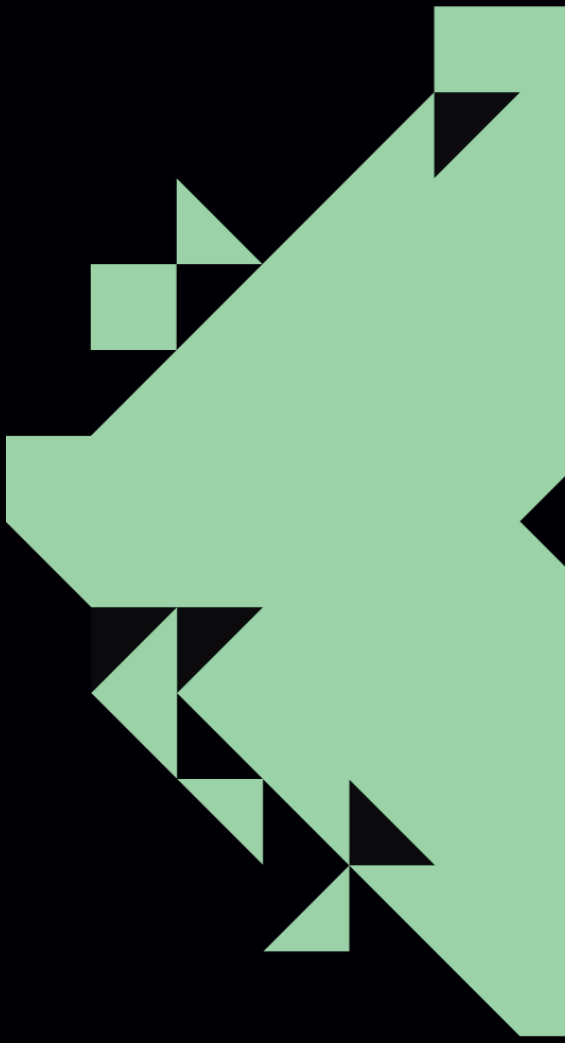
The State of ZK

Q2-2024



Compiled by

ZKV

zkv.xyz

Table of Contents

The State of ZK

Brief

Welcome to the latest edition of the State of ZK Report for Q2 2024, produced by ZKV.

ZK Research continued in Q2 with the release of new papers on sum-check protocols, optimizations around small fields and ZK hardware. There was also new work on benchmarking ZK-Rollup performance, something we have long been asking for.

On the infrastructure and engineering front, zkVMs took center stage, with Jolt, SP1, and Risc Zero each releasing updates that pushed the boundaries of verifiable computation. Jolt was released as an open-source implementation this past quarter. Succinct released SP1 GPU. However, it was Risc Zero's zkVM 1.0 that marked a major milestone in the field as the first production-ready zkVM to be released.

This quarter also witnessed the first mainnet launch of a ZK application platform, with Mina's Berkeley upgrade. Their zkApps environment will make building ZK applications much more accessible to non-ZK-native developers, and we expect other programmable ZK platforms, such as Aleo and Aztec, to launch soon as well. In terms of ZK applications, several new products addressing payments, on-ramps, voting, and ID were announced or released this past quarter.

On the ZK Supply Chain front, we saw additional teams announce their plans include a prover marketplace in their systems, and a new category of project emerged in this stack — proof verification aggregators. In the next section of the report, we share our Map of ZK, where we list and group high potential teams working on ZK infrastructure and application types, including those that make up the ZK Supply Chain.

One of the most contentious moments in Q2 came with the news that Matter Labs, the company behind zkSync, had filed a trademark for "ZK." This raised the ire of some community members, and while the trademarking was done by the company for defensive reasons, it was perceived by many as contradictory to the open-source ethos of the space. After some deliberation, the Matter Labs team decided to abandon the trademark application in solidarity with ecosystem sentiment. The entire episode not only raised questions about the rights to use specific terms and technologies but also unified the community around the topic of stewardship of ZK technologies. When asked, "Who owns ZK?", the community was quite adamant in its answer: "all of us" and "no one" simultaneously.

One thing is sure: there is never a dull day in ZK.

The State of ZK

Map of ZK

Payments
ZKP2P
Payy Network
Daimo
Zcash

DeFi
Panther Protocol
ZigZag
Renegade
Offshift
Penumbra
Dark.fi

Identity
ZK Email
zkLogin (Sui)
zkPass
zPass (Aleo)
Privado (Polygon ID)
zkPassport
Semaphore
Rarimo
World ID (Worldcoin)
Holonym
Proof of Passport
Verida
zk.me

Gaming
Immutable
Dark Forest
Cartridge
Blade Games
Zypher
Tileville
Ronin
ZK Race
Argus
Zordle
ZK Holdem

ZK Rollups
Aztec
zkSync
Taiko
Scroll
Polygon zkEVM
Linea
Manta Pacific
Starknet

Privacy L1s
Mina Protocol
Namada
Penumbra
Aleo
Horizen
Zcash
Aleph Zero
Anoma

Hardware
Irreducible
Ingonyama
Cysic
Supranational
Fabric

Prover Networks
Lagrange
Gevulot
Nexus
Fermat's Layer

zkVMs
zkVM 1.0 RiscZero
SP1 by Succinct
Lita
Jolt by a16z
Ola

Coprocessors
Axiom
Brevis
Herodotus
Marlin
Ritual

Proof Verification
Nebra
Aligned
Hylé

Tools
Pluto
Clique
Railgun
Protoit

Cross-chain
Union
AggLayer by Polygon
Succinct
Nil foundation
Zeko
Elastic Chain by zkSync

ZK in Bitcoin
Alpen Labs
Citrea
BVM

ZKML/AI
EZKL
Modulus
zkAGI
Noya
zkML

This map was curated and organised by the ZKV team, but if you see any errors in our categorisation or believe there are important projects missing, please contact us about it at research@zkv.xyz

ZK Research

The Sum-Check Protocol over Fields of Small Characteristic by Suyash Bagad, Yuval Domb and Justin Thaler: They explore optimization techniques for the sum-check protocol within SNARKs (Succinct Non-Interactive Arguments of Knowledge), particularly focusing on fields with small characteristics. The protocol involves the prover sending univariate polynomials to the verifier over multiple rounds. Each polynomial's degree is constrained, and the verifier checks these degrees and random evaluations to ensure correctness. The authors present new algorithms that minimize expensive extension-field multiplications by leveraging cheaper base-field multiplications, especially in the initial rounds. They propose an optimal switching strategy between their new algorithms and existing ones to balance computational costs efficiently. The improvements are significant when base-field multiplications are substantially cheaper than extension-field multiplications, potentially accelerating the sum-check prover by multiple orders of magnitude. The results are particularly relevant for modern SNARKs that use polynomial commitment schemes, which render the sum-check protocol a critical performance bottleneck.

A Time-Space Tradeoff for the Sumcheck Prover by Alessandro Chiesa, Elisabetta Fedele, Giacomo Fenzi and Andrew Zitek-Estrada: This article centers on new prover algorithms for the multilinear sumcheck protocol, focusing on achieving different tradeoffs between time and space efficiency. The protocol itself is used to verify the sum of a low-degree polynomial over a hypercube, and it plays a critical role in constructing efficient succinct non-interactive arguments of knowledge (SNARKs). The proposed algorithms, named BlendySC, parameterize the tradeoff by an integer kkk, where increasing kkk reduces memory consumption at the cost of increased running time. The core technical contribution includes partitioning the n rounds of the sumcheck protocol into kkk stages, performing precomputations at the start of each stage, and efficiently updating and evaluating Lagrange polynomials sequentially to minimize space requirements. This method improves upon previous algorithms by adjusting the balance between time and space, leading to concrete efficiency improvements in memory usage while maintaining competitive running times.

ZK Research

Polymath: Groth16 Is Not The Limit by Helger Lipmaa: The paper explores potential improvements to Groth16's argument length, particularly focusing on bit length rather than group elements, while maintaining prover efficiency and achieving higher security levels. The authors propose a new zk-SNARK, Polymath, which replaces Groth16's G2 elements with polynomial commitments in G1 to reduce communication overhead. Polymath achieves a shorter argument length by leveraging the Square Arithmetic Program (SAP) constraint system, opening polynomials, and employing a novel public input verification method. Despite having a longer Structured Reference String (SRS) and a slower prover, Polymath is optimized through exhaustive parameter search and demonstrates significant improvements in communication size and verification efficiency at the 192-bit security level, making it well-suited for high-security application.

zk-SNARK	Groth16	Polymath
Arithmetization	R1CS	SAP
$\|\mathtt{srs}\|$	$(m+2n)\mathfrak{g}_1 + n\mathfrak{g}_2$	$(\tilde{m}+12\tilde{n})\mathfrak{g}_1$
P computation	$(m+3n)\mathfrak{m}_1 + n\mathfrak{m}_2$	$(\tilde{m}+13\tilde{n})\mathfrak{m}_1$
$\|\pi\|$	$2\mathfrak{g}_1 + 1\mathfrak{g}_2$ (1536 / 3072 bits)	$3\mathfrak{g}_1 + 1\mathfrak{f}$ (1408 / 1792 bits)
V computation	$3\mathfrak{p} + m_0\mathfrak{m}_1 \quad (\mathfrak{m}_1 = \Theta(\lambda\mathfrak{f}))$	$2\mathfrak{p} + 2\mathfrak{m}_1 + 1\mathfrak{m}_2 + O(m_0 \log m_0)\mathfrak{f}$
V batch-computation	$3M\mathfrak{m}_1 + M\mathfrak{p} + Mm_0\mathfrak{m}_1$	$4M\mathfrak{m}_1 + O(Mm_0 \log m_0)\mathfrak{f}$

Volatile and Persistent Memory for zkSNARKs via Algebraic Interactive Proofs by Alex Ozdemir, Evan Laufer and Dan Boneh: This paper explores how to efficiently offload complex non-native arithmetic operations, such as Boolean operations, field arithmetic, or public-key cryptography, from a zero-knowledge circuit. In particular, the work presents techniques to offload equality of discrete logarithms across different groups, scalar multiplication without requiring elliptic curve operations, and proving knowledge of an AES encryption using methods derived from rejection sampling and lookup protocols. The authors also benchmark their implementation of the presented techniques to highlight the practicality of the developed approaches.

ZK Research

On Proving Parings by Andrija Novakovic and Liam Eagen: The paper presents efficient methods for verifying elliptic curve pairings, essential in cryptographic protocols like SNARKs and BLS signatures used in public blockchains. It addresses the high computational cost of pairings by proposing replacing the final exponentiation step with a residue check and precomputing necessary lines in the Miller loop, especially when the second pairing argument is fixed. Additionally, the paper introduces a method to combine quotients for more efficient verification of higher-degree relations. These optimizations, demonstrated using the BN254 curve, are particularly beneficial for on-chain verification in Ethereum and Bitcoin, enhancing the efficiency and scalability of pairing-based cryptographic protocols.

ICICLE v2: Polynomial API for Coding ZK Provers to Run on Specialized Hardware by Karthik Inbasekar, Yuval Shekel and Michael Asa: ICICLE v2 is an advanced cryptography library designed to accelerate ZKPs using GPUs. It implements various hardware primitives through native CUDA code, facilitating efficient modular arithmetic and group operations. The library is structured with a "stacked tile" architecture, where core computational tasks are managed by CUDA kernels. It offers a Polynomial API that abstracts complex polynomial operations, enabling researchers and developers to prototype and implement cryptographic protocols without deep knowledge of hardware specifics. By leveraging this API, ICICLE v2 provides a device-agnostic framework that ensures high performance across different hardware environments, aiming to streamline the development of ZKP applications.

zkSNARKs in the ROM with Unconditional UC-Security by Alessandro Chiesa and Giacomo Fenzi: The paper addresses the challenge of achieving universal composability (UC) security for zkSNARKs within the random oracle model (ROM). UC-security is a critical goal in cryptography as it ensures strong security guarantees even when protocols are integrated into larger systems and subjected to adaptive adversaries. The authors demonstrate that existing zkSNARK constructions, specifically the Micali and BCS constructions, inherently meet UC-security without requiring modifications, proving that these widely used zkSNARKs can be securely employed in real-world applications. This result contrasts with previous approaches that often compromised efficiency or simplicity to achieve UC-security.

ZK launches

zkVM 1.0

RISC Zero launched zkVM 1.0, a production-ready general-purpose zero knowledge virtual machine. This technology allows for off-chain computation and on-chain verification, without cycle count or gas fee limitations. Developers can use any Rust crate for complex logic. The network supports proof composition through recursion. The zkVM 1.0 architecture includes continuations, enabling the splitting of large programs into smaller segments for parallel proving and fixed memory requirements. The platform can achieve interoperability with any blockchain that supports a RISC Zero verifier.

SP1 Testnet

Succinct Labs released the SP1 testnet 1.0. The main update includes performant STARK recursion, which is said to facilitate fast end-to-end ZK proof generation with on-chain verification for EVM-compatible chains. SP1 now supports the Rust standard library; customisable precompiles, and a precompile-centric architecture to optimise common operations like hashing and elliptic curve operations.

Berkeley

Mina Protocol went through a significant hard fork, named Berkeley Upgrade. The upgrade leverages recursive ZKPs to create an open database of verified statements, allowing seamless interaction and composability between different applications within the Mina ecosystem. According to a blog post by Mina co-founder Evan Shapiro, this approach eliminates redundancy, reduces state bloat, and enhances scalability by distributing data and computations across the network rather than replicating them. The Berkeley Upgrade is said to enable applications like zkKYC, zkIdentity, zkVoting, zkGaming, and zkDeSci.

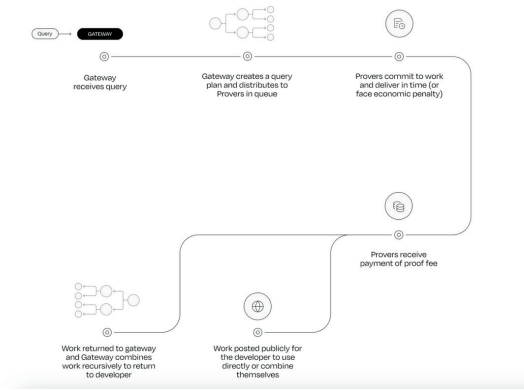
ZK launches

ZaKi

ZaKi by Ingonyama introduces a ZK hosting service optimised for ZKP generation using specialised hardware. The service uses the ICICLE acceleration library and its variant, ICICLE-NG. ZaKi offers a managed, pay-per-proof model for ZK computations. The service supports GPU-based ZK computation, aiming to reduce operational costs through optimised hardware utilisation and prover efficiency.

Lagrange Prover Network

Lagrange Labs launched its Prover Network on EigenLayer. This network is a production-ready ZK prover network designed to handle complex computations by distributing tasks among decentralised provers. Each prover commits to generating proofs within a specified time, backed by collateral, to ensure reliability and liveness. Lagrange's ZK Coprocessor offloads intensive computations off-chain, generating proofs that are verified on-chain. The network's architecture includes Gateways managing queues of work for Provers, who earn rewards for timely proof generation and face penalties for delays.



A Diagram illustrating the Prover Network by Lagrange

Initiatives

Euros onramp from Revolut: The latest release of ZKP2P introduces a workflow that leverages the TLSNotary protocol to facilitate Euro to USDC onramping for Revolut users on the Base network, operating without gas fees. This update includes a browser extension called Peer, which is necessary for generating web proofs of Revolut accounts and associated payments. Previously, ZKP2P used zkEmail for verifying DKIM signatures and extracting payment information from email receipts as proof of payment. However, platforms supporting Euros lacked the necessary payment details. The integration of TLSNotary addresses this by generating privacy-preserving proofs of HTTPS calls using MPC, thereby enabling the same functionality without exposing sensitive data.

SnargsBook: This book, written by Alessandro Chiesa and Eylon Yogev, thoroughly examines cryptographic proofs using ideal hash functions, focusing on SNARGs like STARKs. It discusses transforming probabilistic proofs (SPs, IPs, PCPs, IOPs) into cryptographic proofs, emphasising security reductions with explicit error bounds. The analyses are tight, and the terminology is consistent to address gaps in current literature. Aimed at students, researchers, and practitioners with basic knowledge in discrete probability and algorithms, it provides a comprehensive reference on succinct arguments. The book and its source code are available on GitHub under a Creative Commons Attribution-ShareAlike 4.0 International License.

ZK Grants Round Winners: The Ethereum Foundation, along with Aztec, Polygon, Scroll, Taiko, and zkSync, has announced the winners of the ZK grant round, focusing on advancements in zero-knowledge proofs (ZKPs). The selected projects aim to enhance ZKP security frameworks, analyse cryptographic schemes, develop benchmarking tools for performance and scalability, and integrate advanced cryptographic models into practical applications. Notable recipient ZK Hack, a project that was initially incubated by ZKV, received a grant to produce Season 2 of the ZK Whiteboard Sessions

Ronkathon: The Pluto team released Ronkathon a Rust-based implementation of cryptographic primitives inspired by Plonkathon, aimed at demonstrating theoretical properties of applied cryptography through practical application. Built from first principles, it avoids reliance on external libraries to focus on mathematical transparency and simplicity. The library includes modules for finite fields, polynomial commitment schemes, and elliptic curves, providing a foundation for constructing KZG proofs. Additionally, it features implementations of RSA, ECDSA, and hash functions like Sha256 and Poseidon. Ronkathon serves as an educational tool, not optimized or secure for commercial use, to help users understand cryptographic implementation details.

Initiatives

End-to-end, FPGA-accelerated Polygon zkEVM prover: The FPGA-accelerated Polygon zkEVM prover aims to optimise proof generation by integrating FPGA modules for Merkle tree construction and low-degree extension (LDE) computation, along with memory layout modifications for improved data transpose performance. According to the blog post shared by Irreducible, this setup achieves a 500-transaction batch proof in 84 seconds, significantly faster than the non-accelerated version. The system uses two FPGA cards connected via QSFP and AMD's Aurora protocol. One FPGA handles the LDE, while the other performs leaf-hashing, streaming data through PCIe 4.0. Memory layout changes ensure polynomials align with CPU cache lines, enabling efficient data transposition. Irreducible says that further FPGA acceleration could reduce proof times to under 60 seconds.

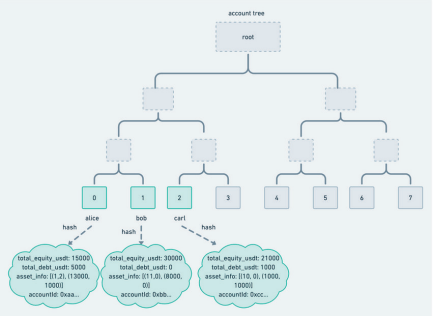
Polygon x SP1: Polygon Labs and Succinct Labs announced that Polygon's AggLayer will use SP1, an open-source zkVM built with Plonky3. The AggLayer will use SP1 to generate pessimistic proofs, ensuring secure cross-chain interoperability by treating every chain with suspicion to protect the shared bridge. According to the announcement, this integration allows non-ZK chains to connect without compromising security. The pessimistic proof code is open-source under MIT/Apache.

Jolt Implementation: Jolt is a zkVM designed by a16z to optimize verifiable computation by using the Lasso lookup argument and sumcheck-based methods. It supports the RV32I (RISC-V 32-bit base integer) instruction set. Jolt addresses performance through optimized polynomial commitment schemes and supports Rust. Future enhancements include extending support for additional RISC-V instruction sets and implementing proof recursion for longer computations.

Mina x Celestia: Mina Protocol and Celestia are collaborating to introduce the first modular decentralised data availability (DA) solution to the Mina ecosystem, led by Geometry Research with support from o1Labs. By incorporating Celestia's modular DA layer, Mina increases its capacity to handle high-throughput zero-knowledge applications (zkApps).

Friction points

Binance Proof of Reserves: Enrico Bottazzi from the Privacy and Scaling Explorations discovered a potential attack on Binance's Proof of Reserves (PoR) solution. This attack leverages the ability to add dummy users with positive positions in low-quality assets and negative positions in high-quality assets, allowing Binance to claim solvency while reducing the required reserves of high-quality assets. Consequently, if real users attempt to withdraw high-quality assets, Binance might lack immediate availability and need to liquidate low-quality assets, risking withdrawal delays due to market conditions. PoR protocols are designed to verify that a Centralized Exchange (CEX) fully backs user deposits with actual reserves, using zk-SNARKs for liability accounting through an Account Merkle Tree and asset commitments. However, the design flaw permits adding dummy users, undermining verification. Enrico proposed a solution involving modifying the PoR protocol to introduce Collateral To Asset (CTA) Pair Trees, which enhance transparency and user verification but increase computational complexity.



A representation of the Merkle Tree used in the CEX PoR design

Critical Bug in MACI: During ETHDam's Quadratic Funding round on clr.fund, a critical bug in MACI was discovered due to a lack of validation for MACI public keys within the Poll contract. This allowed a user to submit an invalid public key not on the Baby JubJub elliptic curve, causing a denial of service (DoS) that halted the round. Initially misdiagnosed as a frontend issue, the bug was traced to the zk-SNARK circuit failing to generate a proof due to the invalid key. To resolve the issue, the team re-submitted valid signups and contributions to a new contract, excluding the invalid message, allowing proof generation and final tally validation. The bug was fixed by adding validation to ensure public keys are valid curve points, and the updated MACI version 1.2.1 was released.

Ecosystem Funding

This quarter saw a 52% drop in funding for public rounds. However, the number of public rounds stayed flat at nine. The median ticket size increased, with a median of $10M for Q2, up from $8M last quarter.

Project	Industry	Amount
Nebra	Universal Proof Aggregation	$4.5M
Cystic	Hardware	$12M
Hinkal	Privacy	$1.4M
Lagrange	Prover Network	$13.2M
Alpen Labs*	Bitcoin Rollup	$10.6M
Irreducible	Hardware	$15M
Hylé	L1	$2.6M
Zeko	Interoperability	$3M
Aligned	Proof Verification	$26M

* Note: ZKV is an investor in Alpen Labs

Conclusion

As Q2 comes to a close, the ZK ecosystem stands at a crossroads. New teams are forming, investments and funding continue to flow into ZK, and projects are steadily progressing. However, the adoption of the infrastructure by app developers remains slow, and the “killer application” remains just out of reach. This leads us to believe that more ZK application development and experimentation are very much needed if we are to realize the full potential of ZK.

See you in Q3!

Scan and download it digitally

A bit about us: ZKV is a mission-driven company running validator and node infrastructure on 12 networks. We were founded in 2019 and our team has strong ties to many of the organisations shaping the ZK industry, such as The Zero Knowledge Podcast, ZK Hack, zkSummit, rhino.fi, Geometry, and University College of London. We have led multiple ZK-focused initiatives including public goods funding, events series and legal education. You can find out more about our work at www.zkv.xyz

ZKV

Follow us

@zkv_xyz