapted from [ChainBridge Docs](#), [Cointelegraph Research](#)

Land blocks represent unique metaverses that are privately owned.



Source: Bit.Country



Inside of a land block are buildings and people.

Source: Bit.Country

Parachain Technology

They are planning to launch as a parachain on Kusama and Polkadot through crowd loans.

The Concept

Polkastarter is a protocol that facilitates initial DEX offerings (IDO) with its token auctions and pools. Based on Polkadot, Polkastarter is a cross-chain decentralized exchange (DEX) for fundraising on Ethereum, Binance Smart Chain and Polygon.

Technology

The on-chain component of Polkastarter is a smart contract bundle in Solidity. The project, therefore, targets Ethereum Virtual Machine-compatible chains and is currently deployed on three of the four targeted networks, pending its launch on Moonbeam.

The core product is the token sale logic, currently implemented as Fixed Swap Pools — smart contracts offering the finite predetermined amounts of IDO tokens for a fixed price until the allotted amount runs out. Swap pools based on other types of pricing curves — together with oracle-driven slippage warnings for them — are planned in the full version.

The ultimate technological vision of Polkastarter is a cross-chain IDO platform with DAO-curated listings and a wide range of features and options, including permissionless listings, whitelisted and open pools, Know Your Customer compatibility, liquidity mining and staking programs for the platform token, etc.

Parachain strategy

Polkastarter is not pursuing a parachain deployment. Since the project is implemented using Solidity, the team decided to launch on a Solidity-enabled parachain, Moonbeam (covered in the corresponding section). This integration will allow Polkastarter to retain a consistent code base across multiple chains and get access to the Polkadot ecosystem (including cross-chain bridges) through Moonbeam.

Ecosystem Value

Developing a decentralized token launch platform for promising crypto projects, Polkastarter has become a crucial cornerstone of the decentralized finance (DeFi) ecosystem. Polkastarter democratizes venture capital by bridging DeFi proponents with those who build the decentralized future. Polkastarter enables trustful fundraising for projects building the Web 3.0 future and boasts a long list of notable IDOs on its platform, including Polkadex, Cere Network, Shyft Network, Ethernity Chain and Phuture among others.

Polkastarter conceives cross-chain fundraising, enabling simultaneous fundraising on several chains at once thanks to the inherent interoperability of its versatile DEX. With Polkastarter, up-and-coming projects take advantage of the cross-chain pools and auctions, raising capital on Ethereum, BSC and Polygon.

Project developers who seek to raise funds derive substantial benefits from using Polkastarter for two reasons. First, projects can use the platform to increase awareness and to set out their vision and product description, thus building a dedicated community of 300,000 Polkastarter enthusiasts. Second, projects gain access to capital at an early stage when it's vital for growth.

Polkastarter is a boon for users in a way that it serves as a powerful tool to search for startups at their early days and get a chance to bet on their future for a reasonable price. What's more, the DEX ensures more transparency and greater safety for users when joining token sales. Polkastarter POLS tokens, which are a part of the IDO ticket participation system and are required to participate in IDOs on the platform, are available on major exchanges, including Binance, Huobi, OKEx and Gate.io.

Closing Notes

The online world of 2021 is a strange place. Hardly believable, levels of interconnectivity and the variety of applications — penetrating every aspect of civilization and taking at least some part in most aspects of everyday life — are matched with all-time-high concentrations of power, relentless attacks on privacy, and ever-growing polarization of information bubbles. There are certainly societal tensions and undercurrents that drive this dynamic, but the role of technology in propelling some of the worst aspects of it through positive economic feedback loops should not be underestimated.

Arguably, the technological and business configurations that led to the accumulation of power in small — sometimes unwilling — groups of people or organizations could be named as the central influence. Often, there are no “natural” countermeasures to these forces, as the existing infrastructural landscape can only offer centralization-prone instruments supported by a long history of management practices and mental models that further promote concentration.

A different approach focuses on decentralization as a concept: reviewing and rebuilding digital infrastructure and executive bodies in a way that specifically eliminates the concentration of power. The quest to empower entrepreneurs to build working products up to the functionality and UX quality expected in 2021 is quite long, as many of the deeply ingrained centralized subsystems (such as banks and card payments) are extensive and have to be replaced or upgraded to fit the vision.

The Polkadot ecosystem and the wider crowd around the Web3 Foundation have been running this modernization effort for several years, which is a long time in the blockchain space, given its pace of innovation and refinement. The bedrock layer for the new internet is now there, running smoothly for over a year and about to launch its first slot auctions for hosted chains. The candidates are lined up, ready to fill many of the key roles in the decentralized infrastructure. The future awaits.

Authors and Contributors



Demelza Hays | Cointelegraph Research

 demelza@cointelegraph.com



Alexander Bokhenek | Cointelegraph Research

 alexander.b@cointelegraph.com



Solomon Guy | Cointelegraph Research

 sol.guy@cointelegraph.com



Helen Rosenberg | Cointelegraph Research

 h.rosenberg@cointelegraph.com



Igor Kravchenko | Cointelegraph Research

 igor.doyle@cointelegraph.com



Ron Mendoza | Cointelegraph Research

 ron.mendoza@cointelegraph.com



Nikita Malkin | Cointelegraph Research

 nick.malkin@cointelegraph.com



COINTELEGRAPH
Research

Cointelegraph Consulting offers bespoke research on digital assets and distributed ledger technology. Our services range from phone calls with clients when they have a question to educational seminars for companies via online conferencing, and in-depth written reports on a wide range of topics. Our team comprises management consultants, professional researchers and seasoned blockchain technologists who have a passion for providing unbiased buy-side research.

Disclaimer

Neither Cointelegraph Research is an investment company, investment advisor, or broker/dealer. This publication is for information purposes only and represents neither investment advice nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice. Readers should be aware that trading tokens or coins and all other financial instruments involves risk. Past performance is no guarantee of future results, and I/we make no representation that any reader of this report or any other person will or is likely to achieve similar results. The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice. The authors have exercised the greatest possible care in the selection of the information sources employed; however, they do not accept any responsibility (and neither does Cointelegraph Consulting or Crypto Research Report) for the correctness, completeness, or timeliness of the information, respectively the information sources made available as well as any liabilities or damages, irrespective of their nature, that may result therefrom (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts). In no event shall Cointelegraph Consulting or CryptoResearch.Report be liable to you or anyone else for any decision made or action taken in reliance on the information in this report or for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence or other tort, arising out of or in connection with this report or the information contained in this report. Cointelegraph Consulting and CryptoResearch.Report reserve the right to make additions, deletions, or modifications to the contents of this report at any time without prior notice. The value of cryptocurrencies can fall as well as rise. There is an additional risk of making a loss when you buy shares in certain smaller cryptocurrencies. There is a big difference between the buying price and the selling price of some cryptocurrencies and if you have to sell quickly you may get back much less than you paid. Cryptocurrencies may go down as well as up and you may not get back the original amount invested. It may be difficult to sell or realize an investment. You should not buy cryptocurrencies with money you cannot afford to lose.