HORIZEN™ 2.0:

An Advanced and Efficient EVM for Zero-Knowledge Applications

Horizen Labs Research

research@horizenlabs.io

v1.0 - January 6, 2025

Abstract

We introduce an **EVM chain specifically tailored to building zero-knowledge (ZK) dApps.** By tightly coupling Horizen as a parachain to zkVerify's relay chain, developers gain access to multiple proving mechanisms within EVM-compatible smart contracts. Horizen 2.0 is an EVM with precompile extensions for the most advanced ZK proofs, enabling rapid and inexpensive proof verification. This is designed to overcome the limitations of ZK capabilities on existing networks while enhancing cost efficiency, performance, and trustlessness. Developers can continue to build applications in a familiar way, now with the advantage of leveraging the most optimal proving mechanisms their dApps require. This is only a **starting point of providing ZK tools** to developers creating decentralized applications.

Contents

1 Introduction

Horizen 2.0 aims to be the **most efficient and effective ecosystem** for building blockchain solutions leveraging **zero-knowledge technology.**

Horizen has a long history marrying blockchain with zero knowledge, with the goal of providing individuals sovereignty over their data and monetary activity. We started with the Horizen network and ability for users to transact in a private manner. We then developed a sidechain network with Zendoo, with the goal of scaling throughput by bundling transactions using ZK certificates between sidechains and the mainchain. Due to regulatory concerns of transferring assets, we made a strategic decision to remove private transaction capability from Horizen's network.

The possibilities of integrating ZK have advanced greatly and thus its potential for improving blockchain networks. We see great opportunity in these new capabilities, so we have architected a new network that is more optimal to our ultimate aim. Moreover, the landscape and culture of Web3 has changed over the years with both developers and governments creating a partnership to empower blockchain's real-world benefits. This new approach solves multiple problems for the parties involved by ensuring privacy to users while also transparency to regulators. However it does not end there, there are a wide range of problems to be solved using zero-knowledge technology in decentralized networks.

Blockchain's breakthrough technology completely evolved the landscape for multiple industry sectors; however, its limitations have prevented it from reaching its ultimate potential. Regulatory restrictions and concerns over privacy have made it difficult to reach mainstream adoption. Additionally, blockchain has not been scalable enough for most real-world use cases. ZK cryptography provides the capability needed for blockchain to overcome these obstacles. It does this by **scaling throughput, protecting privacy, and maintaining security** while ensuring decentralization. However, using ZK within EVM (Ethereum Virtual Machine)-compatible smart contracts comes with many challenges such as high gas costs and limited proving mechanisms.

We present Horizen 2.0 as an EVM parachain to the zkVerify relay chain in order to give access to proving mechanisms directly within the application layer. This allows developers to verify proofs **using the proving system best suited to the application** that they are building. While zkVerify [1] can be used from any application or network, doing so within one secure network removes the need for cross-chain communication and further decreases cost. Additionally, the interoperable capabilities within a Substrate environment decreases the latency introduced with normal interchain communication, increasing the speed and overall performance of ZK applications.

1.1 The State of ZK dApps

The need for ZK capability within decentralized applications has reached a critical point. The benefits of ZK are multifaceted, which include the ability to reduce computational load, lower costs, and safeguard data between parties. These advantages have the potential to significantly enhance the functionality within decentralized applications and bring to light previously unseen opportunities for innovation. However, **ZK capability within decentralized applications remains limited,** hindering its widespread implementation and utilization.

Firstly, the vast majority of the Web3 space is built on EVM-compatible applications [2, 3], enabling seamless communication, interoperability, and a common set of tools and protocols. This widespread adoption has made the EVM the technology of choice for building in Web3. However, the EVM standard was not initially designed with ZK capabilities in mind, which necessitated a new set of tools and protocols to build ZK applications (which are not EVM compatible). Unfortunately, these advancements come with a caveat: the need for different programming languages, interfaces, and tools, which can create a barrier to communication and fragmentation within the broader Web3 community.

The alternative to using non-EVM compatible protocols is to use Ethereum for building ZK applications. This comes with two significant challenges: cost and technical limitations. Ethereum is already a congested network, and verifying proofs is a computationally intensive process, making it costly for ZK dApps to operate. Ethereum's verification process for zk-SNARKs is restricted to a single elliptic curve, alt_bn128, and constrained types of proving systems (e.g. Groth16) whose proofs are relatively cheaper to verify on the Ethereum network. This both limits capability and decreases efficiency.

ZK technology is advancing swiftly, necessitating more sophisticated proving systems for optimal performance. It requires an ecosystem that can keep pace with its advancements. Since the introduction of Ethereum's precompiled contracts, which provide a set of mathematical operations used for verifying proofs, seven years have passed without any significant updates to the proving methods. Given Ethereum's extensive network and multitude of priorities, of which ZK is just one, it is improbable that Ethereum can keep pace with developments in this dynamic space.

1.2 Our Contribution

Horizen's goal is to **provide an ecosystem with advanced and efficient tools for building ZK dApps** while ensuring cost-effectiveness. Being part of a network optimized for proof verification (zkVerify) fosters a symbiotic relationship that makes this possible. Each

module is designed for a specific purpose yet can seamlessly hand off processes to other specialized modules, resulting in optimal performance and shared capabilities.

The new iteration of the Horizen ecosystem will be an EVM parachain to zkVerify's relay chain. This integration enables the EVM to **leverage the latest proving mechanisms within the smart contract application layer,** providing unparalleled flexibility. Horizen is the first to build this solution, bringing unprecedented interoperability for ZK applications with the rest of Web3.

Moreover, Horizen's ecosystem will be better equipped to keep pace with this rapidly evolving space, as its primary focus is zero-knowledge technology. Offering additional tools and enhancing ZK capabilities will remain the primary driving force within this ecosystem.

1.3 A Parachain to zkVerify

Horizen as a parachain to zkVerify relay chain comes with many strategic benefits. zkVerify is a chain whose singular purpose is to verify proofs. Attaching Horizen to zkVerify allows for optimal verification possibilities directly within the application layer, removing the challenges currently existing within EVM environments. Adhering to this modular approach, each chain can optimize for its own use case while also being able to access features from each other. This is a characteristic advantage to using Substrate as builders can achieve interoperability while maintaining security. Lastly, zkVerify is a network whose main focus is providing services for applications using ZK, and its growth will only continue to add value to Horizen's EVM and the possibilities available to smart contract developers.

2 Horizen 2.0 Architecture

2.1 Overview

Horizen 2.0 is the **first specialized EVM blockchain designed with precompiles directly built into the EVM for proof verification.** It is the home for ZK dApps, where a ZK dApp is defined as any type of decentralized application (dApp) that generates, utilizes, and/or verifies ZK proofs.

Developers of ZK dApps often encounter difficulties in writing and auditing verifier contracts, which are essential for validating ZK proofs. These custom contracts are not only complex but also prone to vulnerabilities that can be exploited. The need for a more streamlined and secure solution has led to the development of Horizen 2.0, which offers **built-in precompiled contracts to handle proof verification,** thus reducing development overhead and enhancing security.

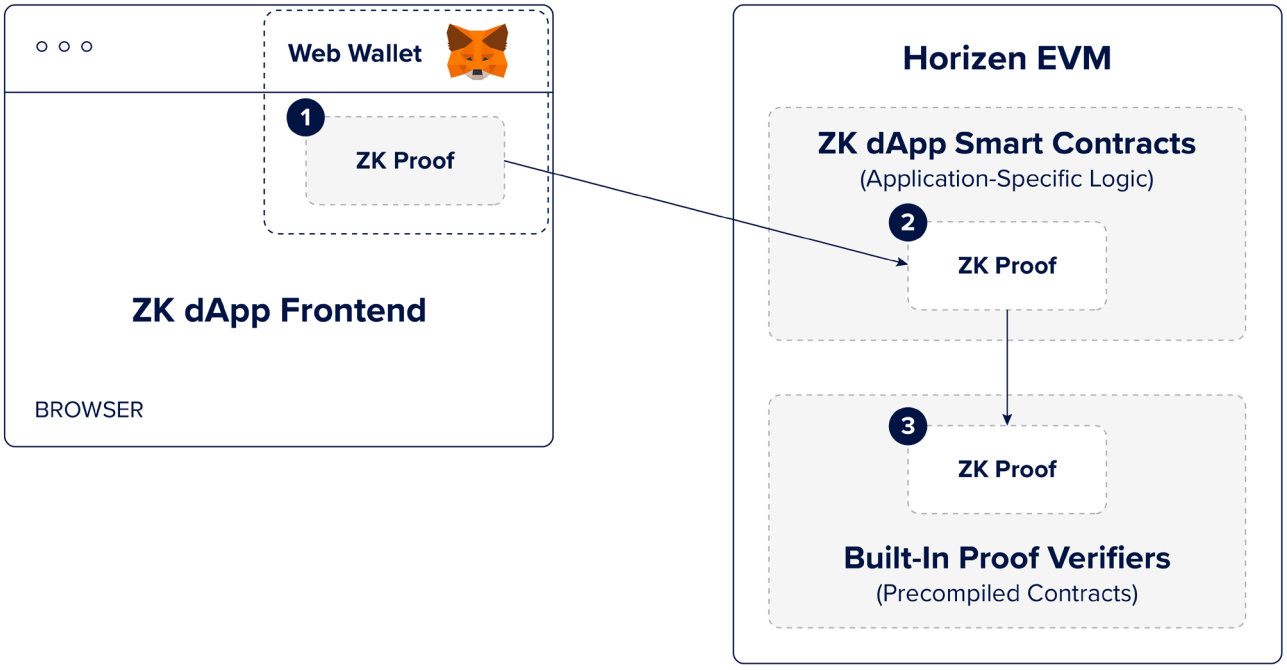


Figure 1: High-level workflow of a ZK dApp, interacting with the built-in proof verifiers provided by the Horizen EVM as precompiled contracts. ZK dApps no longer need to write nor audit verifier contracts on their own.

Precompiled contracts are specialized, internal contracts embedded directly within the EVM. These contracts are designed to perform complex and computationally intensive operations more efficiently than if they were implemented in Solidity. By being integrated into the EVM, **precompiled contracts can execute operations at a lower gas cost and higher speed, providing significant performance benefits.**

In Horizen 2.0, the precompiled contracts (also known as precompiles) are specifically designed to handle the verification of ZK proofs. These precompiles include verifiers for an expansive range of ZK proof systems, such as Groth16 [4], Fflonk [5], RiscZero [6], and UltraPlonk [7]. Each precompiled contract encapsulates the necessary cryptographic operations within it, including elliptic curve operations, hash functions, and pairing-based cryptography.

ZK dApps can easily access the functionality of these contracts, each identifiable by its unique smart contract address.

Contract	Solidity Smart Contract Address
Generalized Verifier	0x0000000000000000000000000000000000000800
Groth16 Verifier	0x0000000000000000000000000000000000000801
Plonk Verifier	0x0000000000000000000000000000000000000802
Fflonk Verifier	0x0000000000000000000000000000000000000803
UltraPlonk Verifier	0x0000000000000000000000000000000000000804
Halo2 Verifier	0x0000000000000000000000000000000000000805
STARK Verifier	0x0000000000000000000000000000000000000806
Boojum Verifier	0x0000000000000000000000000000000000000807
RiscZero Verifier	0x0000000000000000000000000000000000000808
...	...
Binius Verifier	0x0000000000000000000000000000000000000888

Figure 2: An illustration of precompiled contracts and their potential addresses, allowing ZK dApp developers to directly verify their ZK proofs simply by utilizing the built-in functionality of Horizen 2.0's EVM precompiles.

2.2 Key Components

2.2.1 Node Architecture

Horizen 2.0 utilizes the Substrate framework [8] to structure its node architecture into two main components: the Core Client and the WebAssembly (Wasm) runtime. This division allows for a modular and efficient design where there is a clear separation of responsibilities:

1. **Core Client:** Serves as the foundational layer, handling network activity such as peer discovery, managing transaction requests, reaching consensus with peers, and responding to RPC calls.

2. **Horizen Runtime:** Contains all of the business logic for executing the state transition function of the blockchain. This involves creating new modules (pallets in Substrate jargon) and integrating them with built-in ones.

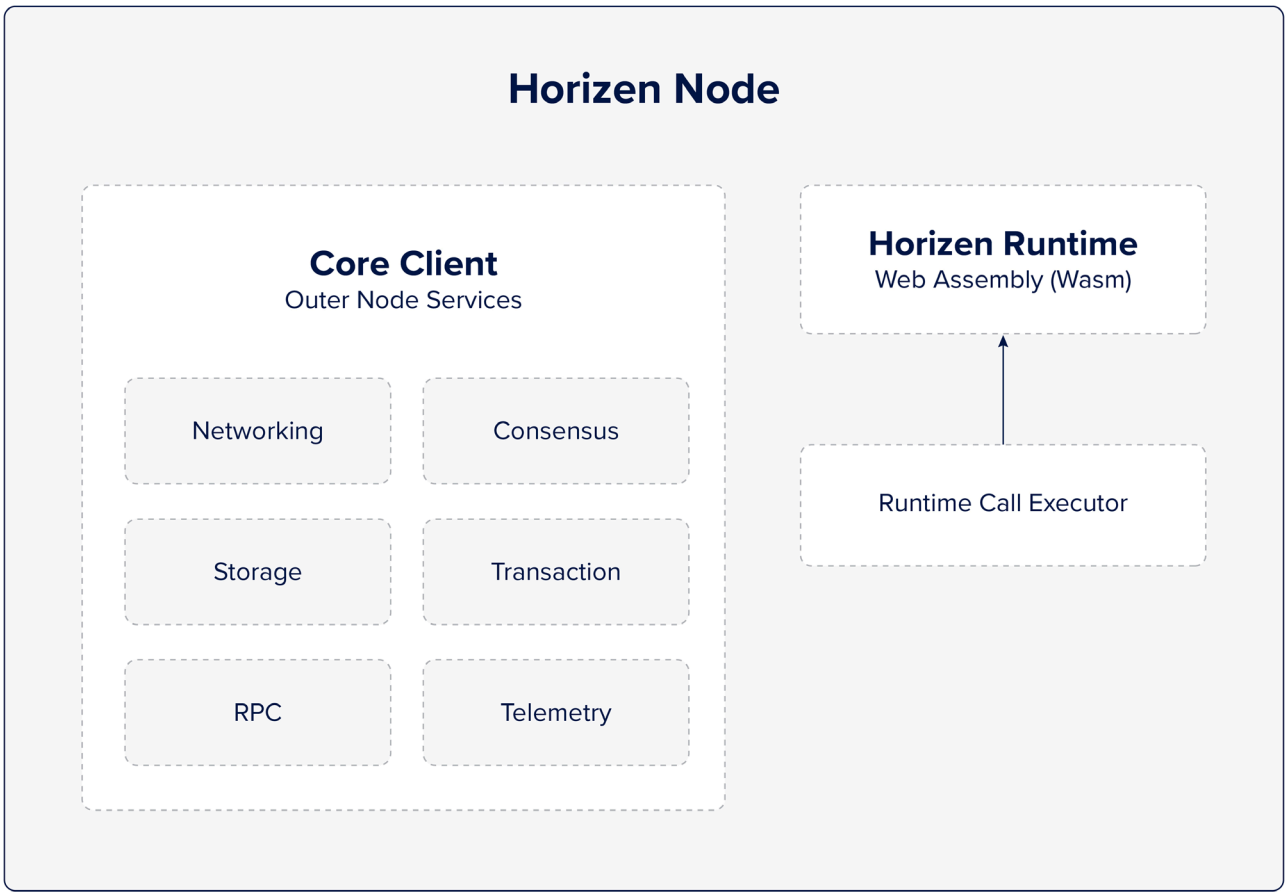


Figure 3: A view into a Horizen node, which utilizes the Substrate framework to structure the node architecture into two main components: the Core Client and the Horizen Wasm Runtime.

2.2.2 Horizen Runtime

The Horizen Runtime is an advanced and highly-configurable WebAssembly (Wasm) runtime built using Substrate's FRAME (Framework for Runtime Aggregation of Modularized Entities). FRAME allows developers to create modular, reusable, and composable runtime components known as pallets.

At the heart of the Horizen Runtime are the proof verification pallets. These specialized pallets are solely responsible for verifying ZK proofs: each of them will expose the functionality through an EVM precompile enabling ZK dApp developers to access verification functionality in a synchronous way.

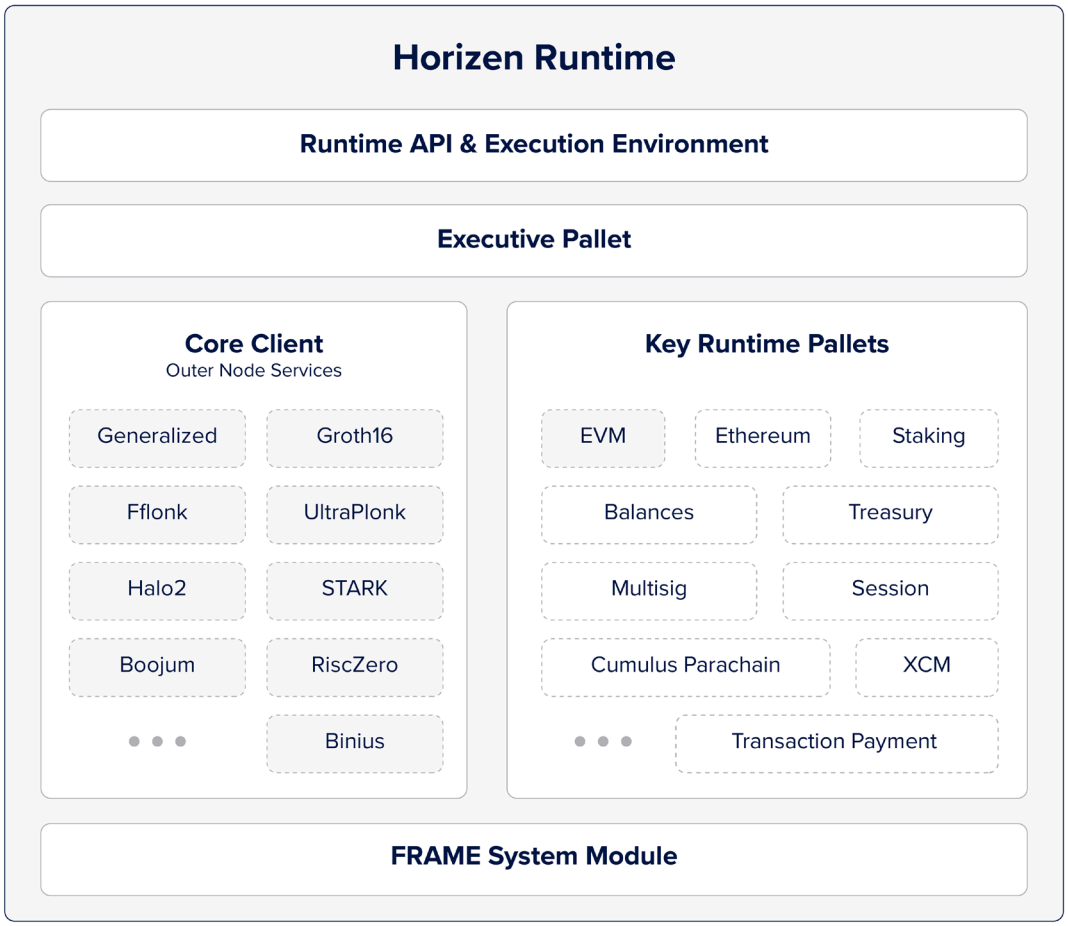


Figure 4: A deeper look into the Horizen Runtime, highlighting the various proof verification pallets and their integration with the EVM pallet. This integrated approach enables the use of precompiled contracts for efficient and secure ZK proof verification in zkDApps.

Each precompile is optimized for rapid and synchronous verification of proofs (within milliseconds for some proof types) with a focus on cost efficiency.

2.2.3 Generalized Verifier

The Generalized Verifier is a **unique precompile that taps directly into the capabilities of zkVerify's comprehensive verification framework,** giving access to the most recent verifiers that may not yet be available in Horizen 2.0 precompiles. It allows developers to pass the name of the proof type and the corresponding verification key, leveraging the broad array of verifiers available on zkVerify. This integration is facilitated by the tight relationship between Horizen 2.0 operating as a parachain to the zkVerify Relay Chain. Utilizing Cross-Consensus Messages (XCM), the Generalized Verifier enables asynchronous proof verification, abstracting the complexities involved in the process. This design

simplifies integration and expands the range of supported cryptographic protocols for ZK dApps. When new proof verifiers are added to zkVerify, they are immediately available for use by Horizen 2.0 developers.

Figure 5: A depiction of the Generalized Verifier's workflow, showing its direct access to zkVerify's latest proof verifiers, including those not yet available in Horizen 2.0 precompiles. This is done by passing the proof, proof type, public inputs, and verification key to the Generalized Verifier.

One of the key aspects of the Generalized Verifier is its asynchronous nature. Unlike the other precompiles that perform immediate, synchronous verification, the Generalized Verifier allows proof validation to occur independently of other processes. This flexibility lets developers integrate zkVerify's comprehensive verification capabilities into ZK dApps that may not need instantaneous validation, enabling more efficient and scalable applications.

2.3 DPoS Consensus

Delegated Proof of Stake (DPoS) is a consensus mechanism that enhances the efficiency and scalability of blockchain networks by introducing a **layer of delegation in the staking process.** Token holders vote to elect a small number of delegates who are responsible for producing blocks and maintaining network operations. DPoS is currently the consensus mechanism for EON and will continue to be used in Horizen 2.0, ensuring continuity and stability. However, in this new iteration, EON forgers will be referred to as **collators**, reflecting their role within the parachain structure.

Horizen 2.0 will adopt a hybrid consensus model inspired by Moonbeam [9], which has successfully implemented DPoS to achieve high performance and scalability. Accordingly, the Nimbus framework [10] will be employed for the selection of collators, ensuring a sophisticated and fair process. The chosen block will then be validated by zkVerify's Relay Chain validators using BABE (Blind Assignment for Blockchain Extension) [11] for block production and GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement) [12] for block finalization.

Collator selection is a sophisticated process, utilizing filters to ensure that only the most qualified participants are chosen, while using a secure source of entropy to maintain fairness and prevent collusion. The structure includes three key aspects: the Staking Filter, the Fixed Size Subset Filter, and the Entropy Source. Each of these aspects plays a critical role in ensuring the efficiency and fairness of the network:

1. **Staking Filter:** Determines the eligibility of collator candidates based on their amount of stake. Only qualified and committed participants are eligible to produce blocks and maintain network operations, thereby enhancing overall reliability.

2. **Fixed Size Subset Filter:** Further refines this pool of candidates to a manageable number of active collators for each block production slot. It ensures that a predetermined number of collators are elected to maintain the network, providing a balance between decentralization and efficiency.

3. **Entropy Source:** Introduces a secure and unpredictable element of randomness to prevent collusion and ensure a fair distribution of validation responsibilities.

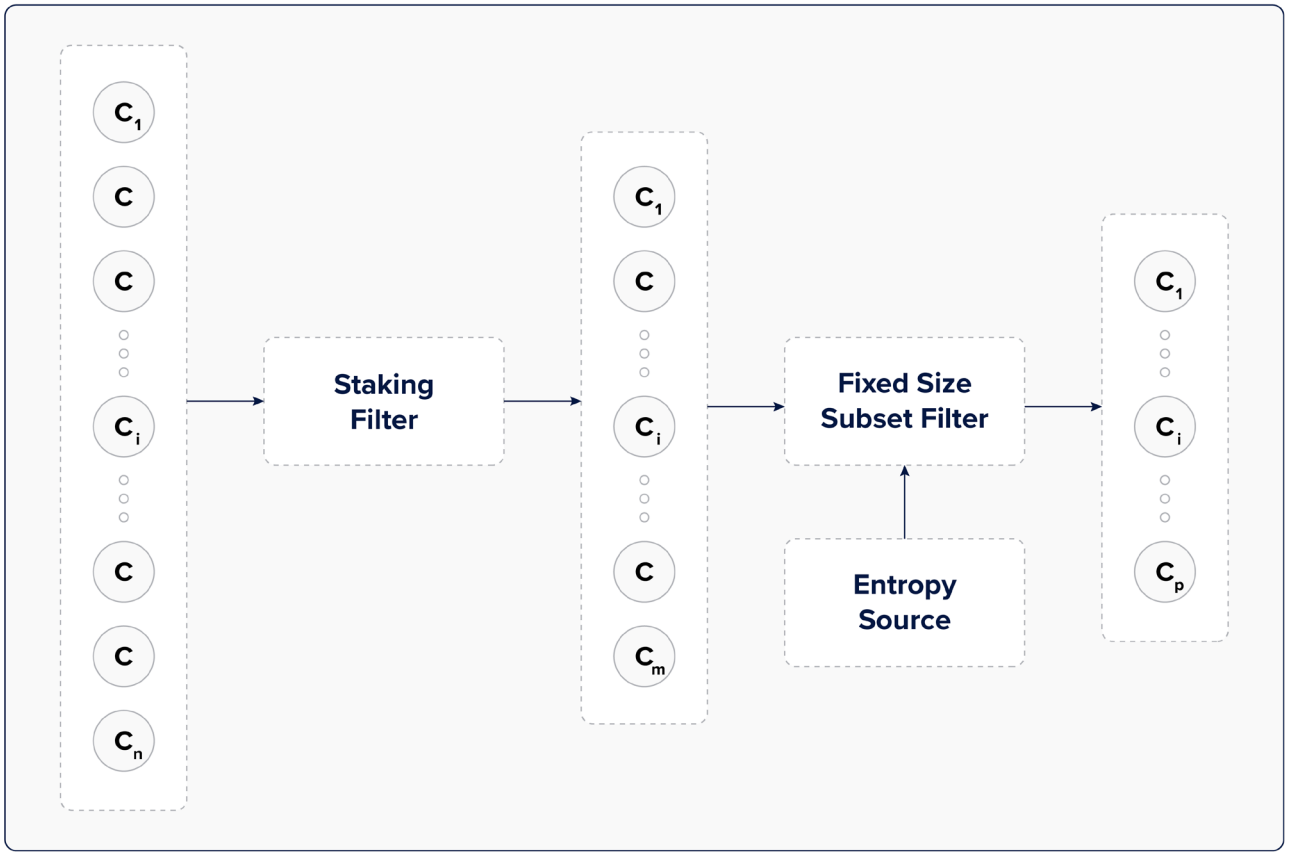


Figure 6: Horizen 2.0 employs Delegated Proof of Stake (DPoS) as its consensus mechanism. The diagram highlights the Staking Filter, Fixed Size Subset Filter, and Entropy Source, which together ensure the selection of qualified collators and maintain network fairness.

3 Tokenomics

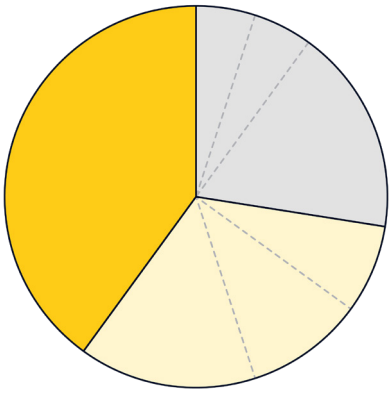
3.1 Overview

The 21 million maximum supply of existing $ZEN will be preserved in the tokenomic model for Horizen 2.0. As Horizen is moving from a proof-of-work to proof-of-stake consensus mechanism, it necessitated some strategic changes. This was outlined in **ZenIP-42407** and approved by the Horizen DAO.

As a fair launch, no pre-mine, no ICO project, Horizen's current block reward allocations do notreflect the modern needs for ecosystem growth. To ensure Horizen's success, a tokenomicsstrategy that aligns with this new direction is crucial. This tokenomics strategy aims to create amore effective framework to accelerate the growth of the Horizen ecosystem while equipping thecommunity with the resources necessary to seize new opportunities, while also honoring the project's legacy max supply cap.

3.2 ZEN Allocations for Horizen 2.0

- **Collator Rewards 40.0%**
- **Horizen Foundation 32.5%**
  Ecosystem Development 15.0%
  $ZEN Growth & Stability 10.0%
  Infrastucture 7.5%
- **DAO Treasury 27.5%**
  ZEN Sustainability Initiative 17.5%
  Community Grants 5.0%
  Growth Marketing 5.0%



Collator nodes contribute to the security of the network by gathering transactions from users and generating state transition proofs for main chain validators. This allocation will ensure proper participation of the network, as well as a competitive reward structure for delegators. The 40% of future ZEN emissions allocated to Collator rewards will be divided between Collators and $ZEN Delegators as follows:

Collator Rewards Splits %

Collator Commission	85%	Delegator Reward	15%

To encourage holders to delegate their $ZEN and participate in network security, we allocate 85% of Collator $ZEN block rewards to its delegates, with 15% retained by the Collator for its node operation services. We recommend allowing Collators to set their own custom reward split with their $ZEN delegates as a future post-launch update.

3.3 Emission Schedule

For the Horizen Foundation and the DAO Treasury allocations will be moving from a per-block emission schedule to a vesting schedule which would release 25% of the allocation at migration, with the remaining 75% to vest linearly, with monthly unlocks, for 48 months. This would result in an increased circulating $ZEN supply at migration, as well as more circulating $ZEN in the short-term. However we believe that unlocking additional resources during the migration to Horizen 2.0 provides the greatest opportunity to cement Horizen at the forefront of ZK application in web3.

Group	Vesting Terms
ZEN Holders	100% at Migration
Horizen Foundation	25% at Migration, linear monthly vesting over 48 months
DAO Treasury	25% at Migration, linear monthly vesting over 48 months
Security Budget	Per Block Emissions via Halving Schedule

$ZEN ‘Security Budget’ paid to Horizen 2.0 Collators will continue to be issued on a per block basis with the emissions rate continuously declining to preserve the 21m $ZEN supply cap. See ‘Replacing the Halving Schedule’ below.

Proposed ZEN Emissions	
ZEN Migrated *	16,000,000
Additional ZEN Unlocked ^	750,000
Circulating ZEN Supply at Migration	**16,750,000**
ZEN Subject to Vesting	2,250,000
ZEN to be emitted via block rewards	2,000,000
Max ZEN Supply	**21,000,000**

* The circulating supply of 16m ZEN at migration was chosen for illustrative purposes, the actual circulating supply at migration will be determined by total circulating ZEN across Horizen PoW and EON chains at migration.

^ In this example the additional ZEN unlocked is equal to 5m ZEN future emissions * 25% vesting at migration * 60% to Horizen Foundation and DAO Treasury.

3.4 Horizen Foundation Allocation

Since there was no premine or initial coin offering precluding the launch of the Horizen network, the community has relied on its 20% allocation of $ZEN block rewards to fund all community initiatives and development. As part of the migration to Horizen 2.0, we propose increasing the Horizen Foundation's share of future block rewards to 32.5%. This will be used to fund the Foundation and its ecosystem development efforts over the long-term. The Horizen Foundation may diverge from these funding guidelines at their discretion, with use of funds from this allocation detailed in the periodic Horizen Foundation transparency reports.

This adjustment will allocate 32.5% of $ZEN emissions to the Horizen Foundation to fund community resources: Ecosystem Development (15%), $ZEN Growth & Stability (10%), and chain infrastructure (7.5%). This allocation will fund the Foundation's operations long-term. While the spending of $ZEN from this allocation will be at the discretion of the Foundation we recommend funds be deployed as follows:

Ecosystem Development	15%	Long-term funding for the operations of Horizen Foundation, its ecosystem development efforts, and maintenance of the Horizen network.
$ZEN Growth & Stability	10%	Funds used to support stable $ZEN markets across both CEX & DEX.
Infrastructure	7.5%	Funds allocated to Horizen 2.0 application integration fees and support of the network's long-term infrastructure needs.

3.5 DAO Treasury

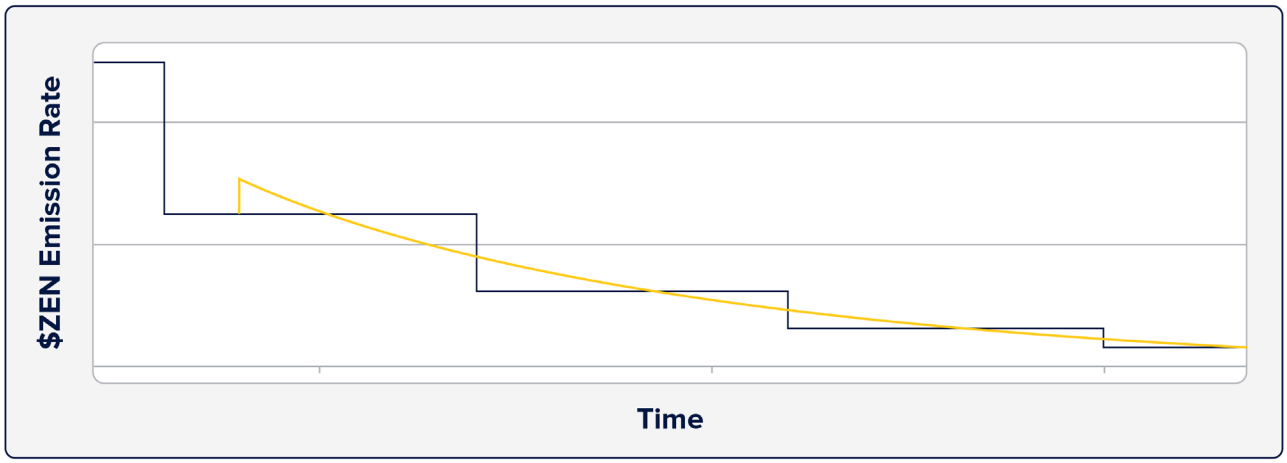
An allocation of 27.5% of $ZEN emissions will go to the DAO Treasury, which is divided into individual tracks. Each track will have its own dedicated funds, with voting conducted exclusively within the scope of those allocated resources. This approach ensures that the community avoids overspending or underspending in any specific area, while ensuring that each track receives the necessary attention and care.

ZEN Sustainability Initiative	17.5%	This is considered one of the most crucial initiatives. The ZK dApp space is still in its early stages and is primed for disruption. The community should focus on funding the next generation of groundbreaking dApps that can transform the decentralized world and challenge traditional industries. To achieve this, we should attract top-tier projects to build within the Horizen ecosystem by offering funding, supporting their efforts, and backing their product initiatives. In return, these funded projects should be required to allocate a portion of project revenue back to the Horizen ecosystem. We propose a governing bodyfor this track to negotiate terms with projects thatinclude revenue shares with the ecosystem via contributions back to the Sustainability Initiative. This will ensure future growth and sustainability of the community.
Grants	5%	For funding requests not suitable for the Sustainability Initiative.
Growth and Marketing	5%	Allocated to drive growth initiatives and support awareness campaigns.

3.6 Replacing the Halfing Schedule

The ZEN community has indicated a clear desire to preserve the 21m max $ZEN supply, which is currently implemented via fixed per-block $ZEN emissions halving every four years. While this is an essential element of $ZEN tokenomic design, abrupt halving events have their downsides. Halving events often bring significant market uncertainty, disrupting both the market and the broader ecosystem. Since users and traders are aware of the halving date well in advance, it can lead to excessive speculation and potentially diminish network participation if users anticipate a sudden 50% cut in rewards.

To address these deficiencies, we propose a smoothly-declining $ZEN emissions rate via Collator / Delegator rewards, which halves over the same time period. Max supply of $ZEN would remain at 21m. In the chart below, the effect of the proposed approach is demonstrated by the green line, versus the current halving schedule depicted by the gray line:



This has the potential to reduce unnecessary speculation and unexpected behavior around a single event. This can bring a level of predictability while promoting healthy participation within the network, attracting a more loyal user base.

3.7 Rational

The community will need the ability to compete in an aggressive market. By providing sufficient resources at migration, we ensure the community can fund network growth and develop strategies to attract developers for ZK applications. Additionally, the vesting schedule for these funds safeguards the community and promotes responsible spending.

The reward allocation for Collators and their $ZEN Delegates will promote adequate participation in protocol staking, while encouraging users to continue to accumulate and hold $ZEN.

This tokenomics will optimally drive the growth of the Horizen ecosystem while still maintaining the existing supply of 21 million tokens.

4 Horizen 2.0 Use Case

There are many problems that can be solved by using ZK technology in decentralized applications. **The power to prove knowledge without revealing data ensures trust between parties, entities and platforms.** This not only benefits end users, but also the ways in which systems interact with each other. While the use cases defined here are broad and are associated with ensuring trust by proving knowledge of data, many use cases have yet to be defined.

4.1 Identity

Being able to verify specific personal details within decentralized applications is incredibly valuable. Some examples of this:

1. Businesses may require users to reveal certain aspects of their financial past before using a platform, such as their credit score or record of due diligence. Applications using ZK can verify thresholds for these credentials without revealing specifics.

2. Applications that need to review medical records may require proving ownership, providing specific data points, as well as authorization to pass information between parties.

3. Proof of uniqueness ensures that each participant's digital identity is distinct and verifiable. This is crucial for maintaining the integrity and security of a DAO's decision-making processes and governance.

4. Any decentralized application that relies on user reviews would benefit from verifying the identity of users.

5. It's very common that laws require users to prove personal details in order to use a service, such as opening up a bank account. With ZK proofs, users can engage in digital banking without the need to divulge unnecessary personal details.

6. A protocol that facilitates trading specialized financial instruments may require users to be accredited investors. By verifying identity alongside specific credentials, it can ensure that users are authorized to trade without revealing their personal identities.

7. Laws may require users purchasing digital assets on a platform to be of a certain age. ZK proofs can verify that users meet the age requirement without disclosing their identities.

8. Local governments may mandate that users in specific areas pay sales tax or restrict access to certain platforms based on jurisdiction. ZK technology can verify a user's state or country of residence without disclosing any additional personal information.

Blockchains allow users to engage in transactions on public networks in a pseudo-anonymous fashion. There are a multitude of issues that arise because of this. While anonymity is a main tenet of blockchain, the inability of dApps to verify who is interacting with their platform has made it difficult to comply with regulations. Governments' concern over the use of specific platforms has put the industry at odds with regulators and has made it difficult for ventures to thrive. A platform's ability to prove identity ensures compliance. Regulators are focused on addressing a variety of issues, including tax evasion, money

laundering, and other financial crimes. These concerns are driven by the need to maintain the integrity of the financial system and prevent illegal activities that undermine public trust. However, this remains at odds with law abiding users who do not want to reveal their identities and/or financial activity. ZK proofs open the door to consolidation between concerned parties.

All platforms need to do is present the proofs to relevant parties to ensure regulatory compliance while protecting user data. This is not an exhaustive list; there are numerous ways identity verification can be integrated into smart contracts.

4.2 Decentralized Finance (DeFi)

Some examples in which proofs could be used to enhance DeFi:

1. New ventures may have developed innovative trading strategies, providing them with a competitive advantage over their rivals. To safeguard their intellectual property, it would be beneficial for these ventures to maintain confidentiality regarding their trades. Public ledgers, which typically record all transactions, would otherwise reveal their strategies, compromising their competitive advantage.

2. DeFi has been prone to sniping, which is a sophisticated trading tactic used by quant traders to front-run transactions in protocols. The nature of how blockchains are built allow for this. ZK can hide the details of these trades from bad actors.

3. Some trading algorithms require substantial computation, making blockchain usage prohibitively expensive. Offloading computation with ZK technology could enhance both profitability and scalability.

DeFi has revolutionized the financial landscape and expanded opportunities for investors, but in many cases, it has not yet achieved the maturity of traditional finance. While decentralized ledgers enhance sovereignty, they also introduce challenges. Traditional finance follows a set of necessary regulations within nations, many of which are designed to protect individuals. Moreover, trading on a public ledger can expose information that users may prefer to keep private. These are just some of the many ways in which ZK could improve DeFi protocols.

4.3 Voting

ZK introduces ways in which:

- Voters can prove their identities, without revealing personal information, enabling secure participation.
- Voters can prove they have cast a valid vote without revealing their actual choice, maintaining the secrecy of individual votes while still allowing verification of the overall election results.
- Create a publicly verifiable record of votes on the blockchain, allowing voters to check if their vote was successfully cast and counted.
- Can be used to optimize the voting process, reducing the computational overhead and increasing the scalability of the voting application.

Because of blockchain's immutability, it is a prime candidate for ensuring trust and security in voting systems. Recently there has been increased concern for societies over the trustworthiness of elections. This is not limited to solely government institutions, but also private institutions and communities.

Governments need to ensure only citizens are voting, and are only doing so once. Moreover, citizens might not want to reveal who or what they are voting for. Even blockchain's introduction of DAOs suffer from similar voting challenges.

4.4 Gaming

There are many interesting use cases which open up possibilities never possible previously.:

- Prove possession of in-game items or completion of challenges/quests without divulging exact details.
- Ensure that players' actions are kept private until they decide to reveal them, preventing cheating and maintaining a level playing field. An example are games requiring fog of war to be maintained while performing public actions.
- Ensure programs are behaving honestly, such as gambling algorithms, or any computation that ensures fair probability.

- Enhance web2 games with web3 features, using zk-proofs to manage the transition on and off-chain.

There are many aspects within gaming that require either intensive computation and/or data to be protected.

4.5 Verifiable Computing

There are many instances where applications require intense computation. However, executing programs on decentralized networks is often impractical due to economic constraints. Verifiable computation in smart contracts provides a solution by ensuring that programs are executed in a trustworthy manner. Risc0 is a pioneering service in offloading computation, and Horizen's ability to verify Risc0 proofs makes it an ideal candidate for developing ZK applications.

Additionally ZK co-processing enables smart contracts to request off-chain computation from coprocessors with access to extensive data. Results of the computation can be returned along with public inputs and a ZK proof of validity.

Moreover, there is the potential for significant cost savings and performance improvements to rollup solutions. Rollups would be able to settle transactions on Horizen by utilizing cheap and fast proof verification, without the need to perform off-chain aggregation or STARK to SNARK conversion.

4.6 Bridge Technology

One of blockchain's biggest challenges is interoperability. Due to independent chains' inability to communicate, bridges were built to send and receive assets or messages to each other. This has been fraught with many issues, mainly due to the necessity of centralized systems to maintain state and communication between chains. Security breaches have become common, resulting in the loss of millions of dollars worth of assets. However, much of this is being improved through the use of ZK technology.

ZK proofs reduce the necessity of trust between parties, as networks can transmit evidence of state transitions from sender to receiver chains [13].

4.7 zkML

With the advent of artificial intelligence (AI), there arises multiple trust issues because machine learning (ML) requires very large datasets for predictions and decision making. Some of the trust issues revolve around keeping the data private, making sure data is not tampered with, and ensuring the machine learning algorithms are operating as they say they are. These trust issues make using blockchain a prime candidate for resolving such problems. ZK becomes a prime candidate for marrying AI and blockchain, as it can verify input data has gone through a proper ML model, without revealing the parameters of the model itself. Operating in a trustless manner could mean that ML algorithms are operated in an open platform (executed directly within a smart contract) or that their operation is provable (verifying a proof on-chain that ensures accurate execution). There are a vast number of applications that could benefit from trustless AI, such as social media platforms, healthcare, risk assessment, and DeFi [14].

The increased barrier to entry for computer hardware running AI software coincides with the emergence of Decentralized Physical Infrastructure Networks (DePIN). Blockchain management systems can be developed to lend out real world infrastructure in a decentralized fashion [15]. Decentralized applications will likely need to verify nodes are executing AI models correctly, supplying proofs that attest to the truthfulness of execution. This will require a protocol that is well-equipped at verifying the most advanced zk-SNARKS, of which Horizen will support.

4.8 Deep Fakes

Recent developments in AI have also raised concern over the ease and professionality at which content can be created or altered. Photo, video, or any media file for that matter can be manipulated to distort reality and promote misinformation. This could be very damaging and dangerous to society, however there are steps being taken to protect against nefarious action.

Authentication of media files is not a new development, however users need to trust a source for verifying authenticity of data. Media files can be converted to hashes which are stored on-chain as a source of truth for validating authenticity [16]. This is only helpful however for authenticating media which has not been altered.

There are numerous reasons why media files should be editable, however. Edits to media files may be necessary for creative purposes or to remove sensitive information from the original media. When the original media needs to remain confidential, the creator may permit such transformations. To protect sensitive parts of the data, zero-knowledge

proofs can be used to verify whether the changes fall within the accepted list of possible transformations a user can make [17]. The results of verifying these proofs, which could be stored on-chain, can help preserve the authenticity of the transformed content [18].

5 Standard Approach for Building ZK dApps

The Horizen protocol has the potential to **establish a standardized approach to building ZK dApps.** We can achieve this by providing rails to the various building blocks within each stage of the ZK development user journey. We'll continue to get feedback and refine this process, with the goal of developing a common and efficient framework for building decentralized ZK applications. Horizen attempts to not only improve this nascent user journey, but to define it.

6 Conclusion

Horizen's EVM is poised to revolutionize the development landscape by enabling multipurpose zero-knowledge verification within smart contracts. It will achieve this with scalability and cost efficiency while also maintaining security and decentralization. This will influence a significant amount of new developments to various industry sectors which were previously unachievable. Horizen will advance projects in DeFi, AI, gaming, identity, and more, pushing beyond their current limitations and inspiring entirely new developments.

This EVM is a complementary way of providing additional value to an ecosystem already supplying tools for ZK efficiency. Substrate's modular approach decouples the responsibility for security and other features, and allows several units to work together in unison. There are several components needed to build optimal ZK applications, each with their own technical challenges and frameworks.

Attaching Horizen to a network optimized for ZK allows for several modules to work together in a specialized manner (Horizen EVM + zkVerify), yet also allows Horizen's ecosystem to continue to grow within that network.

7 References

[1] Horizen Labs Research, “zkVerify Protocol Whitepaper,” https://downloads.horizenlabs.io/file/labs-web-assets/zkverify-protocol-whitepaper.pdf, 2024.

[2] B. Liu, “Two-thirds of EVM smart contract deployments in 2024 are from Optimism,” https://blockworks.co/news/evm-smart-contract-deployments-optimism, March 2024.

[3] G. Matos, “EVM chains see over 637 million smart contracts deployed since Jan 2022,” https://cryptobriefing.com/evm-smart-contract-deployment-surge/, March 2024.

[4] J. Groth, “On the size of pairing-based non-interactive arguments,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques, https://eprint.iacr.org/2016/260.pdf, 2016.

[5] A. Gabizon and Z. J. Williamson, “fflonk: a Fast-Fourier inspired verifier efficient version of PlonK,” https://eprint.iacr.org/2021/1167, 2021.

[6] J. Bruestle, P. Gafni, and the RISC Zero Team, “RISC Zero zkVM: Proof System in Detail,” https://dev.risczero.com/proof-system-in-detail.pdf, August 2023.

[7] Aztec Network, “Aztec Protocol: Proving System Components - UltraPlonk,” https://docs.aztec.network/protocol-specs/cryptography/proving-system/overview, 2024.

[8] Parity Technologies, “Substrate Documentation,” https://docs.substrate.io/, 2023.

[9] Moonbeam Foundation, “Moonbeam Network Resources & Documentation,” https://docs.moonbeam.network/, 2024.

[10] Moonbeam Foundation, “Nimbus Parachain Consensus Framework,” https://docs.moonbeam.network/learn/features/consensus/, May 2024.

[11] H.Alper, “BABE: Blind Assignment for Blockchain Extension protocol,” https://research.web3.foundation/Polkadot/protocols/block-production/Babe.

[12] Stewart, A., Kokoris-Kogia, E., “GRANDPA: a Byzantine Finality Gadget,” https://github.com/w3f/consensus/blob/master/pdf/grandpa.pdf, June 2020.

[13] Bybit Team, “Polyhedra Network (ZKJ): zk-Proof Innovations to Advance Web3,” https://learn.bybit.com/defi/what-is-polyhedra-network-zkj/, June 2024.

[14] SevenX Ventures, “Balancing the Power of AI/ML: The Role of ZK and Blockchain,” https://medium.com/@wunderlichvalentin/balancing-the-power-of-ai-ml-the-role-of-zk-and-blockchain-f07f48855b10, May 2023.

[15] J. Agbo, What Is the Decentralized Physical Infrastructure Narrative in Crypto?, “https://www.coingecko.com/learn/depin-crypto-decentralized-physical-infrastructure-n etworks”, May 2024.

[16] World Economic Forum “Blockchain can help combat the threat of deep fakes.” https://www.weforum.org/agenda/2021/10/how-blockchain-can-help-combat-threat-of-deepfakes/, October 2021.

[17] E. Neiger, “How to Beat Deep Fakes (Part 1)”, https://www.ingonyama.com/blog/how-to-beat-deep-fakes-using-zero-knowledge-crypt ography-for-audio-video-and-image-verification, July 2023.

[18] Eth Global, “ZK Microphone”, https://ethglobal.com/showcase/zk-microphone-8161v, 2023.