Horizen: A Blockchain Platform for Fully Customizable Decentralized Applications

The Horizen Team and Community [*]

October 2019

Abstract

Horizen is a distributed blockchain platform enabling truly decentralized applications. The system is composed of the main Horizen blockchain and its well established tradable ZEN token, a core protocol that behaves as a simple ”truth engine”, and decoupled sidechains that are fully generalizable in consensus and any other design characteristics. Horizen is built from a community with a strong ethos of privacy being a natural right. Following such vision our platform will allow the creation of real-word blockchain applications by giving the possibility of keeping application data private. This will be made possible through a suite of “zero knowledge” cryptographic tools that will be made available.

[*] This project has evolved significantly from its birth as ZenCash in May, 2017. The evolution is only accelerating as our technological frontier expands, and the environment in which we find ourselves changes. For current project state, please visit horizen.global and direct questions or comments to info@horizen.global

Contents

1 Vision

“Critique by creating.” -Michelangelo Buonarroti

Horizen is a massively scalable general-purpose blockchain system with a novel Cross-Chain Transfer Protocol (CCTP) that enables an unbounded and fully decentralized sidechain ecosystem. The CCTP implies a decoupled sidechain network independent of consensus, programming language, or any other design detail in the sidechains. In this way, Horizen is a blockchain-of-blockchains and the core protocol behaves as a simple ”truth engine” adjudicating whether heterogenous consensus across the ecosystem has been properly executed per predefined rules specified by sidechain developers at initialization.

This is a censorship-resistant peer-to-peer network owned by its participants, permissionless in participation, and constructed with incentives for endogenous growth. It is our hope that these tools will enable decentralized social and economic systems that bring people together and empower the human spirit.

2 Technology

The system architecture is designed to allow a modular protocol, stressing functionality over design choice. This framework has at its core a simple ”truth engine” that adjudicates any type of consensus conforming to the CCTP, and all application-specific functions are meant to be deployed on sidechains whose consensus is entirely decoupled from the core. In effect, what this means is that any type of rules can be deployed as a sidechain–whether blockchain or some other type of computing system-and the mainchain function is purely to check whether such rules have been followed and to provide a common token of value. This modularization of function permits massive scalability, freedom in application design, and evolutionary flexibility such that any component can be changed over time so long as the interfaces conform to standards.

The initial system is comprised of a Bitcoin-like blockchain at the core with *Equihash Proof-of-Work (PoW)* augmented with a delayed block penalty algorithm for additional security and a sidechain platform that provides a customizable production-ready node implementation that includes a full *Proof-of-Stake (PoS)* protocol implementation, and a suite of developer tools and a User Interface (UI) made available in the sidechain SDK that abstracts away the complexities of blockchain construction, deployment, and maintenance. In this way, the developer can focus on application logic.

Beyond the initial implementation that we provide, we put no limits or restrictions on what can be developed and extended on top of the base protocol. For instance, the Bitcoin-like core protocol can be swapped out entirely for more modern technologies, like *Directed Acyclic Graphs (DAG)*, PoS blockchains, or really any other *Byzantine Fault Tolerant (BFT)* distributed consensus system; likewise, we will have many types of sidechains starting with a variety of PoS protocols, like *Ouroboros Praos*, DAG, PoW, and implementations built in any number of programming languages, etc.

The industry has seen the development of decentralized public blockchains and a variety of private blockchains tailored for business applications. There is sometimes sensitivity for information being made public and so many businesses have chosen private blockchain solutions; our technology obviates this need by enabling private chains to leverage our public core infrastructure for security and economies of scale, while retaining the option to either keep their sidechains entirely private or leverage our *zero knowledge* cryptographic tools to protect sensitive information. In summary, we provide a new way to bridge the public-private gap that has previously forced bifurcation in either direction.

Finally, even the CCTP can be deployed within sidechains to make them interoperable with other sidechains; it is not just the mainchain with which sidechains will be able to communicate. The implications are that we can have assets and information transfer across blockchains, one important use case being the availability of price stable assets, such as a ZEN Dollar (zUSD), for business applications across the ecosystem.

3 Mainchain

Horizen's mainchain is currently a Bitcoin-like blockchain with *Equihash Proof-of-Work (PoW)* augmented with a delayed block penalty algorithm for additional protection against malicious chain reorganization. Our objective with the mainchain is to strip its complexity to the minimum required to operate the sidechain system, while maximizing security and providing a universal token of value throughout the ecosystem (ZEN). All additional functions and blockchain application features are meant to reside in sidechains designed specifically for those purposes.

The modular architecture of our system means that components can, and will, be swapped over time for performance optimizations, improved security, and scalability. The current mainchain will undergo functionality pruning as we evolve from a privacy coin and into a sidechain-based system, but the current parameters are as follows:

3.1 Delayed Block Penalty

Our engineering team has improved the original Nakamoto Consensus (Nakamoto, 2008) algorithm by creating a penalty mechanism to punish malicious miners. This solution can protect all Proof-of-Work coins from malicious block reorganization, or 51% attack, that use the Bitcoin consensus. It is based on a penalty mechanism for delayed block submission. The penalty affects forks originated by miners that try to mine blocks in private and later inject them into the chain. Malicious forks are penalized based on block height.

We introduced a fork acceptance delay related to the amount of time the fork has been hidden from the public network, time measured in distance from the chain tip. This delay represents the number of blocks for which the adoption of the new parallel chain will be

Table 1: List of mainchain parameters

Description	**Value**
Total coin supply	21 million
Target block time	2.5 minutes
Block size limit	2 MB
Block subsidy halving	840,000 blocks
Initial block subsidy	12.5 ZEN
Allocation to miners	60%
Allocation to nodes	20%
Allocation to Treasury Fund	20%
Equihash (PoW) parameters	(n=200, k=9)
Difficulty adjustment algorithm based on DigiShield v3/v4	

postponed. For an adversary it means that he will need to continue to mine the malicious fork even after revealing it and until the moment when the delay is finished.

For example, let's consider the following delay function DF. To define DF we first introduce BD_i which represents the *block reception delay* for block i defined as the difference between the current mainchain height and height of the received block or -1 in case the height of the received block is greater than the current mainchain height.
E.g. with height $MB = 116$

Table 2: Block reception delays and corresponding penalties

Block Reception Delay	**Penalty**
BD_{MB100}	16
BD_{MB101}	15
...	
BD_{MB115}	1
BD_{MB116}	0
BD_{MB117}	-1
BD_{MB118}	-1

The delay function DF in this case for the whole forked chain will be represented as the $\sum_i BD_{MB[i]}$ values, where i represents indices of the blocks in the forked chain. To see how DF effects malicious actors, we can calculate the number of blocks required to be mined to subvert honest actors, N_{MB},

$N_{MB} = \frac{n(n+1)}{2}$, where n is the desired block confirmation time.

4 Sidechains

The idea of having the core Horizen protocol behave as a simple ”truth engine” interoperable with a system of decoupled sidechains derived from the need to build applications based on blockchain that go beyond the simple use as a cryptocurrency. We wanted to create an ecosystem meant to enable real-world applications to be mapped on a fully distributed, secure, privacy-preserving blockchain architecture, and sharing the use of ZEN as a well established and tradable token with real value. The design of this system obviates the need to create a new coin for each application.

Another purpose of having a common token for the ecosystem is to incentivize decentralization: since these applications are blockchain-based, there exists a need to have a network of nodes running the distributed software, and this network needs to be compensated on the margin to be sustainable.

We segregated application logic from the main blockchain for both security and scalability; it is critical that applications can be fully independent, rapidly deployed, and done so without the consent of other stakeholders in the ecosystem..

The model we are implementing consists of building a platform for developers to allow the creation of decentralized applications implemented as parallel blockchains (sidechains) to our main blockchain (Horizen mainchain) with their own logic and data. Such applications are going to use a single protocol to receive and send back coins (ZEN) from the mainchain to the sidechain, and vice versa. The protocol that will allow this is named Cross-Chain Transfer Protocol (CCTP).

4.1 Cross-Chain Transfer Protocol

As visible from the schema below, our model allows the creation of multiple sidechains - as granular as one per each application - that are connected with the mainchain. The Cross-Chain Transfer Protocol (CCTP) is a unique protocol that must be used by all sidechains, and it doesn’t require the mainchain to follow the parallel blockchains. However, sidechains must track the mainchain.

The Cross-Chain Transfer Protocol allows two main operations:

- transfer coins from mainchain to sidechain (forward transfers);
- transfer coins from sidechain to mainchain (backward transfers).

What we mean with transfer is “burning” coins in the sending chain and “recreating” them in the receiving chain. As we can see in Figure 2, multiple forward transfers can happen during time, from the mainchain to the sidechain. When such transfers happen,

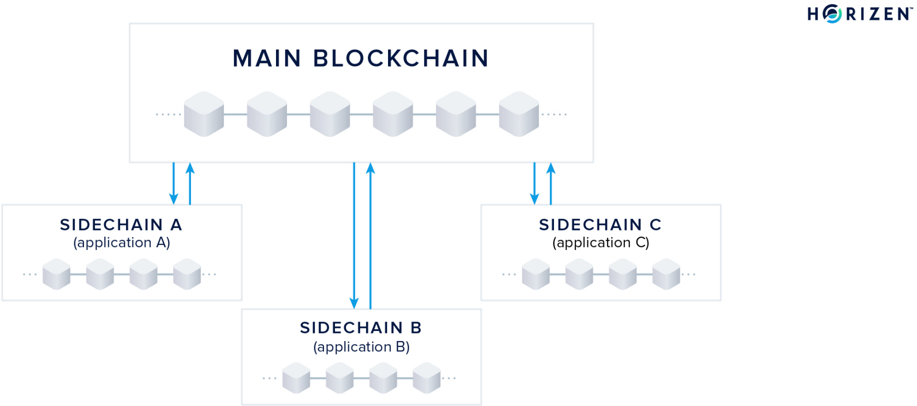


Figure 1: Mainchain-sidechain architecture.

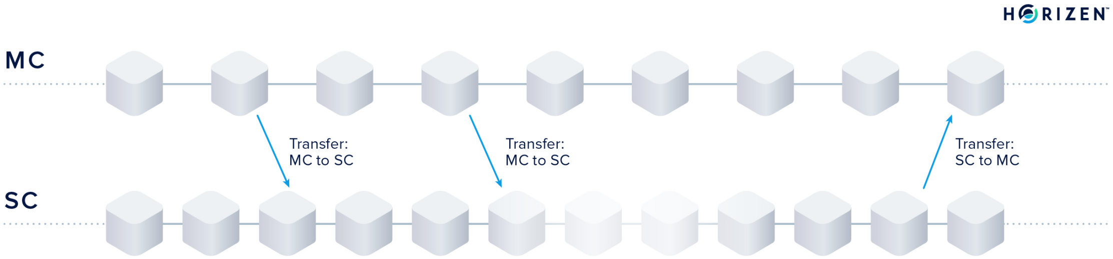


Figure 2: Burning and recreating coins.

those coins will be "burnt" in the mainchain, and "recreated" in the sidechain. The same applies for backward transfers.

The first operation allowed by the CCTP allows the transfer of coins from the mainchain to a sidechain. This is implemented as a regular transaction in the mainchain that spends one or more Unspent Transaction Outputs (UTXO) like a regular transaction, but creating a sidechain specific output. Such a sidechain specific output identifies an address that is in a specific sidechain, and that is owned by the user with the corresponding private key. When such a transaction is included in the mainchain, those coins are spent and are no longer available in the mainchain, but they can then be spent in the sidechain by giving proof of ownership.

Table 2 can be taken as an example: a transaction is created in which two UTXOs are spent. The outputs will be represented by a first one that identifies the sidechain among the many different sidechains, an address, and an amount. Additionally, there may be a change output included.

Table 3: Sending coins from mainchain to sidechain

Inputs	**Outputs**
UTXO1	SC Id, SC address, amount
UTXO2	UTXO3 (change)

Backward transfers are operations that allow the transfer of coins from sidechains to the mainchain. These transfers are initiated in the sidechain, and then propagated to the mainchain. As for forward transfers, in this case the operation will "burn" coins in the sidechain and "recreate" UTXOs in the mainchain that are spendable by giving proof of ownership. However, this operation is much more complex compared to the previous one, because the mainchain does not keep track of sidechains.

A possible strategy to address this problem could have been the usage of a trusted party that is known by both the mainchain and sidechain that could sign transactions to validate them as correct and valid. In that scenario, the mainchain would need to rely on the signature of such actors, but this approach would have led to centralization within the system. What we are implementing instead is a completely decentralized model, in which the mainchain is able to receive certificates from sidechains containing withdrawal requests (WR), and is agnostically able to validate them with no trusted party.

4.2 Sidechain Epochs

The life of a sidechain is split into "Withdrawal Epochs" that are regularly defined time intervals, where certificates are created and signed. Each Withdrawal Epoch is divided into two parts:

- Preparation Stage: withdrawal requests submitted in this stage are going to be included in the next certificate.
- Signing Stage: the withdrawal requests gathered in the preparation stage are aggregated in a certificate and signed.

During the first phase, users that are interested in withdrawing coins from a sidechain to use them in the mainchain create a withdrawal request. When the Preparation Stage ends, the Signing Stage begins. This phase consists of aggregating all the withdrawal requests into a dedicated certificate. Once the certificate is ready, it is sent to the mainchain for validation. As mentioned before, the mainchain will be agnostically able to validate the certificates received, even without following the sidechains, thus allowing massive scalability and decentralization to the system.

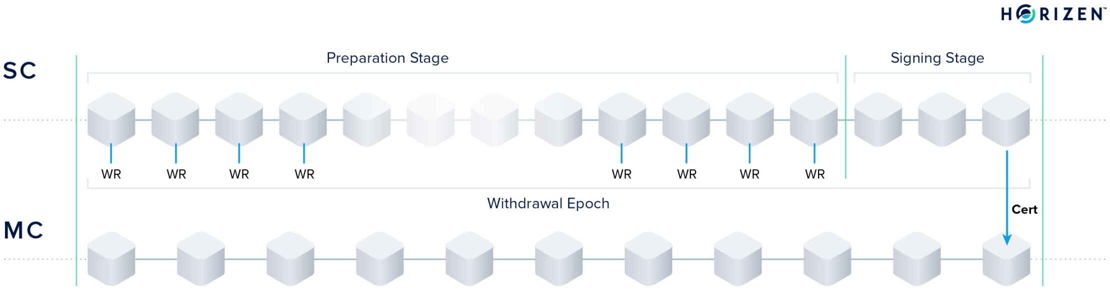


Figure 3: Preparation and Signing stages in sidechain epochs.

4.3 Decoupled Consensus Between Chains

So far we have described the CCTP and the sidechain epochs, but without mentioning the sidechain consensus and its rules. This was because the system is consensus agnostic, so the adoption of any kind of consensus protocol is allowed. From the schema below it is possible to see another graphical example of our mainchain, the Horizen blockchain, and multiple sidechains running in parallel. Our mainchain has a Proof-of-Work consensus, while the two sidechains have their own consensus protocols. These sidechains will have their own epochs, their own custom transactions, with their own consensus rules, withdrawal requests and then certificates sent to the mainchain. Naturally, other sidechains can use completely different consensus rules. For this specific reason, we are calling the model "decoupled consensus between chains."

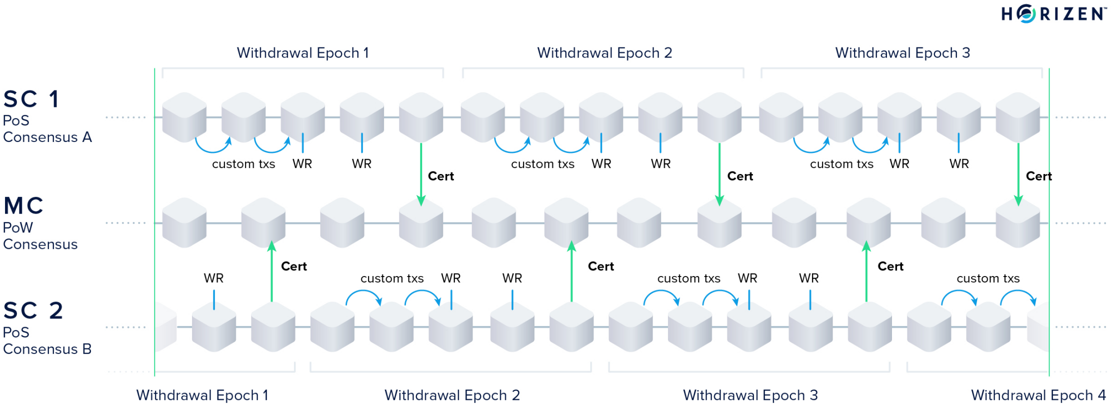


Figure 4: Decoupled consensus between mainchain and multiple sidechains.

4.4 A Platform To Develop Sidechains

Beyond developing the CCTP and implementing it in our mainchain, we also wanted to develop a platform that will make it easier to build truly decentralized blockchain applications. Generally we refer to our platform as the Sidechain SDK, but in reality, it's much more than a software development kit. We started from the consideration that each sidechain needs to be a full blockchain application. This requires implementing all the related aspects: consensus, transactions, network layer, a wallet as the User Interface tool for sidechains, and much more. Building from scratch all these components would be extremely complex and time-consuming for the blockchain developer. This is why we decided to develop a platform to make these steps easier and faster.

In other words, beyond their specific logic and data, all sidechains will use a common part that can be based on the same implementation of many sidechains. So what we are developing and delivering is a platform implementation that addresses most of these aspects, letting the developer focus only on the specific logic and data of his sidechain. This platform can be used by developers to address any kind of use case, and to create any kind of decentralized applications. Real estate tokenization, registries of any kind, and more, are all possible use cases of our system.

4.5 Sidechain Use Cases

In order to better understand our system, a few use cases are listed below as examples of applications that can be created by leveraging the Horizen platform and protocol. These are merely samples - many more applications can be created with our system to address any kind of use case in any market vertical.

4.5.1 Tokenization

The ability to represent assets digitally, tokenize, and transfer them is an important function in the modern economy. The ability to do this at near-zero cost without traditional institutional or geographic restrictions is revolutionary. The sidechain technology will allow developers to create a variety of token standards, similar to current industry standards, such as *Ethereum Request for Comments (ERC)* standards, as well as designing entirely new ones that make use of optimizing consensus to fit the purpose. In addition to that, our ecosystem has the key advantage of offering to a sidechain developer a token that has a value. This is a big plus, as the sidechain user can exchange the new token against Zen, which also translates into the possibility of exchanging the token against fiat currency.

A real estate tokenization use case is presented below. This represents a specific application of the tokenization concept that can be extended to other scenarios. Here it consists of a full blockchain application where users have the ability to tokenize their properties (i.e., a building) and sell them. Any developer could build that application starting from the platform we are providing. In such a sidechain, the developer will have to define what is a property (what is a building, etc...), and to give users a way of providing the details, (where it is, etc...). Obviously, the developer will have to define both data and process for token emission, because the property will have to be tokenized, and also define the rules and data to be used for selling and buying; for instance, how the transactions will be structured for buying and selling tokens of such properties. The following is a summary of the way such a sidechain would work:

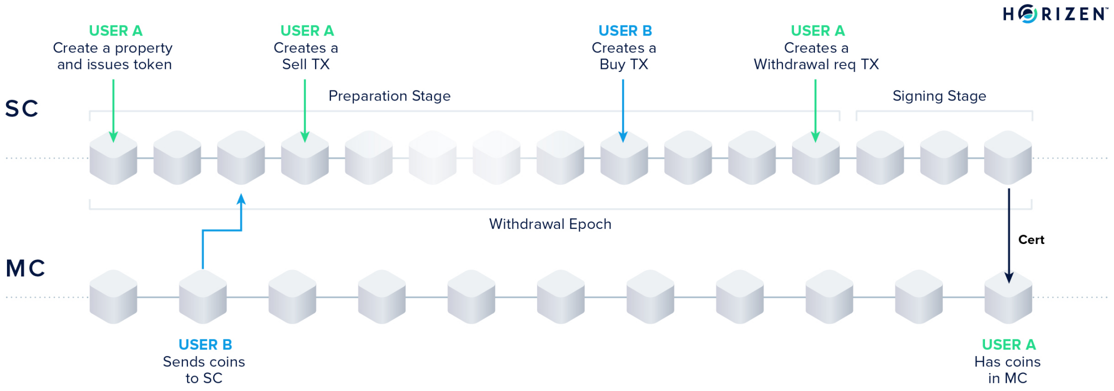


Figure 5: Real estate tokenization example.

A real estate tokenization sidechain was created by the developer, leveraging the Horizen platform. After the sidechain has been customized, anybody can decide to use it, following the sidechain criteria. In this example, $UserA$ declares a property (his house) and issues tokens related to that. This is a specific transaction, with specific data. The transaction will be included in the booking, and accepted by the specific rules of such consensus. By using our platform, all the basic rules of the sidechain will be the same as all the other sidechains in the Horizen ecosystem that use our platform.

At some point, $UserA$ decides to sell his tokens (all of them, or a subset), so he creates a sell transaction. $UserB$, who has coins and is interested in buying tokens of that property, creates a buy transactions for those specific tokens. The coins he has will be spent for that transactions, therefore the ownership of those coins will go to $UserA$. At the same time, $UserA$'s tokens will be transferred to $UserB$. $UserA$ might also decide, at some point, to withdraw some of his coins from the sidechain, so he will create a withdrawal request. This request will be included in the next certificate, and the certificate will be sent to the mainchain for verification. Once verified, $UserA$ will be able to use the coins in the mainchain. This example is purely intended to give a better idea about the potentiality of the system and the way a sidechain like this could work.

4.5.2 Privacy Preserving Blockchain Applications

Our platform will make available to application developers a set of tools that will enable the creation of blockchain applications able to enforce rules on data without the need to expose the data. For example, we can imagine a sidechain where users will be able to prove their financial score without revealing the underlying information. In this way, we can create auditable and privacy-preserving blockchain applications, a requirement for many real-world applications.

4.5.3 Smart Contracts

There is a wide range of valuable uses of conditional scripting, or ”smart contracting”, in blockchain applications. These classes of scripting tools, either partial or Turing complete, have thus far been integrated into the core of blockchain platforms in a fashion that necessitates a single and exclusive design decision. Including extensive scripting at the core of a protocol opens a wide range of possibilities, but also introduces a broad threat surface. Not all blockchain applications require complete scripting, and so our approach is to exclude such complexity from the mainchain, and to enable it in the sidechain system for those applications that need it. Consistent with our general framework, the technology allows for any scripting set to be included in its own sidechain, and the application developer chooses the design.

4.5.4 Price Stable Assets

Extreme price volatility has been a major impediment for cryptocurrency growth in commercial applications, and so we have seen a variety of so-called price stable assets proliferate. These are digital representations of other more commonly used assets in commerce, most often fiat currencies like the US Dollar or Euro. There are a variety of types of price stable assets, everything from pure digital tokens representing the underlying assets held in custody, to those that are purely cryptocurrency-collateralized derivatives. Our technology allows for any and all of these design options to be implemented in ways that are accessible across the entire Horizen ecosystem. One major advantage of implementing a price stable asset system with our sidechains instead of with smart contracts in other systems to date, is that the sidechain owner has design choice in optimizing consensus to facilitate adoption (e.g. via fast confirmation times and/or adoption or velocity incentives) and continued use of the digital assets; smart contract users in other systems have no such flexibility to modify core chain consensus.

5 Network Infrastructure

A performant and robust Peer-to-Peer (P2P) network is the foundation for building any type of advanced blockchain application. The infrastructure should be resilient against node- as well as network failures. It is a stated goal of the Horizen project to build a highly robust infrastructure to support not just the main blockchain, but also a vibrant marketplace for nodes available to host a large number of sidechains. Node operators will have the option to support individual sidechains based on built-in incentives.

In total there are three tiers of nodes: regular full nodes, *Secure Nodes* and *Super Nodes*. Secure and Super Nodes are incentivized with a share of the block subsidy of each mined block. Currently, both node classes receive 10% of the total block subsidy, respectively. The effect of two independent funding pools is to create a dynamic equilibrium in node count and returns to node operators. As returns either increase or decrease, the count of the respective class of node naturally increases or decreases, ceteris paribus.

Additional objectives in creating a system of user owned infrastructure are to have a channel for wider dispersion of block subsidies, and to have geographic placement of the infrastructure optimally dispersed to reduce network latency.

Incentives are tied to a set of minimum requirements that have thus far been verified by sending computational challenges to nodes and monitoring their response times. A central database hosted on Foundation-managed server clusters has been maintained to track performance and compensation eligibility.

Node operators should have a stake in the Horizen Ecosystem, so we require a deposit in a transparent address for each node. This deposit is not locked, so the node operator is free to move it at any time, though the node is not eligible to receive rewards while the balance is below the required minimum. Furthermore, we require each node to have the *zend* P2P port configured with a valid SSL/TLS certificate to provide communication security. Nodes must not restrict peer connections and must run approved *nodetracker* software. Nodes must not fall behind the current block height by more than four blocks.

5.1 Secure Nodes and Super Nodes

The goal with setting minimum requirements is to ensure that Horizen's node network is sufficiently capable of running a robust ecosystem of sidechains and the valuable applications that will reside on them. In this sense, we require skin in the game (staked ZEN), availability, computational, and storage minimums. A basic overview of the requirements for each node class is provided in Table 3.

5.2 Node Tracking and Payments

Early implementations of the Horizen node system involved server clusters running a centralized database of registered nodes and their performance history in the challenge system. Challenges were made by requiring nodes to perform a computational challenge within specified time thresholds, ensuring that the systems running the software met minimum standards.

In keeping with the objective of decentralization, Horizen will migrate this centralized

Table 4: Secure and Super Node Requirements

Requirement	Secure Node	Super Node
Stake	42 ZEN	500 ZEN
Availability	92%	96%
Challenge response time	200 sec	100 sec
Computational requirement		8GB RAM
Storage requirement		100GB storage

system to a decentralized version running on a sidechain dedicated to this purpose. The Node Tracking & Payment sidechain will take receipt of block subsidies designated for each node type, and disperse funds autonomously based on a P2P system of performance and eligibility tracking.

6 Ecosystem

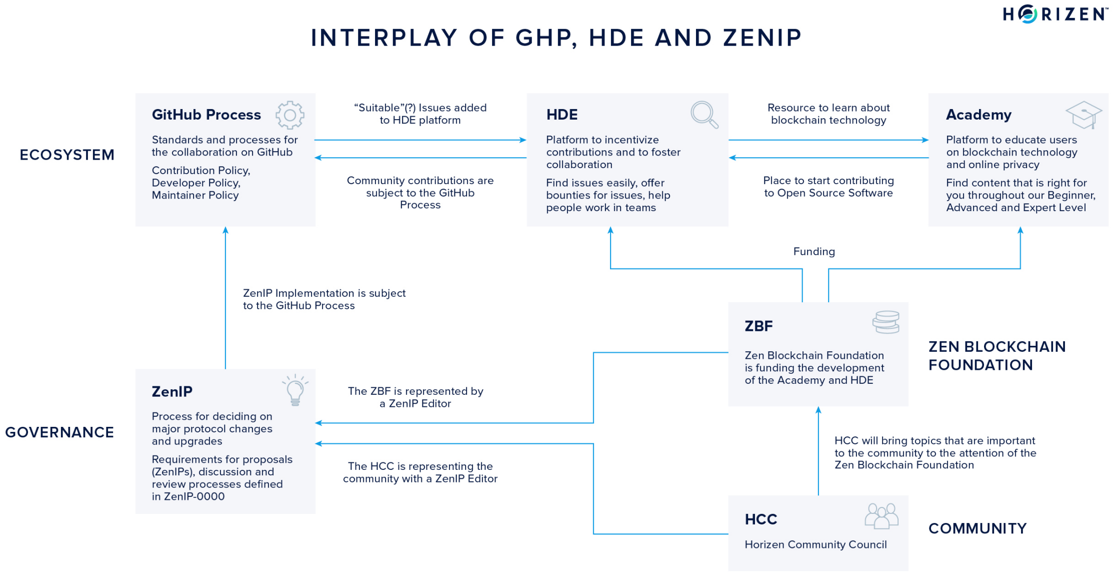
Horizen's ecosystem is a broad collection of stakeholders, including the Zen Blockchain Foundation (ZBF), the Horizen Community Council (HCC), an open-source developer community organized into a curated and compensated Horizen Developer Environment (HDE), a free educational resource called Horizen Academy, various corporate and academic partners, miners, node operators, and end-users. The ecosystem is perpetually shifting as new stakeholders join and others grow their involvement.

6.1 Zen Blockchain Foundation

The Zen Blockchain Foundation (ZBF) was created in 2017 as a Delaware nonprofit corporation. The Foundation's mission is to facilitate focused protocol research and development, as well as growth of the ecosystem. As the first legal entity to bootstrap the project, ZBF performed a variety of legal functions such as filing trademarks, establishing and maintaining critical infrastructure, such as code repositories, and allocating Treasury resources on behalf of the community until the Voting System is sufficiently mature to assume this role. The Foundation maintains a Board of Directors independent of any other entity within the ecosystem. Additionally, the organization appoints a representative ZenIP editor.

6.2 Horizen Community Council

The Horizen Community Council (HCC) is a bridge between the community, the Foundation, and our corporate and academic partners. Its aim is to bring topics of interest to the community to the attention of the broader ecosystem, and to document interactions in a transparent and accurate way in order to become an information pathway and resource for



HORIZEN
INTERPLAY OF GHP, HDE AND ZENIP
ECOSYSTEM
GitHub Process
Standards and processes for the collaboration on GitHub
Contribution Policy, Developer Policy, Maintainer Policy
"Suitable"(?) Issues added to HDE platform
Community contributions are subject to the GitHub Process
HDE
Platform to incentivize contributions and to foster collaboration
Find issues easily, offer bounties for issues, help people work in teams
Resource to learn about blockchain technology
Place to start contributing to Open Source Software
Academy
Platform to educate users on blockchain technology and online privacy
Find content that is right for you throughout our Beginner, Advanced and Expert Level
Funding
ZenIP Implementation is subject to the GitHub Process
ZBF
Zen Blockchain Foundation is funding the development of the Academy and HDE
ZEN BLOCKCHAIN FOUNDATION
GOVERNANCE
ZenIP
Process for deciding on major protocol changes and upgrades
Requirements for proposals (ZenIPs), discussion and review processes defined in ZenIP-0000
The ZBF is represented by a ZenIP Editor
The HCC is representing the community with a ZenIP Editor
HCC will bring topics that are important to the community to the attention of the Zen Blockchain Foundation
HCC
Horizen Community Council
COMMUNITY

Figure 6: Overview of Horizen Ecosystem.

the community. The HCC is formed around central topics of interest and has at least one representative member from the community who actively participates, and is invested, in the respective topic. Along with the Foundation, HCC has a role as ZenIP editor.

6.3 Horizen Developer Environment

The Horizen Developer Environment (HDE) is a key tool for our open-source contributors. It is a platform that makes GitHub issues and other tasks discoverable across repositories, and matches work to individual contributors or teams. The main objective of the HDE is twofold: incentivize open-source contributions and foster collaboration between contributors. This is the focal point for our developer community.

The Foundation can use the HDE to place bounties on certain issues that are deemed especially valuable or of high priority. This increases the number of community contributions, but, importantly, channels effort to align with broader project objectives. HDE is a work curation tool, developer social platform, and education resource. Contributors new to open-source software development get the support of the Horizen team, as well as experienced developer community members.

Besides lowering the barrier to entry for contributors by more easily finding support, the HDE is also a focal point for the development of the Horizen ecosystem in that it contains all project-specific resources to get started working on Horizen. Our GitHub process comprising our Contribution-, Developer-, Review-, and Maintainer Policy are all accessible via the HDE and referenced where applicable.

6.4 Horizen Academy

The Horizen Academy provides free education around the topics of blockchain technology, online privacy and the Horizen project itself. The goal is to lower the cognitive barrier to entering the ecosystem, and to provide educational resources to make the experience of using cryptocurrencies and blockchain technology better.

The core topics mentioned above are available in three levels, Beginner, Advanced and Expert. Articles are mapped across levels, so when a user starts reading and wants to change the level from within the article he can do so and is directed to the corresponding content on a different level, explaining the topic in simpler or more sophisticated terms.

6.5 Corporate Partners

A healthy, stable ecosystem has a variety of organizational partners that contribute in different ways. Some partners contribute to technology development, others drive usage, and still others participate in ideas, governance, or education. Horizen's current corporate partners include:

Table 5: Horizen's corporate partners

Company	**Description**	**Website**
Zen Blockchain Foundation	Software development and community growth	www.horizen.global/
Horizen Labs, Inc.	Software development company	https://horizenlabs.io/
InfoPulse	Software development company	www.infopulse.com/
NTT Data	Software development company	www.nttdata.com
Code Particle	Software development company	www.codeparticle.com/
IOHK	Software development, R&D	https://iohk.io/en/
Deep Dive Technology	Software development	https://deepdive.tech/
Digital Currency Group	Investment company	https://dcg.co
Grayscale	Investment trust managers	https://grayscale.co
Genesis Trading	Institutional crypto trading	https://genesistrading.com
Interfactura	Digital invoicing	www.interfactura.com/
HeroEngine World	Gaming, Smart Cities	www.heroengine.world/
Atlas Bank	Banking	www.atlasbank.com/
Wachsman PR	Public relations	https://wachsman.com/

This list focuses on direct contributors to our codebase or project, design partners, or early users of our technology. We also have 100+ exchange, point of sale, third party wallet, merchant, and other industry partners with whom we've integrated our technology.

6.6 Academic Partners

Horizen has a growing set of academic partnerships to support the project in a number of areas, including scientific and engineering R&D, exploring blockchain use cases with industry and government, and joint educational programs. It is our goal that over time our academic partners will participate in ecosystem governance.

Table 6: Horizen's academic partners

University	Relationship	Website
Università degli Studi di Salerno	Cryptography R&D	https://www.unisa.it/
Politecnico di Milano	Blockchain Observatory	https://www.polimi.it/
Tecnológico de Monterrey	Blockchain R&D	https://tec.mx/es
Duke University	Engineering / FinTech	https://duke.edu/
NC State	Cryptography R&D	https://www.ncsu.edu/
Northumbria University	UI/UX Testing	https://www.northumbria.ac.uk/
Management Center Innsbruck	Blockchain R&D	https://www.mci.edu/en/

7 Governance

Horizen is a decentralized public protocol with a broad and diverse ecosystem, user owners, PoW blockchain consensus, the largest node network in the industry, and a Voting System in development. A system of governance has many variables, everything from how decisions are made to how participants are optimally incentivized. Even deeper inquiries go to heterogeneous user preferences, utility functions mapping those preferences, how to make utility-maximizing decisions, and then how to direct resources to achieve objectives. There are many choices in how to construct such a system, how user preferences are to be measured and aggregated, how voting mechanisms should be designed, what thresholds should be set for action in elections, etc. There are no easy answers, only tradeoffs that can be tuned to better match goals. These are some of our governance goals,

- ecosystem stability
- broad decision-making participation
- checks and balances to prevent stakeholder capture
- influence that scales with skin in the game

- endogenous growth mechanism within the protocol
- incentives to favor good governance and penalties for bad
- a voting mechanism that does not unduly influence outcomes

We have a long term perspective on developing the ecosystem that starts with the premise that we are building a community startup, one that relies heavily on technology, but also social technologies. The framework we've adopted is stable, maturing, and on the path towards greater decentralization.

7.1 Economics

In defining the economic rules of any system, it is helpful to define a set of utility functions over which optimizations can be made. Public blockchains present a challenge similar to a public good, except that decentralization is a key constraint, or at least a strong revealed preference by early communities; in this sense, public goods problems cannot be solved by a central planner optimizing utility for a homogenous agent.

A key objective for Horizen is to have an embedded system of endogenous growth. What this means is that the protocol, itself, provides rewards on the margin for contribution that supports growth. Simply put, $\sum_{i,t} MB_{i,t} = \sum_{i,t} MC_{i,t}$. Identifying, valuing, and programming such contributions over time presents a serious challenge, but Horizen takes an iterative approach with strong governance to at least point the project in the right direction and to leave it flexible to evolve over time.

Thinking of ecosystem contributions on the margin has some big implications. For instance, we are forced to think of classes of contributors, such as miners, as providing a service for which we have diminishing returns over an objective range. In this case, think of mining as providing security to the network, and after some threshold hash rate, additional security has diminishing returns. Rewarding contribution on the margin would imply dynamically matching block rewards with the utility of hash rate. Doing this in practice is much more difficult, as there is uncertainty in security thresholds and potentially severe consequences for not meeting the minimum, let alone the engineering challenges of implementing such a dynamic system.

Currently, Horizen distributes 60% of the block subsidy to miners, 10% to each of two classes of node operators (Secure and Super Nodes), and 20% to a Treasury Fund to fund development, operations, and growth of the ecosystem. Rewards to miners are automatic with block append to the chain, node operators are currently rewarded in batches at weekly frequency, and Treasury funds go into a pool currently governed by the Foundation, with the objective of democratizing the Fund with the Voting System. There are no endowments to founders, team members, or investors in the Treasury Fund; resources are allocated purely for operation of the team to achieve clearly stated roadmap objectives at competitive market rates.

7.1.1 Macroeconomic Properties

Horizen's native cryptocurrency, ZEN, is finite in supply with an asymptotic limit of 21 million that is reached over a predetermined supply emission path. This is defined in the core mainchain protocol and matches the design of Bitcoin. Each block mined is rewarded with a combination of predetermined ZEN plus the sum of fees for all transactions included in the block. The finite supply of ZEN implies a deflationary monetary policy in that there is natural supply attrition as users lose private keys, or funds get burned in certain operations. Finite supply is key to bootstrapping this system in that expectations of demand for ZEN to access valuable utilities, such as sidechain creation and operation, creates coin value.

The supply path takes the following form:

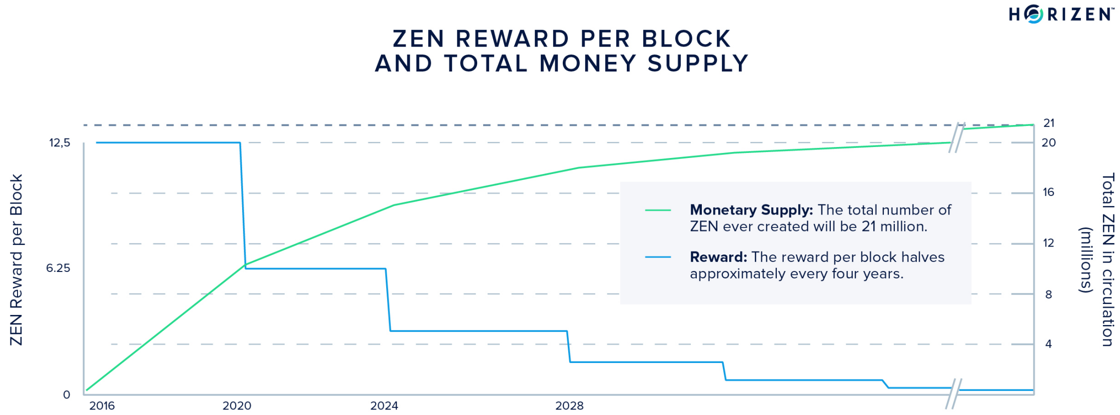
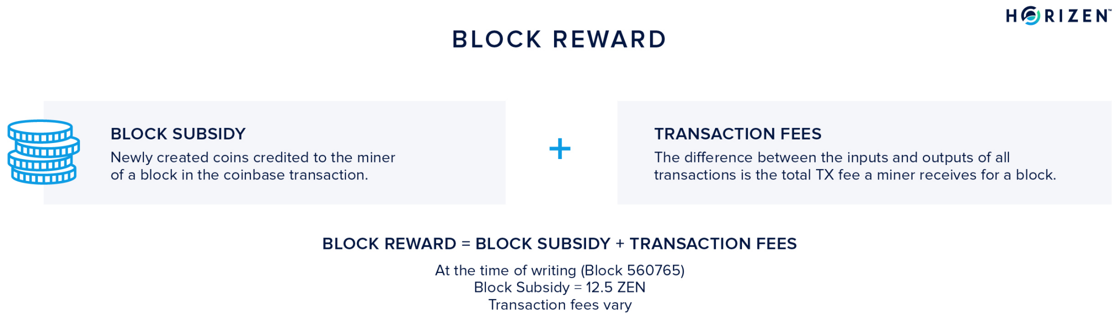


Figure 7: ZEN supply path.

The *block subsidy* is cut in half regularly (every 840,000 blocks, roughly equal to four years), and the total circulating supply asymptotically approaches its limit, 21 million. Miners are incentivized to secure the network and provide *Sybil resistance* with 60% of the block subsidy. The block subsidy is the number of new coins issued with each block, and the block reward composes the cumulative transaction fees of a block and the block subsidy.

Initializing and using Horizen sidechains requires committing, or burning, ZEN so that funds can be used in the sidechains. ZEN is the transaction currency for all sidechains in that it is required for transaction fees within SCs and every time funds are withdrawn from sidechains to the mainchain. Assets within sidechains may also be represented in ZEN, and therefore, demand for ZEN from this channel will be a function of the success of the sidechain system in creating real-world value. Further, at least one price stable asset sidechain implementation will use ZEN as underlying collateral for synthetic price-pegged



BLOCK REWARD

BLOCK SUBSIDY

Newly created coins credited to the miner of a block in the coinbase transaction.

+

TRANSACTION FEES

The difference between the inputs and outputs of all transactions is the total TX fee a miner receives for a block.

BLOCK REWARD = BLOCK SUBSIDY + TRANSACTION FEES

At the time of writing (Block 560765)
Block Subsidy = 12.5 ZEN
Transaction fees vary

Figure 8: Horizen's block reward is the sum of subsidies plus fees.

assets, such as the zUSD, zEUR, zPeso, etc.

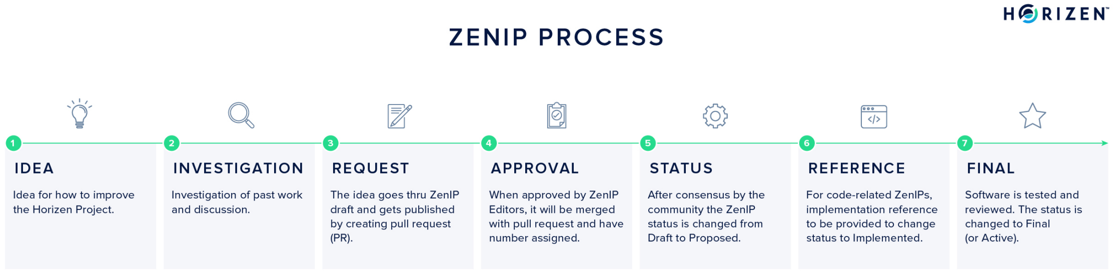
7.2 Zen Improvement Proposals

Protocol Improvement Proposals are an established mechanism to decide upon new features and core protocol changes in many blockchain projects. We adopted our own version of an improvement proposal system — the Horizen Improvement Proposal System (ZenIP). ZenIPs are meant to standardize the process of suggesting major changes to the Horizen codebase and processes around the protocol. This is a key element of transparent, collaborative, and stable governance.

A ZenIP is a document that describes a new feature or process. It explains the rationale behind the proposal and elaborates on why certain design decisions were made. The first ZenIP (ZenIP-42000) specifies the format and structure of a ZenIP as well as the process that will ultimately lead to its activation.

There are different types of ZenIPs, and, depending on the type, the process from proposal to activation differs. *Consensus* and *Standards Track* ZenIPs are code-related and therefore include a more thorough review process than *Process* and *Informational*.

Each ZenIP starts with an *Owner* proposing an idea by specifying it according to the ZenIP process and creating a pull request against the ZenIP repository. The *ZenIP Editors* are responsible for the ZenIP repository and help Owners through the ZenIP process. They will review all Improvement Proposals and merge the pull requests if all requirements are met. At this point, they will assign the ZenIP a number according to the numbering conventions. When the ZenIP has been publicly discussed and any substantiated objections have been addressed the Editors need to approve the ZenIP with a supermajority in order for its status to change to *Proposed*. After the review and testing phases, a ZenIP becomes activated on the Horizen mainnet if it meets our quality standards and reaches consensus within the community.



ZENIP PROCESS

1 IDEA

Idea for how to improve the Horizen Project.

2 INVESTIGATION

Investigation of past work and discussion.

3 REQUEST

The idea goes thru ZenIP draft and gets published by creating pull request (PR).

4 APPROVAL

When approved by ZenIP Editors, it will be merged with pull request and have number assigned.

5 STATUS

After consensus by the community the ZenIP status is changed from Draft to Proposed.

6 REFERENCE

For code-related ZenIPs, implementation reference to be provided to change status to Implemented.

7 FINAL

Software is tested and reviewed. The status is changed to Final (or Active).

Figure 9: Schematic of the ZenIP process.

7.3 Voting System

Our goal is to decentralize decision-making for both resource allocation and technical or other substantive changes to the system. The first steps were to bring other organizations into our ecosystem, extend decision-making authority to collaborative processes, like ZenIPs, and ultimately to implement a democratic system where every ZEN holder is a voter.

In collaboration with IOHK, we have prototyped the voting system described by Zhang, Oliynykov, and Balogun (2019), which is a provably secure voting protocol that is stake-weighted, allows delegation of stake to other voters, rewards voters for participation, and imposes secret balloting using zk-SNARKs.

The general idea of the voting system is to have *Project Owners* submit proposals to be funded to the community. All Zen holders are eligible voters and their vote is weighted according to the locked up stake of each voter. Besides being able to vote on proposals directly, voters will have the option to delegate their vote to an *Expert*, similar to how votes are delegated in a representative democracy. An important distinction is that there are no election terms for which the delegation remains active. Voters can delegate to experts on a case-by-case basis and withdraw their delegation at any time, in effect keeping their delegate accountable. Delegates can further delegate the voting power they accrue, a concept called *liquid democracy*. After a number of proposals have been voted on during one voting period, the accepted proposals will be funded.

Future development of the Voting System should generalize from resource allocation to any type of collaborative decision-making. In this sense, we aim to create a general purpose voting system that can be used for both Treasury and other substantive system changes. It is our goal to render this process fully decentralized such that any ZEN holder can shape the future direction of the project.

7.4 User Owners

Users ultimately own Horizen, and are in control of protocol and ecosystem evolution. The researchers, developers, entrepreneurs, and organizations who created the protocol have the same control rights as any other stakeholders who join at any time. Everyone votes as to what is the latest version of the protocol every time they launch a client and participate in the network.

8 Conclusion

Horizen offers a new type of blockchain-based platform, a system of blockchains with decoupled consensus linked through common CCTP, indefinitely scalable, fully configurable to meet heterogeneous needs, and inclusive of embedded incentives for endogenous growth. The core mainchain is designed as a relatively simple "truth engine" with modified Nakamoto consensus robust to malicious majority attacks, and with application-specific logic offloaded to sidechains designed for those purposes. Our sidechain SDK offers application developers a suite of tools to deploy blockchains that leverage a large compensated node network and a suite of textitzero knowledge privacy tools.

The technology presents a novel approach at compartmentalized architecture that both significantly extends design options and limits adverse spillover from those designs to other parts of the system. In this way, the Horizen ecosystem can grow to include a full complement of services provided by any number of design paths. The project need not choose between specific implementations at the exclusion of alternatives, and no single group of developers is in control of which blockchains or applications enter the ecosystem.

The system is governed by a diverse group of stakeholders in a decentralized, transparent, and collaborative process that balances interests, gives everyone a voice, and democratically allocates resources. Stability is the first objective of our governance framework, and to this end we've introduced a mixture of nonprofit and commercial corporate organizations, academic institutions, and community groups to balance perspectives and interests.

The Horizen team is committed to building a better, more inclusive future for society by providing tools that empower our users. This type of distributed, user-owned network offers a new way of bringing people together, creating and sharing value, and giving voice to everyone by participating in a common ecosystem built on a shared public infrastructure.

We are fortunate to live in an age of incredible innovation in both technology and ideas. We are building on top of the shoulders of the proverbial giants, some of them listed below, but many others go unnamed only because they are so numerous and the contributions so foundational.

References

[1] Garoffolo, A., & Viglione, R. (2018). Sidechains: Decoupled consensus between chains. arXiv preprint arXiv:1812.05441.

[2] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[3] Zhang, B., Oliynykov, R., & Balogun, H. (2019, February). A treasury system for cryptocurrencies: Enabling better collaborative intelligence. In The Network and Distributed System Security Symposium 2019.