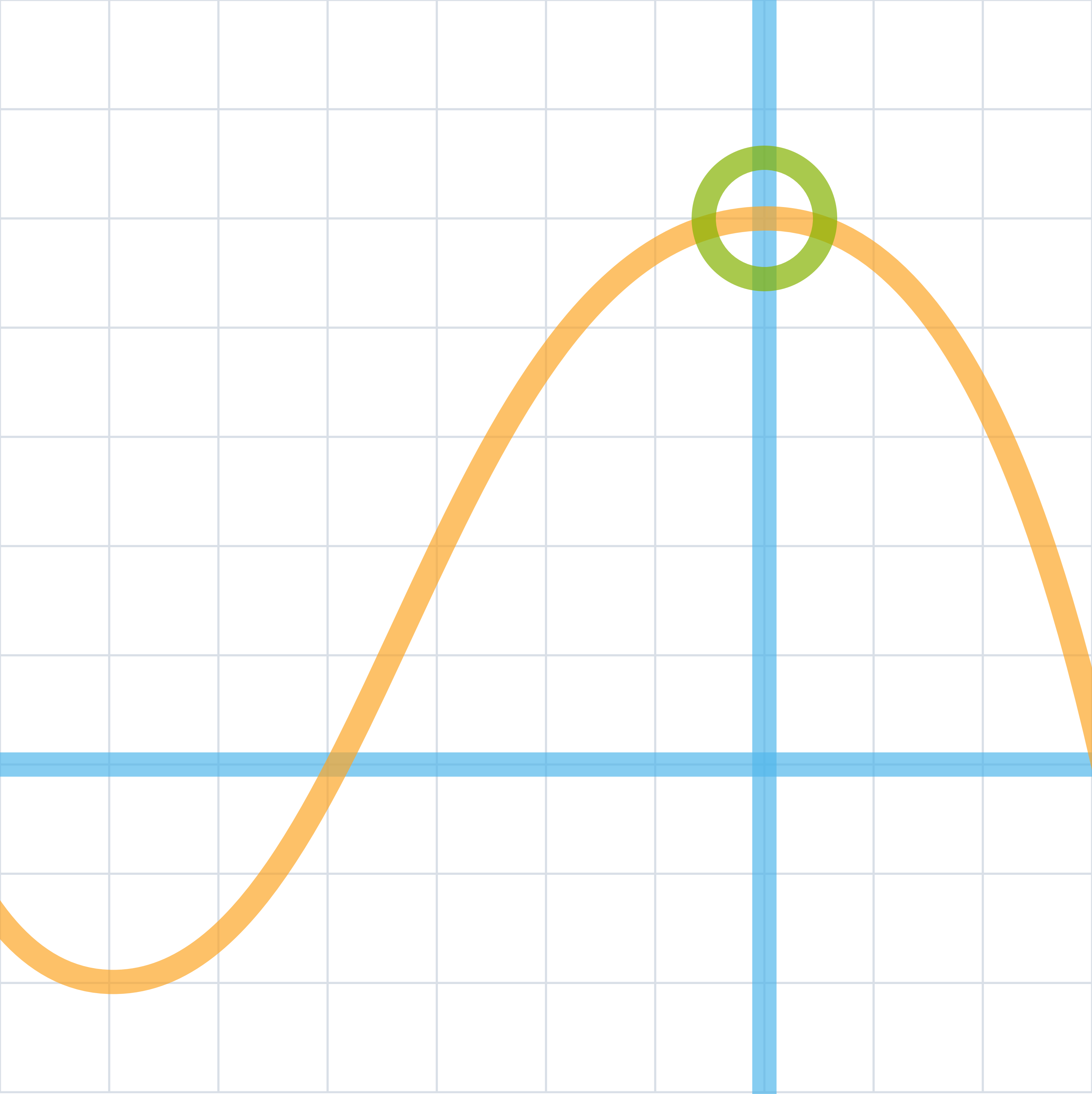




2026 ZK Industry Report

Produced by **ZK**  **Succinct**

Index

3	Brief
4	Foreword
5	What Is A Zero-Knowledge Proof
6	The Trust Tax
7	What Trust Costs Today
8 - 9	The State Of The Technology
8	State Of Proving
9	State Of Research
10 - 14	ZK Adoption Across Industries
10	Digital Asset Infrastructure
11	Private Payments
12	Institutions
13	Identity & Credentials
14	Frontier
15	What's Next

Produced by **ZK** **Succinct**

In this report, we offer a snapshot of the state of zero-knowledge (ZK) cryptography, including the current state of technology, research, and various novel use cases. In the following pages, we cover where the technology stands, where it has found real users, and what comes next. It is produced in collaboration between Succinct and the Zero Knowledge Podcast.

One of 2026's headlines was that within the digital asset industry, ZK proving is no longer a bottleneck. Real-time proving for blockchains, long treated as the industry's moonshot, was achieved in 2025, with 99% of Ethereum mainnet blocks now proven using ZK in under 10 seconds. Outside that benchmark, proving general computation still costs orders of magnitude more than running it. Closing that gap, along with the emergence of AI-accelerated engineering and the move to hash-based quantum-resistant constructions, now drives the research agenda.

As it advances, ZK has moved into production in crypto and beyond. Today we are seeing governments issuing digital identity using ZK at civic scale, consumer wallets using ZK to verify age without collecting documents, regulators writing ZK into digital identity frameworks, and banks settling assets with ZK proofs.

Demand for privacy and verifiability is now mainstream. Two questions remain open: will proving get fast enough to match general computation — and will the market meet that demand with proofs, or with trusted operators?



Written By
Dan Boneh

In recent years we have seen tremendous progress in the design and deployment of succinct proof systems (a.k.a. SNARKs).

Briefly, a succinct proof is a way to verify a computation without redoing it.

The last decade has seen an impressive research and engineering effort focused on making succinct proofs practical. The result is that proving got fast, cheap, and usable. Succinct proofs can now be deployed in many different settings: blockchains, identity verification, media provenance, and many others.

Beyond performance improvements, proof systems are now far more usable. A few years ago, building using SNARKs meant hand-crafting circuits in a domain-specific language. With the advent of general-purpose zkVMs, any engineer can now produce a proof of correct execution for ordinary Rust code. The result is that most engineers can now make use of this technology in a wide array of applications.

Some challenges remain, most notably preventing implementation bugs. To address this challenge we are entering a golden age of formally verified proof systems. Formal verification tools, such as Lean, can be used to prove that an implementation has no soundness bugs. Moreover, modern LLM systems are surprisingly good at generating Lean proofs. As a result, we are getting close to a time where a SNARK system will only be deployed once one has a complete Lean proof that the system is sound.

Looking ahead, we are seeing many intersections with AI. AI systems are regularly used to hunt for soundness bugs, optimize prover implementations, and break some (weak) cryptography. We expect that in the near future, every deployed cryptographic system will be vetted by a frontier AI system. Conversely, cryptographic techniques will be needed to contain and constrain advanced models.

The pace of discovery in this area is astounding, and we expect progress to further accelerate in the coming years.

These are exciting times for proof systems. Enjoy the report.

Professor of Computer Science and Electrical Engineering, Stanford University. Co-director of the Stanford Computer Security Lab

What is a zero-knowledge proof

Today, proving something usually means handing over the evidence: your ID, your financial records, your code. A zero-knowledge proof separates the two. It proves a fact is true while the information behind it stays private, so anyone can verify the claim without seeing the data.

State your fact

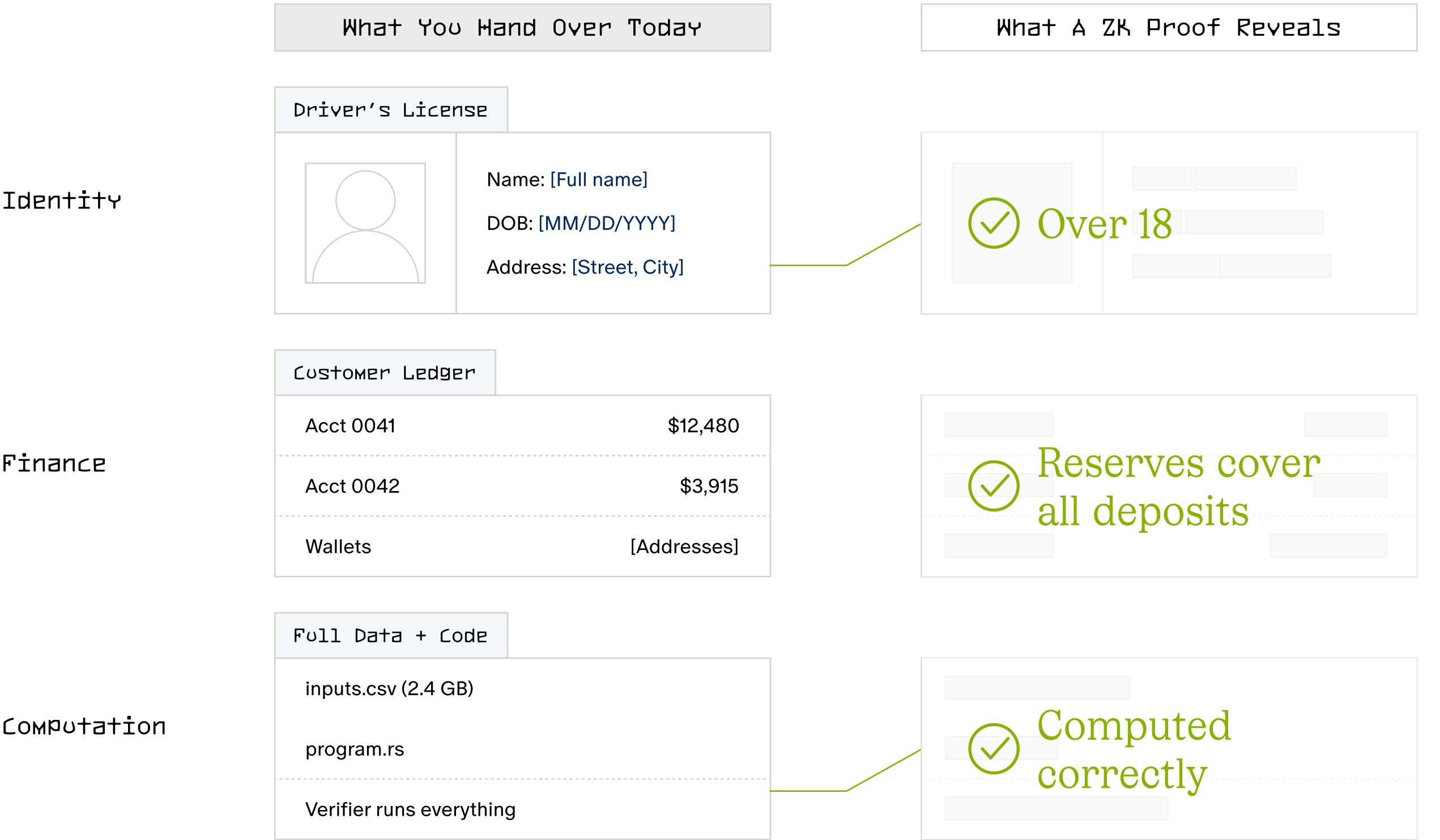
- I'm over 18.
- This block executed correctly.
- These reserves cover all balances.

Cryptographically prove it

A small proof is generated from the private data, which never leaves your hands.

Anyone can verify

Verification takes milliseconds and requires no trust in whoever made the claim.



[Go deeper ↗](#)

Watch a cryptographer explain zero-knowledge proofs at five levels of difficulty, from a child to an expert.

Source: Computer Scientist Explains One Concept in 5 Levels of Difficulty | WIRED

The Trust Tax

The internet has always run on outsourced trust.

You could not personally check that a counterparty was who they claimed, that a record was unaltered, or that a computation had run correctly, so you relied on whoever sat in the middle: a bank's internal ledger, a platform's moderation team, a KYC vendor inspecting a scanned ID, an auditor sampling records once a year.

We outsourced trust to a few central parties because they could verify at scale.

This worked as long as verifying information cost less than faking it. With AI, the math no longer holds. Synthetic documents, receipts, images, and behavior now cost next to nothing to produce, while intermediaries build ever more expensive systems to catch them. A bank onboarding a customer, a fintech settling a payment, a platform moderating a feed, a registry issuing a credential. Verification has only gotten more expensive, and trust must now be paid for.

A zero-knowledge proof moves the cost of verification back to the claimant by requiring them to produce cryptographic evidence for their claim. When claims are anchored to a source such as a signed sensor, an issued credential, or a verified computation, anyone can verify them cheaply, and false ones cannot be forged. Until recently, producing these proofs was slow and expensive. That is no longer true. Proving costs have fallen sharply, and tooling has matured from bespoke circuits to general-purpose virtual machines, so an engineer can write ordinary code and get a proof. ZK proofs are already in production across national governments, major consumer products, and global banks.

What Trust Costs Today

Every organization is now already paying for trust. It shows up as fraud losses, manual review, audit fees, compliance headcount, and the counterparties who charge more or move slower because your claims cannot be verified. Where that cost lands is different for every business.

Policy Compliance	Data Integrity	Proof Of Reserves	Agent Authorization
-------------------	----------------	-------------------	---------------------

Verifiability for your products

Your product is only as valuable as the trust others extend to it. Every output it produces – a balance, a settlement, a credential, a report – is a claim someone else must accept before acting on it. Today that acceptance is earned with audits, integrations, brand, and time.

ZK proofs make that output self-verifying. Anyone can check it without access to your systems or your data.

Age Verification	Credential Checks	Private Payments	Confidential Records
------------------	-------------------	------------------	----------------------

Privacy for your users

Your users share confidential information because it is the only way to prove their identity. But every record you hold is a liability you carry on their behalf. ZK proofs let you verify claims without your users surrendering the data behind them. You can grant access, approve accounts, and clear transactions without storing sensitive data.

On-Prem Proving	Permissioned Access	Verifiable Audits	Tamper-Proof Logs
-----------------	---------------------	-------------------	-------------------

Security for your infrastructure

Anyone who needs to verify your operations needs privileged access inside your perimeter: auditors with read access, vendors with data feeds, counterparties with API keys. ZK proofs move verification outside your walls. The only thing that leaves your environment is a proof, which any counterparty can verify without touching your infrastructure.

KYC/AML	EU Digital Identity Wallet	GENIUS Act	GDPR
---------	----------------------------	------------	------

Compliance for your company

Regulation is pulling in two directions at once. Verify more, from customer identity to transaction screening, while collecting and retaining less data. Meeting one demand requires violating the other. ZK proofs satisfy both demands at once by demonstrating compliance without collecting the underlying data.

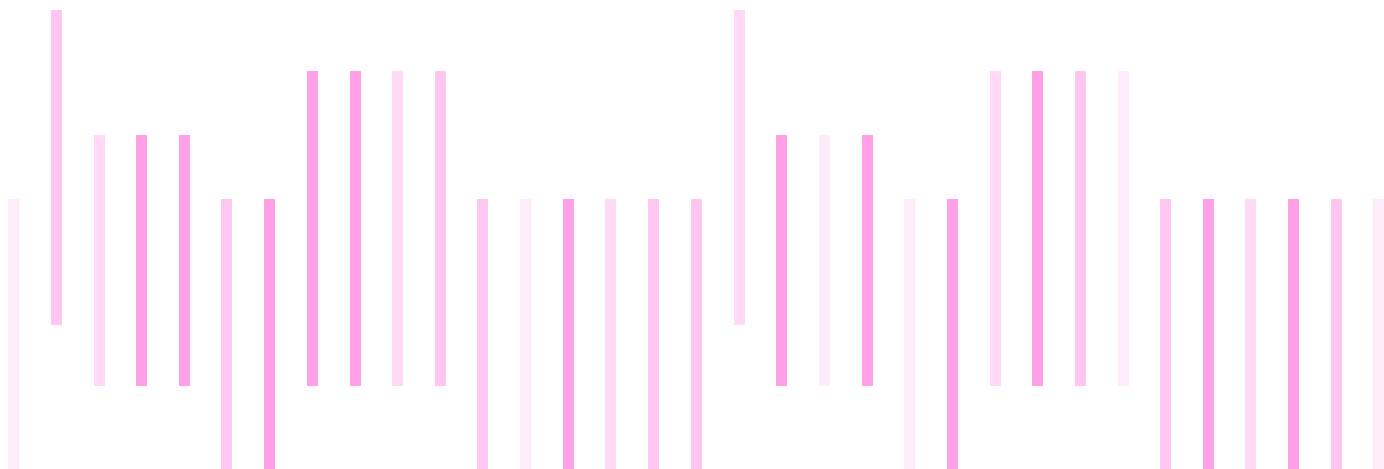
The State of the Technology

ZK systems are faster than we could have imagined. A decade of progress has been speedrun: proofs that once took minutes now take seconds, and bespoke circuits have given way to general-purpose zkVMs. ZK already runs in government identity systems, consumer applications, and bank settlement infrastructure. The technology is no longer the bottleneck. What follows is where proving stands, where research is heading, and what the world will look like.

State of Proving

Ethproofs launched in January 2025 as a simple dashboard tracking ZK proofs of Ethereum L1 blocks, but it quickly managed to align teams towards a singular goal. Within a year it had become the scoreboard for a ZK-themed space race. By the Ethproofs team's own accounting, latency fell 5x and cost-per-proof 15x during 2025, with eight zkVMs and fifteen provers verifying roughly 200,000 blocks.

In December 2025, the Ethereum Foundation declared the milestone reached: real-time proving works, with participating zkVMs proving 99% of mainnet blocks in under 10 seconds on target hardware. The goalposts have since moved — sub-8s P99 latency, energy-per-proof replacing cost-per-proof, and formally verified 128-bit security as the 2026 bar — a sign the race has shifted from raw speed to reliability and hardening.



5x

Lower proving latency

15x

Reduction in proving cost

8

zkVMs

4.9s

Latency per proof

\$0.0048

Cost per proof

Source: [Ethproofs](#)

State of Research

Pattern #1 — Toward Zero Overhead

The blockchain benchmark has been achieved, but proving a general computation still costs orders of magnitude more than running it. Much of the ZK engineering power over the last few years has been put towards this, pushing prover time toward parity with the cost of native execution.

Pattern #2 — AI and competitions as engineering accelerants

The field's engineering culture has progressively reorganized around open scoreboards and high-velocity competition. ZK Hack Online competitions trained a generation of practitioners; L2Beat made decentralization claims comparable; Ethproofs turned block proving into a public leaderboard and helped align the industry; and newer formats, like snark.fast, zk.golf, and better.codes, are pairing experts with purpose-directed AI agents. These Auto Research competitions compress the engineering cycle from months to days.

Pattern #3 — Hash-based, PQ-resistant constructions

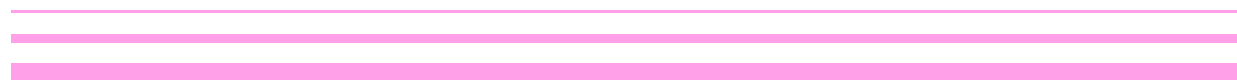
The field is moving away from elliptic curves and pairings toward hash-based proof systems. While initially motivated purely by better performance, it has had lucky secondary benefits: hash-based constructions resist quantum attacks and pairing-based ones do not. They also rely on fewer assumptions. So systems using hash-based constructions are considered post-quantum secure — an important security consideration for practitioners with Q-Day on the horizon (see sidebar). But these hash-based systems must still be battle-tested, especially the newer constructions, and we must make these transitions carefully.

The Quantum Clock Has Sped Up

Q-Day estimates moved closer this year. Not because quantum hardware leapt forward, but because the algorithms that interface with that hardware did. Google's latest resource estimates cut the projected cost of breaking today's public-key cryptography by roughly 20x, prompting both Google and Cloudflare to set 2029 deadlines for their own post-quantum migrations. Ethereum put together a dedicated PQ security team in January 2026 (pq.ethereum.org), with a migration built on signature agility. Now, individual accounts can adopt PQ signatures via account abstraction, and hash-based signatures replace BLS at the consensus layer. For ZK, the exposure is specific — pairing-based SNARKs break, hash-based systems don't — one reason the field's move toward hash-based proving (Pattern #3) doubles as quantum insurance.

ZK Adoption Across Industries

The demand for privacy and verifiability is now mainstream-validated; the open question in each category is whether it gets met with ZK or with trusted operators.



01 Digital Asset Infrastructure

Every cross-chain action depends on one chain trusting another. ZK proofs accomplish that using verification. A chain checks a proof of another's state instead of waiting days or relying on a committee of signers.

Settlement



The three largest optimistic rollups are all converging on ZK. Base activated its Azul upgrade in May 2026, running ZK and TEE proofs in parallel to cut withdrawals from 7 days to about 1. Optimism named Succinct its first preferred ZK provider in February 2026 to make validity proofs canonical across the OP Stack. And Arbitrum can now generate ZK proofs for real Arbitrum One mainnet blocks using its existing execution code, potentially reducing withdrawal times to Ethereum from days to hours, pending further integration and a DAO-approved upgrade.

Bridging



Cross-chain messaging is adopting ZK proofs as part of its verification flow. In September 2026, Chainlink's CCIP 2.0 opened its verification layer to independent providers, including a ZK verifier, so high-value transfers can require both Chainlink's committee and a ZK proof before executing.

Asset Issuers



For issuers, cross-chain risk is existential: when Kelp's bridge was drained in April 2026, the damage spread to rsETH collateral across more than 20 chains. ZK systems now enforce issuer guarantees directly. Polygon's Agglayer uses proofs to ensure no chain can withdraw more of an asset than it holds on record, which kept \$200M in volume flowing while other chains paused.

Exchanges



Lighter, a perpetuals exchange built as a ZK rollup, encodes order matching, risk checks, and liquidations in ZK circuits, so traders can verify every order executed in price-time priority and every liquidation followed the rules. It has processed over \$1.6 trillion in cumulative volume since launching in October 2025.

7 days → ~1 day

Withdrawal times on Base after upgrading to ZK proofs

\$1.6T

Lighter's ZK rollup volume since Oct 2025

\$200M

Bridge volume safely settled by Agglayer's ZK bridge during the Kelp exploit.

02

Private Payments

Public blockchains make every payment visible to everyone, which is a non-starter for most financial transactions. ZK proofs let a network verify that a payment is valid without revealing who paid whom or how much.

Zcash



In August 2026, Grayscale launched the first US privacy-coin ETF on Zcash, and usage backs the demand: roughly 30% of supply is now held privately, up from 8% in early 2024, and shielded transactions hit an all-time high of 59% of network activity in February 2026.

Aztec zk.money



Relaunched in September 2026 as a self-custodial wallet on Aztec's privacy L2, zk.money hides balances, amounts, and counterparties while giving users readable payment handles in place of addresses.

Pay



Pay brings ZK privacy to everyday stablecoin spending. Its self-custodial wallet and Visa card serve over 100,000 users in 120 countries, processing roughly \$130 million in annualized volume, and in 2026 it launched Pay Network, an Ethereum L2 where token transfers are private by default.

Circle USDC



In January 2026, Circle's privacy-preserving version of USDC went live on Aleo, using ZK proofs to encrypt balances and counterparties while letting institutions grant auditors and regulators view access.

8% → 30%

Share of Zcash supply held privately, from early 2024 to today

59% shielded

Zcash network activity shielded, an all-time high (February 2026)

100,000+ users

Pay users spending stablecoins privately

03 Institutions

Banks and exchanges are using ZK to prove what they hold and to settle with each other without exposing client data.

Proving Reserves



OKX publishes monthly proof-of-reserves reports using ZK proofs, covering \$27.7 billion in on-chain assets, and Binance updated its ZK-based reserve proofs in January 2026. Customers can verify that their balances are backed without the exchange revealing anyone else's.

Private Bank Settlement



Seven US regional banks, including Huntington, M&T, and KeyCorp, are building a tokenized deposit network on ZKsync's Prividium, with production launch targeted for the end of 2026. Deutsche Bank's tokenized fund platform already runs on a private ZK chain, cutting fund deployment from months to weeks.

Confidential Transactions



Santander, Itaú, and JPMorgan's Kinexys have piloted Rayls, a bank-focused network that uses ZK proofs alongside encryption to hide sender, recipient, and amount while giving designated auditors visibility. Brazil's central bank used the same privacy technology in its Drex digital currency pilot.

\$27.7B covered

On-chain assets covered by OKX's monthly ZK proof-of-reserves reports

7 US Regional Banks

Building a tokenized deposit network on ZKsync's Prividium

Months → Weeks

To deploy a fund on Deutsche Bank's private ZK chain



04

Identity & Credentials

Identity forces a bad trade-off: to prove one fact, like being over 18, users must hand over an entire ID. ZK proofs reveal only the claim that matters, so businesses get a verified answer without collecting or securing the data behind it.

Regulation



The European Commission has developed an open-source age verification app that is built around ZK to help users prove they meet minimum age requirements for online platforms without sharing personal data. With every member state required to offer a Digital Identity Wallet by the end of 2026, ZK is emerging as the standard for privacy-preserving identity across the EU.

Big Tech



Google shipped ZK age verification in Google Wallet, allowing any app or website to request a ZK proof using an API. In 2026, Google expanded to the EU with Sparkasse, Germany's largest savings bank group, which issues age credentials its customers can use for one-click age checks without disclosing personal data.

Consumer Platforms



World has become the largest proof-of-personhood network, with more than 18 million people verified by its Orb and ZK proofs that confirm uniqueness without revealing identity; Tinder, Zoom, and Okta have integrated it since April 2026. Celo's Self instead builds on IDs people already carry. Users scan the chip in their passport or ID and prove facts like age or nationality in ZK, an approach Google Cloud already uses.

Enforcement

2026 has seen a sharp rise in enforcement against self-declared age gates, from a £14.47 million UK fine against Reddit to EU action against Meta under the Digital Services Act. Platforms now face a choice between collecting more identity data or proving age without it.

475M+ proofs

World ID proofs generated since launch

7 member states

EU states piloting ZK age verification

450M people

EU population covered by the 2026 Digital Identity Wallet mandate

05 Frontier

The next wave of ZK is being built around one problem: in an AI-saturated world, how do you prove what's real?

Verifiable AI

Proving that a specific model produced a specific output, without revealing its weights, went from impractical to possible for large language models in 2026. Attestable proved inference for production-scale models including Gemma 4 31B at 53 to 77 tokens per second on a single GPU, with proofs that verify in under a second.

Responsible Disclosure

In March 2026, Google Quantum AI released a paper warning that quantum computers could break the elliptic curve cryptography protecting Bitcoin and Ethereum much sooner than previously estimated. In the paper, they published a ZK proof generated by SP1, proving a new quantum algorithm beat the previous state of the art without revealing how to reproduce it.

Provenance & Media Authenticity

With AI fakes outpacing detectors, the industry is shifting to fingerprinting real media. C2PA content credentials are now mainstream, but their signatures break on any edit and can expose the signer. ZK fills both gaps: Microsoft Research prototyped proofs that let journalists authenticate C2PA content anonymously, and ZK-JPEG proves a published image was faithfully compressed from a signed original.

Private Moderation & Reputation Scoring

Research such as zk-promises lets platforms moderate, score, and block users based on their history without ever seeing it, enabling accountability for anonymous accounts.

53–77 TPS

Tokens per second of proven AI inference

10x

Fewer quantum resources needed to break Bitcoin

\$1.65B

Deepfake fraud losses in 2025

Proving is no longer the bottleneck

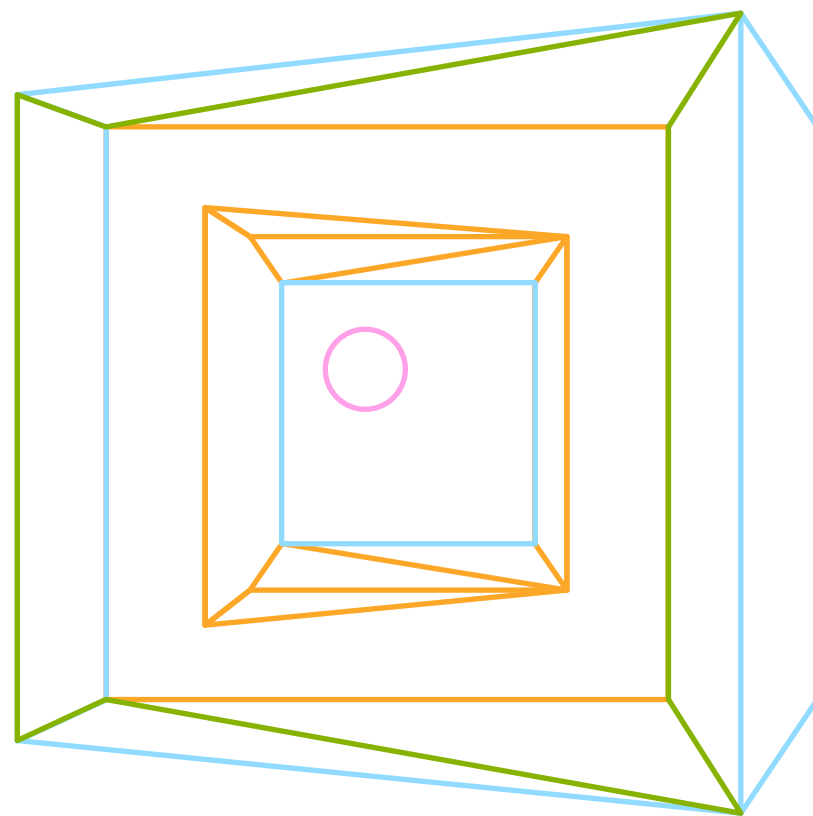
ZK is in production well beyond crypto

Regulators are pushing ZK into the mainstream

The forces that made ZK urgent are not slowing down. AI keeps collapsing the cost of fabrication — documents, media, identities, even the results of computation — while inspection keeps getting less reliable as a check. Regulators keep demanding stronger verification, while privacy law keeps raising the price of holding the data those checks have traditionally required. And the quantum deadline has now moved up on the calendars of Google, Cloudflare, and Ethereum. In that environment, ZK shifts from nice-to-have to need-to-have. The organizations that build verifiability in now are building protection against all three forces at once.

Everything this report describes — real-time proving, civic identity, shielded payments, bank settlement — existed only on whiteboards a few years ago. Demand for privacy and verifiability is mainstream-validated and growing. The open question is whether ZK will become fast enough to match general computation and whether the market choose ZK over trusted operators. That answer belongs to the people building right now, and we hope some of them found their next project in these pages.

2026 ZK Industry Report



Produced by

