



From Concept to Code:

Integrating zkVerify into your dApp

Daniele Di Benedetto - Engineering Manager, zkVerify
Steve Rushby - Senior QA Automation Engineer
Luca Giussani - Cryptographic Engineer



Agenda

- **Background Context**
- **Technical Core**
- **Web2 Apps Integration**
- **Web3 DApps Integration**
- **Looking Ahead**



Background Context

Current: World of Continuously-Generated Data



Highlights (Data Created Per Minute)

- 46.1 Million WhatsApp Messages
- 241 Million Emails
- 102 MB of Data Per Person
- 360K Tweets Sent on X
- ~7K Prompts to Chat GPT

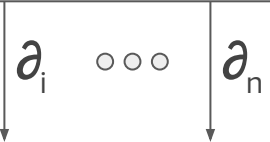
Source: Digital Information World, Dec 2023.

Explosion of Data: Continuous & Overflowing



Web 2

- Web Browsers
- Mobile Devices
- Social Media



Web 3

- Decentralized Blockchains
- Privacy Applications
- ZK Virtual Machines



Web 4

- Artificial Intelligence (AI)
- Internet of Things (IoT)
- Augmented & Virtual Worlds



∂ = Data Created

Future: *Continuous Stream of Proofs*

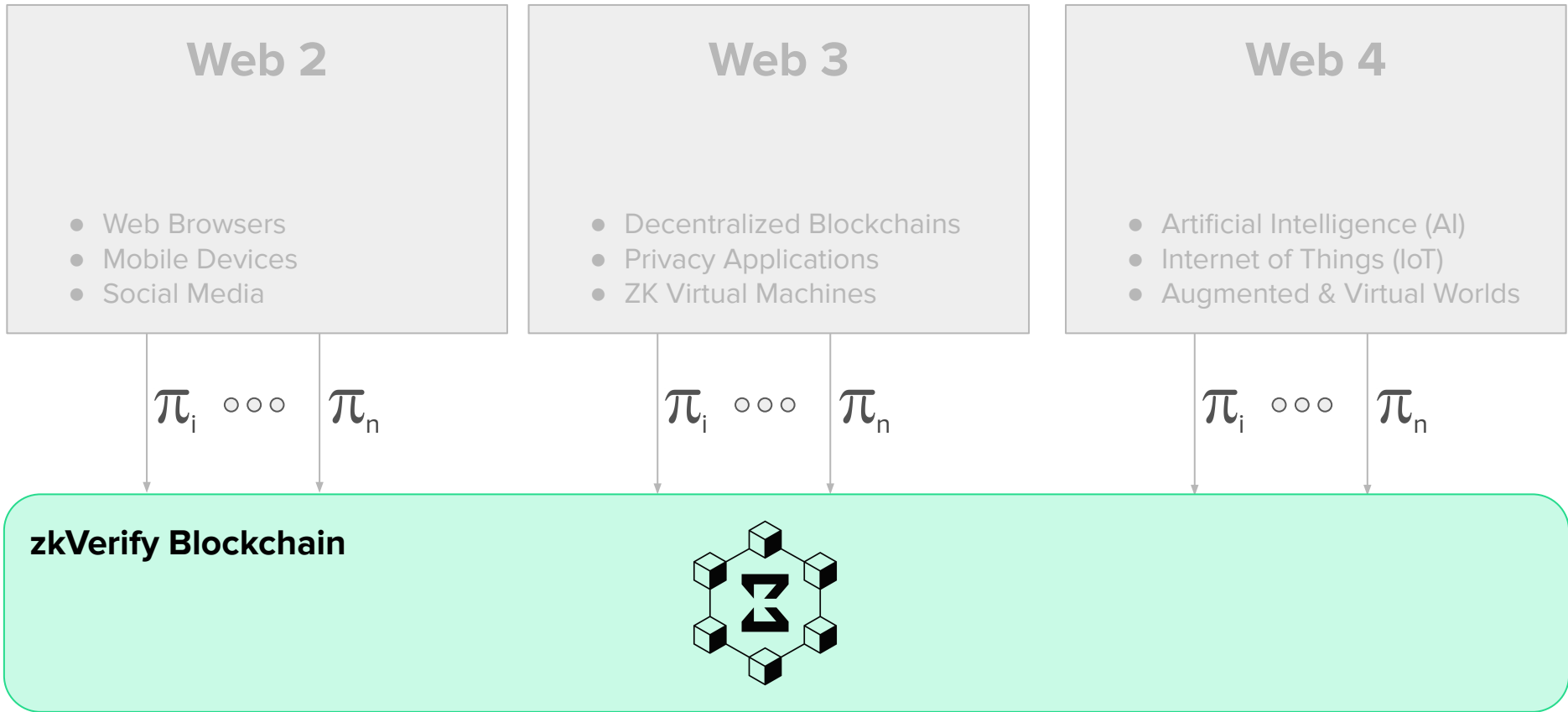


$$\pi_i \cdots \pi_\infty$$

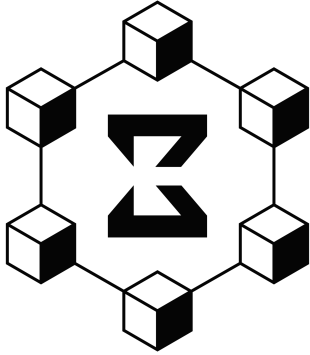


Overflow of Data = Overflow of Proofs

zkVerify: Decentralized Blockchain to Verify Proofs



What is zkVerify?



“zkVerify is a modular layer that focuses on verifying proofs at scale.”

Why zkVerify?



1. Developer Flexibility

- *Allows developers to choose the proving system that best suits their needs without worrying about underlying verification infrastructure.*

2. Enabler for Continued Innovation

- *Critical driver in evolving ZK landscape.*
- *Foster broader adoption & innovation across ecosystem.*

3. Cost-efficiency

- *Reduces verification costs, making cryptographic proof integration more accessible and sustainable across diverse applications.*

Greater ZK Narrative: *How zkVerify Fits In*



The image displays a grid of ZK ecosystem categories and their associated logos. A green arrow points to the 'Verif. Agg.' category, which is highlighted with a green border. The 'Verif. Agg.' category includes logos for NEBRA, ALIGNED, HYLE, zkVerify, and pi².

Category	Logos
Payments	ZCASH, firo, Daimo, payy
L2s	ZKsync, polygon, Aztec, Linea, taiko, STARKNET, Scroll
ID/Wallets	Privado.iD, semaphore, rarimo, WORLDCOIN, OpenPassport, Pass, zkLogin (sui), demox labs, Aptos Keyless, verida
Games	dark forest, Immutable, BLADE, ZYPHER, ZORDLE, zkH..., TileVille
Prover Network	GEVULOT, Succinct, FERMAH, lagrange, RISC ZERO, ZKPOOL
ZK in BTC	Alpen, Citrea, BVM
DeFi	RENEGADE, PANTHER, Darkfi, PENUMBRA, offshift
L1s	MINA, Aleo, PENUMBRA, ANONYMOUS, ALEPH ZERO, anoma
ZKML/AI	EZKL, NIOYA, Modulus Labs, ZkAGI, ZKML
Verifiable Compute	Jolt, RISC ZERO, NEXUS
Cross-chain	Hyperlane, =nil;, zeko, polygon, Succinct, Union
Verif. Agg.	NEBRA, ALIGNED, HYLE, zkVerify, pi ²
R&D/Audit	geometry RESEARCH, DxPARC, reilbcs, Zelic, ZKS, NETHERMIND, AMBDA, ZK HACK, Veridise, PROBING + SCALING, PROQUESTIONS
Hardware	Irreducible, INGONYAMA, SUPRA NATIONAL, CCYSIC, FABRIC
Coprocessor	AXIOM, BREVIS, ERODOTUS, marlin, lagrange, RITUAL, vlayer
Misc/Tools	Nouns DAO, TACEO, Anonymous DAO, Delphinus Lab, Snarkify, CLIQUE, Cursive, power, RAILGUN, ZK EMAIL

Source: ZK Summit 12, October 8th 2024, Lisbon.



Technical Core

Three Key Technical Components

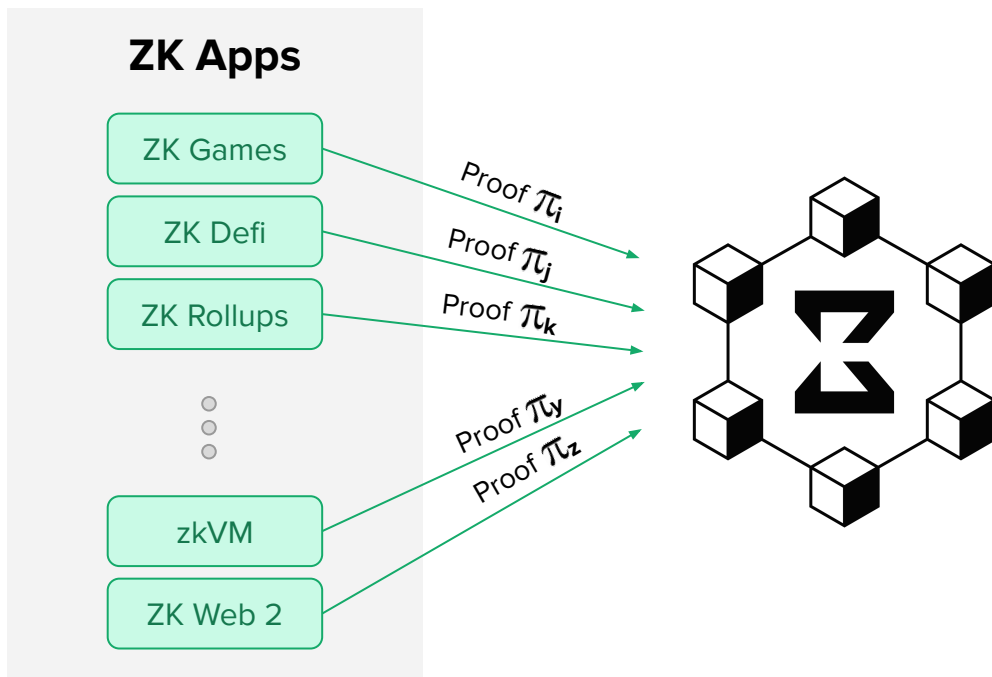


**L1 Framework
For Verification**

**Secure
Receipt
Broadcasting**

**Aggregated
Receipt
Data Structure**

Input: Proofs of Various Types from Various Sources



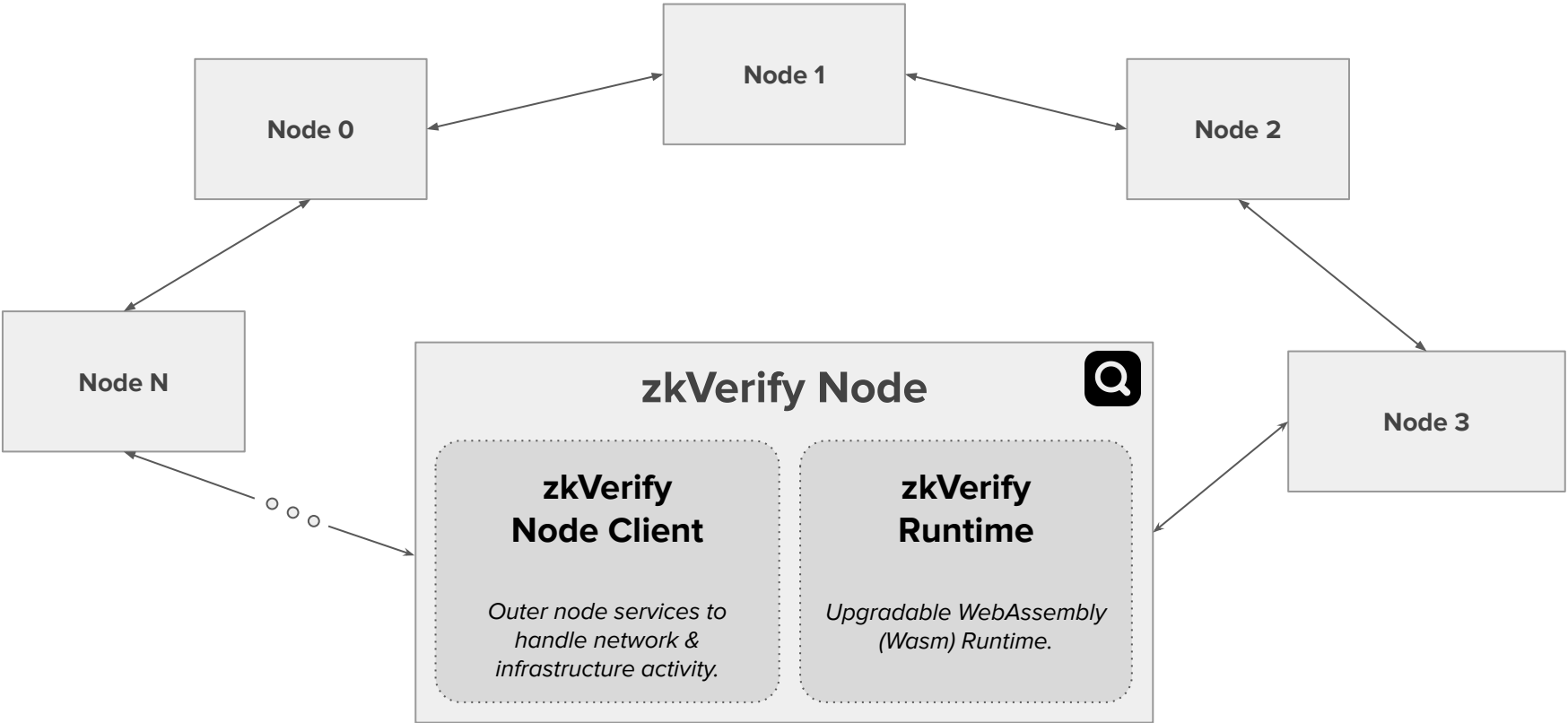
L1 Blockchain

- **Sole purpose:** Verify proofs at scale. No EVM.
- **Foundation:** Rust Substrate Framework.
- **Core Design Principle:** Modular Pallets.

Why L1 Blockchain?

- Censorship Resistance
- Publicly-Accessible Record
- Decentralized Incentive Model

L1 Blockchain: *Rust & Substrate Framework*



Verifier Pallets: Runtime Client via Node Acceleration



zkVerify Node

zkVerify Node Client

Proof Verification:
Node Acceleration

Arkworks
Extensions

Substrate Primitive
Elliptic Curve Utils

RPC

Consensus

Storage

Telemetry

Transaction

Networking

zkVerify Runtime Client

Proof Verification:
Proof of SQL

Proof Verification:
Fflonk

Block Authoring:
BABE

Proof Verification:
Risc0 STARK

Proof Verification:
UltraPlonk

Block Finalization:
GRANDPA

Proof Verification:
Groth16

Proof Verification:
zkSync Era

Security:
Staking

Proof Verification:
New Proof Type

Verification Receipt:
Aggregate

Account:
Balances

Receipt Bridging:
Hyperbridge

Governance:
Referenda

Fund Mgmt:
Treasury

Three Key Technical Components

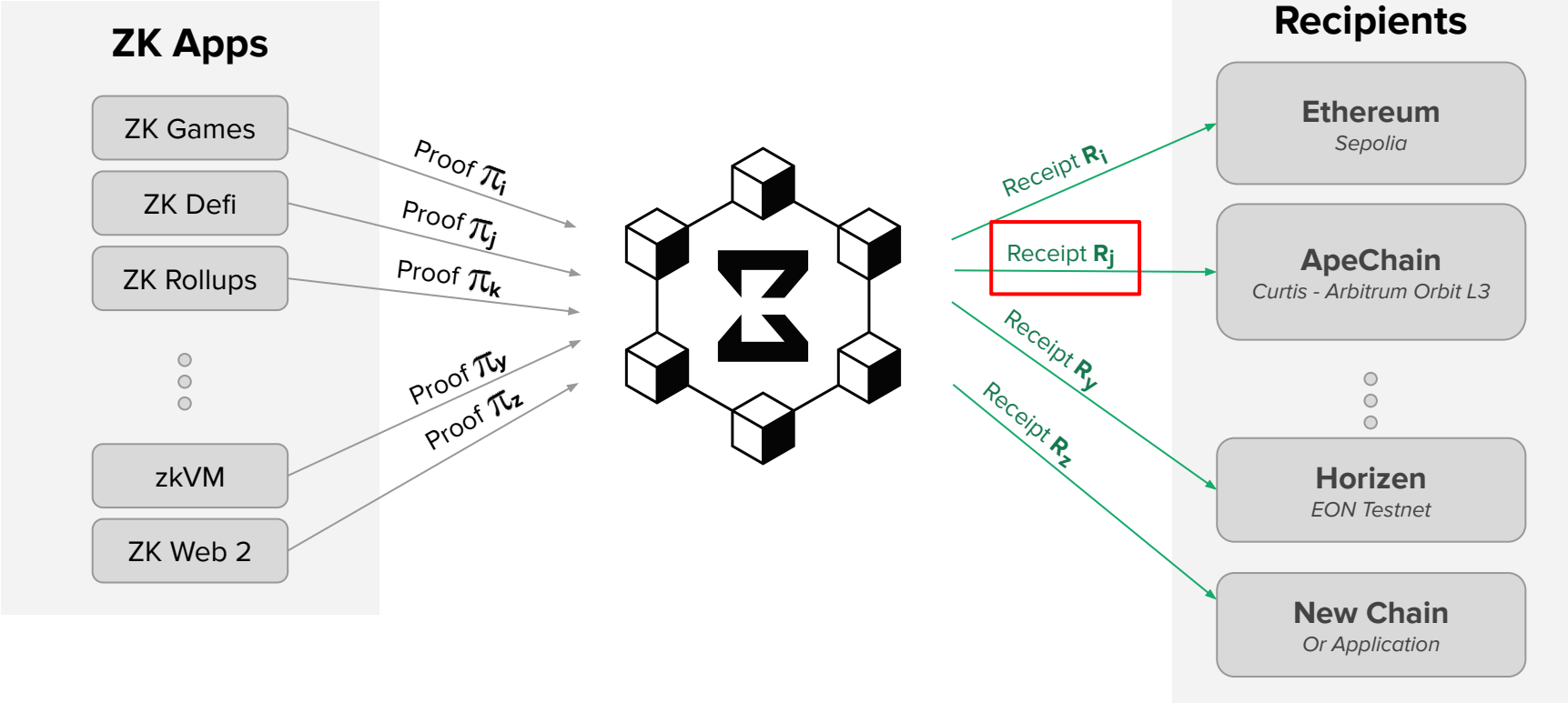


**L1 Framework
For Verification**

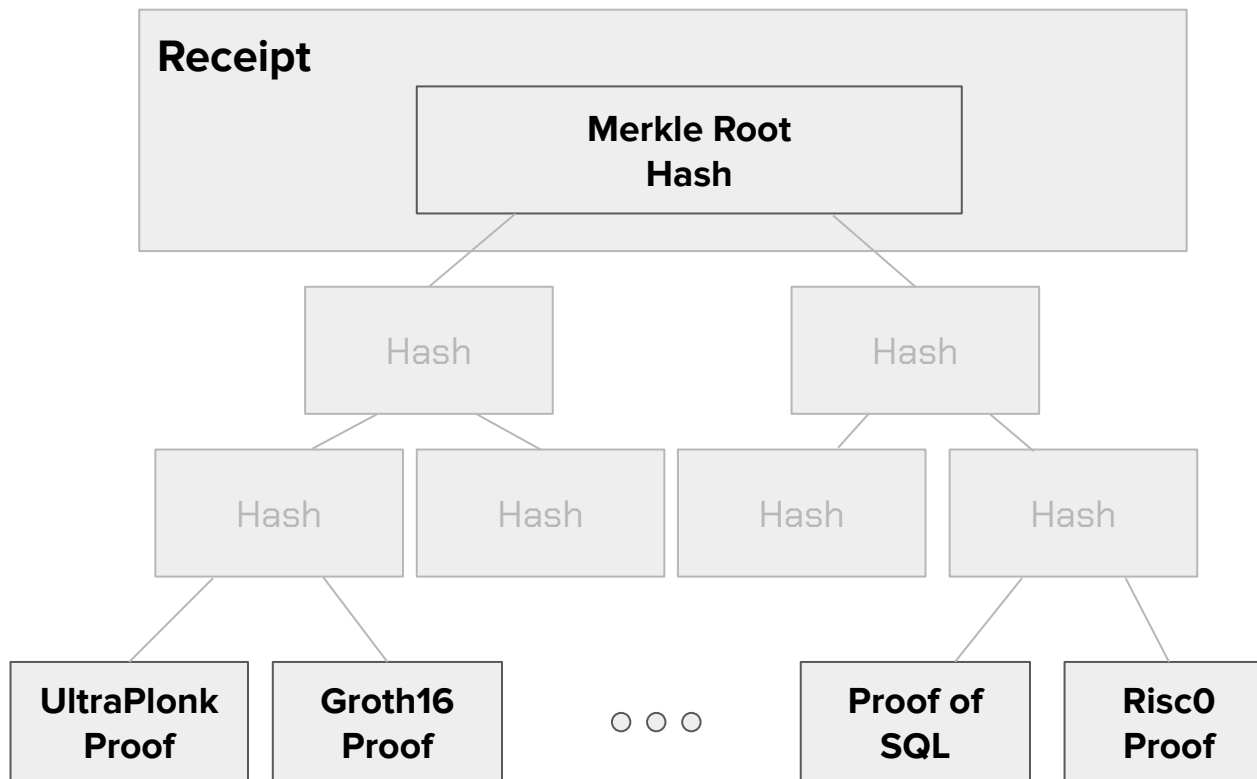
**Aggregated
Receipt
Data Structure**

**Secure
Receipt
Broadcasting**

Output: Receipt of Aggregated Verifications



Aggregated Receipt Data Structure



Natural aggregation of heterogeneous proofs

Three Key Technical Components

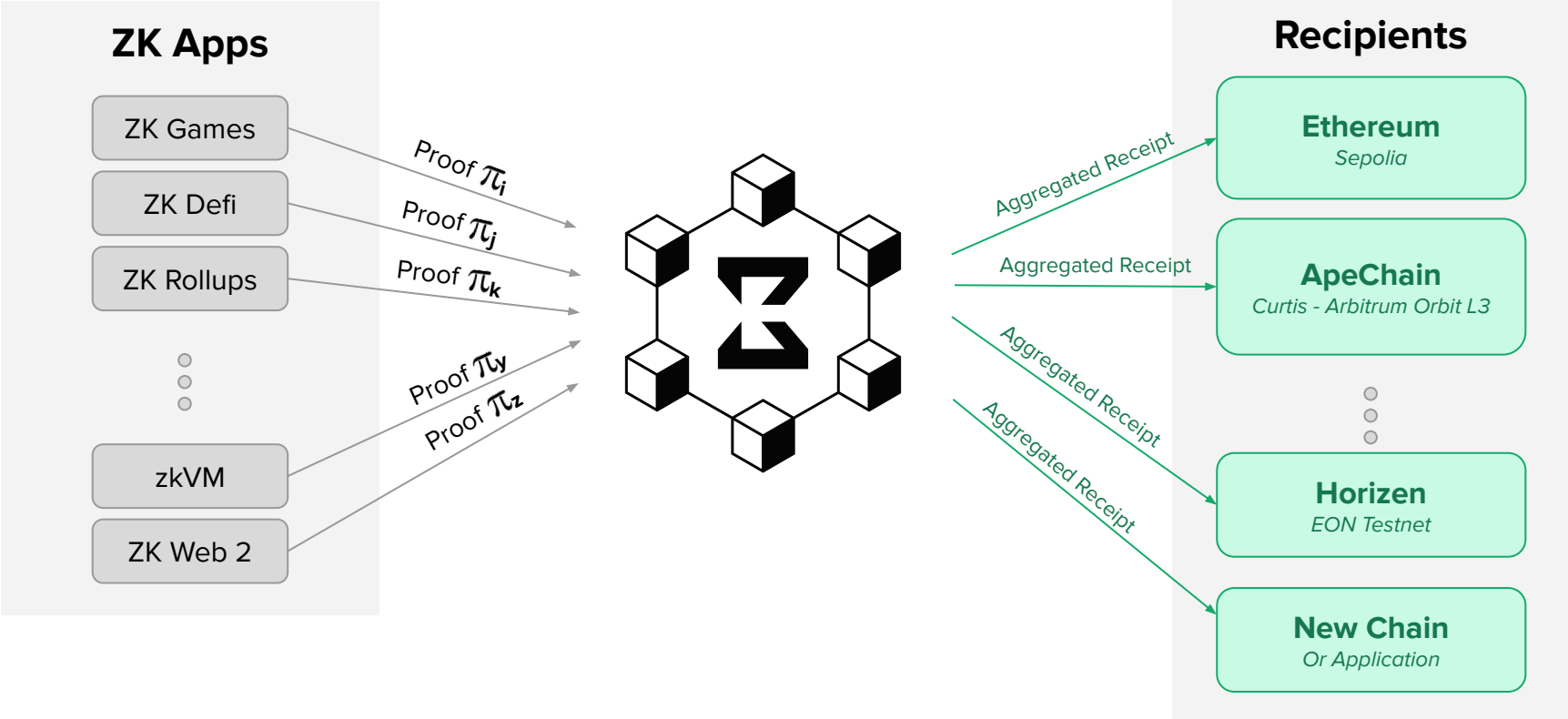


**L1 Framework
For Verification**

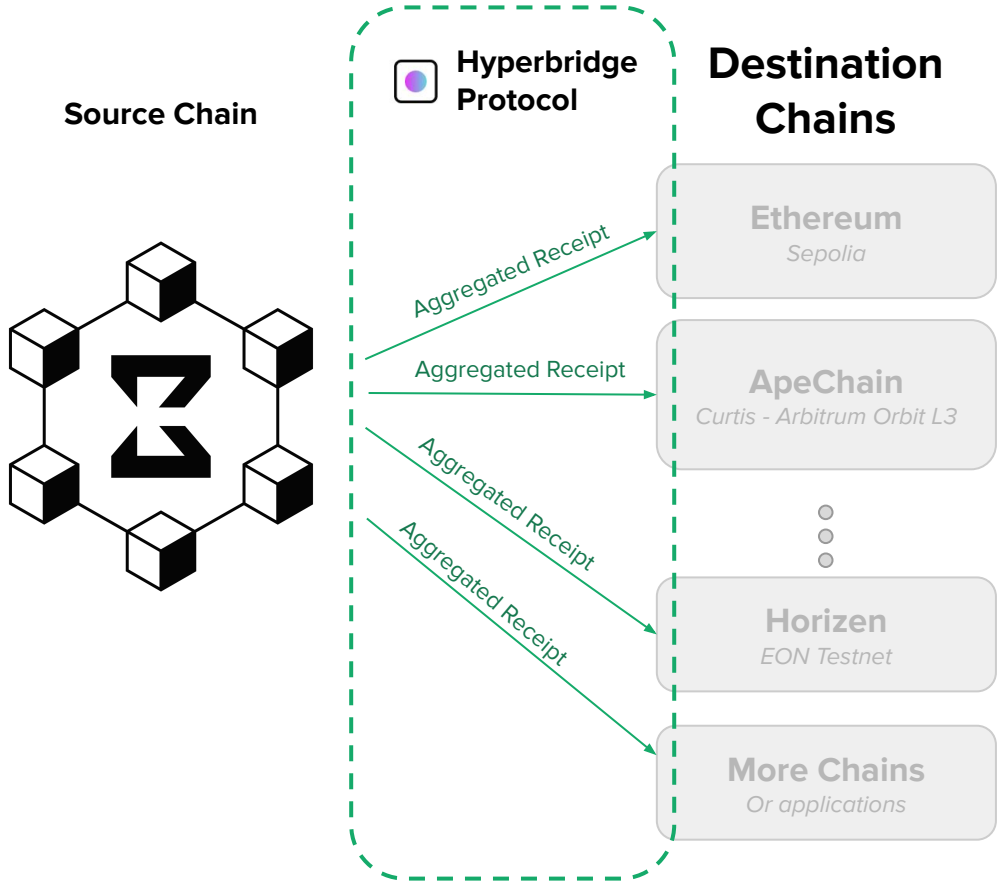
**Aggregated
Receipt
Data Structure**

**Secure
Receipt
Broadcasting**

Cross-chain Receipt Broadcasting

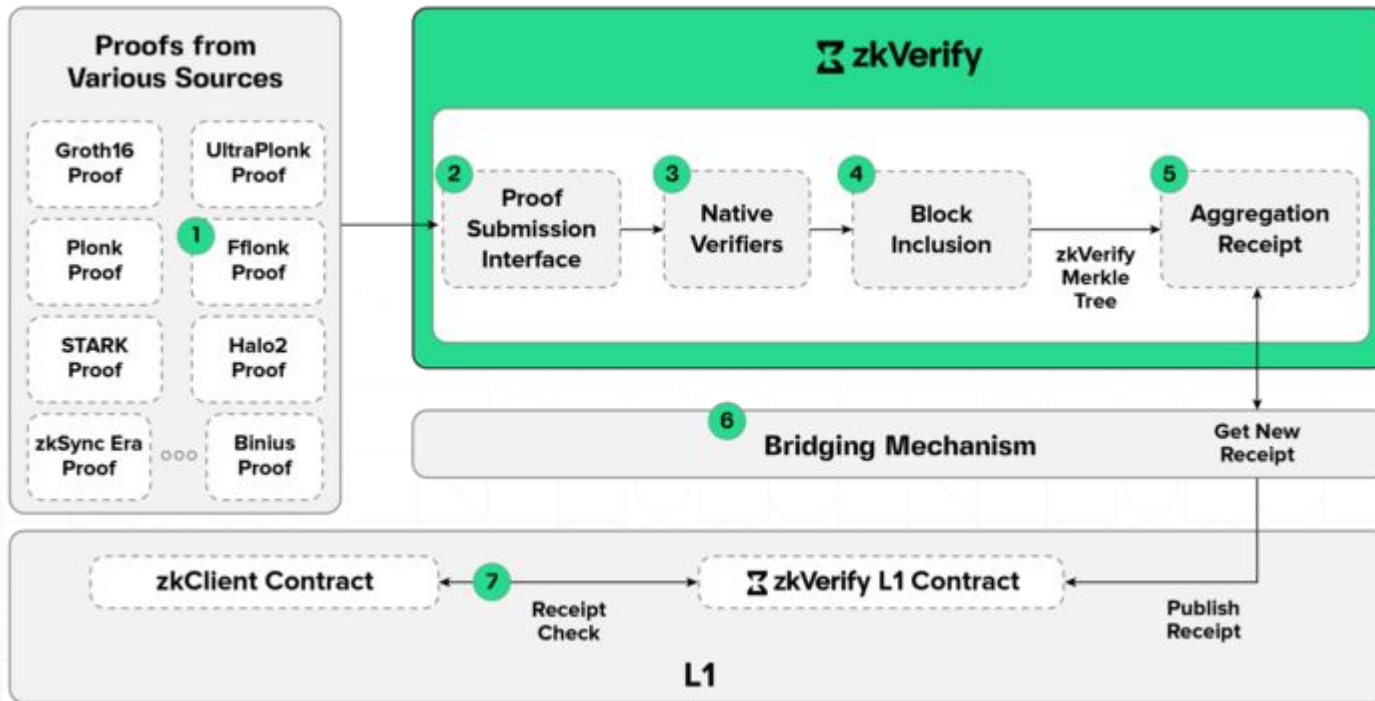


Cross-Chain Receipt Broadcasting



Hyperbridge Protocol

- **ISMP (Interoperable State Machine Protocol)**
 - Streamlined framework for **secure cross-chain messaging & state reads**.
 - Simple architecture w/Consensus Client, State Machine Client, Router, and Dispatcher.
- **Interoperability Proofs**
 - Includes **consensus proofs** and **state machine proofs** to validate the finalized states of counterpart chains, ensuring trustworthy, secure communication between blockchains.
- **Decentralized Relayer Network**
 - Utilizes permissionless, **incentivized relayers** to transmit messages and consensus proofs across chains without requiring whitelisting or staking, powered by cryptographic proofs.





Digging Deeper

Integrating a Web3 Dapp - Overall Flow



1. Submit proof to **zkVerify** via the ***Proof Submission Interface***

1. Listen to ***ProofVerified*** event on **zkVerify**

**Web2 App
Integration
Flow**

1. Listen to ***NewProof*** event on **zkVerify** and get the ***AggregationID***

1. Listen for ***NewAggregationReceipt*** event on **zkVerify**

1. Get the Merkle Path of your proof on **zkVerify**

1. Listen for the ***AttestationPosted*** event on the corresponding L1 chain containing your ***AggregationID***

1. Invoke the ***verifyProofAttestation*** method of the zkVerify smart contract from your smart contract



Web2 App Integration Demo



Web3 zk Dapp Integration Demo



Looking Ahead

Roadmap



Q1 2024

Q2 2024

Q3 2024

Q4 2024



Public Testnet MVP

- Relay chain bootstrapped
- Fflonk verifier
- Block explorer
- Polygon CDK node on Sepolia testnet
- Polygon CDK node submitting proofs to zkVerify

Public Testnet Beta

- Enable public to run validator and RPC nodes
- Switch consensus from Aura to BABE
- Add Groth16 Verifier
- Add Risc0 Verifier
- Add zkSync Era verifier

Incentivized Testnet - Phase 1

- Add Ultraplank Verifier
- Add 1st Validators Set
- Launch Incentivized Testnet Tasks
- Publish Grant for zkApps
- Integrate OpenGov
- Explorer UX Tuning
- Improved Testnet Faucet
- Launch KPI Dashboard
- Integrate Subsquid

Incentivized Testnet - Phase 2

- Additional verifiers TBA
- Full Initial Validator set
- Hackathons and Workshops
- Mainnet Preparations
- Bridge Integrations
- Oracle Integrations

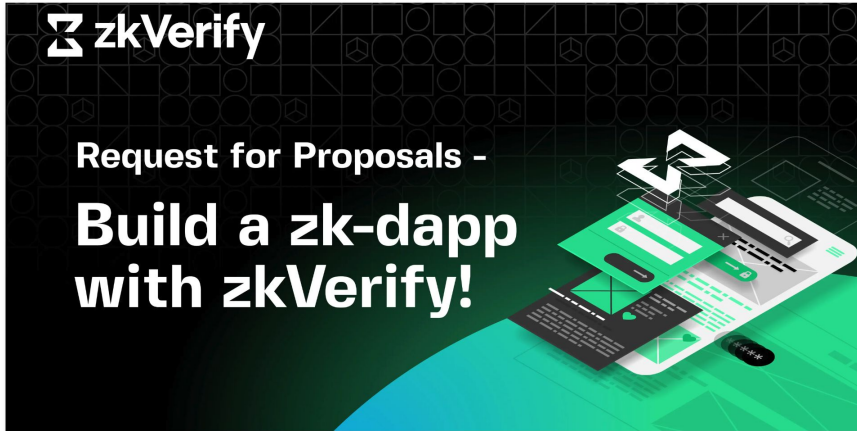
Call To Action: *Come Build With Us*



Grant Program

zkVerify blog

Grant: Build a zk-dapp with zkVerify!



Incentivized Testnet



Hackathons

- ZK Hack Montreal
- ETHWarsaw
- ETHSofia
- ZK Hack V

Call To Action: *Online Hackaton in progress !*





zkApp and Infra Builder Online Hackathon



Submission Deadline: December 10

(ANNOUNCING WINNERS ON DECEMBER 12)

<https://zkverify-zk-application-and-infrastructure-buildin.devfolio.co/>

\$26,000
Available in Prizes

 zkVerify Z... \$15,000	Horizen Labs \$5,000	Hyperbridge \$3,000
zkPass \$2,000	Sindri \$1,000	 All prizes >

RUNS FROM
Nov 20 - Dec 10, 2024

HAPPENING
Online

APPLICATIONS CLOSE IN
3d:16h:23m

Apply now

Horizen 2.0: Crypto-accelerated EVM Parachain on zkVerify



Horizen 2.0

(AN ADVANCED & EFFICIENT EVM OPTIMIZED FOR ZK APPS)

Native Token
Gas: \$ZEN
Governance: \$ZEN

Consensus
Delegated Proof of Stake

NEW
Target Block Time
~ 6 sec

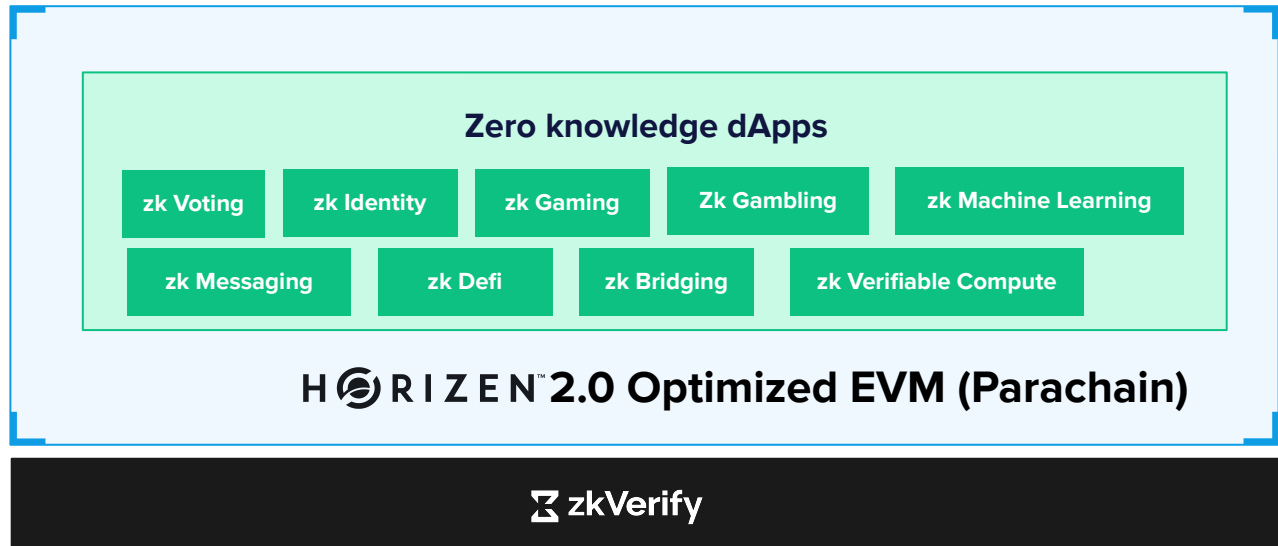
NEW
Tech
Substrate framework, written in Rust

NEW
ZK-Optimized

- Leverage fast, native ZK proof verification from zkVerify
- Modular and upgradable architecture of future ZK advancements, such as new proving systems

NEW
Backwards Compatibility

- Preserve max \$ZEN supply
- Full Solidity and EVM support
- \$ZEN, EON snapshots
- Prolonged claim window
- Enable incentives for ecosystem participants



<https://www.horizen.io/>

Get In Touch



Get in Touch:

Horizen Labs

- x.com/HorizenLabs
- github.com/HorizenLabs
- research@horizenlabs.io
- horizenlabs.io

zkVerify

- x.com/ZKVProtocol
- docs.zkverify.io
- discord.gg/zkverify
- zkverify.io



Currently Hiring

- Product Manager
- Dev Relations Engineer
- Senior Rust Blockchain Engineer
- Senior DevOps Engineer
- Web3 Content Creator



Thank You



Questions ?