

Privacy & Zero-Knowledge Proofs

A Visual Introduction

Prof. Dr. Joerg Osterrieder

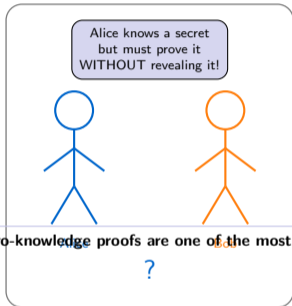
University Lecture Series

"Privacy is the power to selectively reveal oneself to the world."

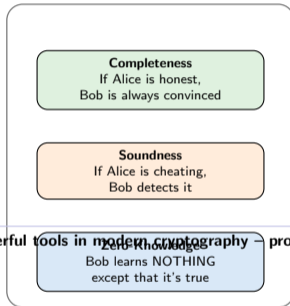
— Eric Hughes, A Cypherpunk's Manifesto (1993)

What is a Zero-Knowledge Proof?

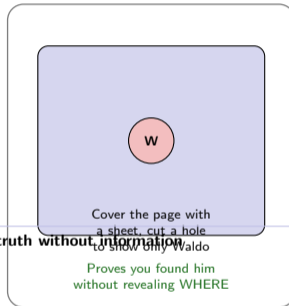
The Challenge



Three ZK Properties



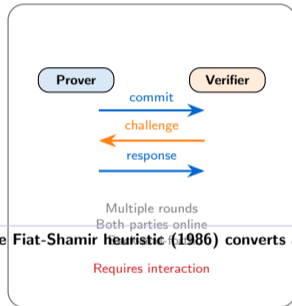
The Waldo Analogy



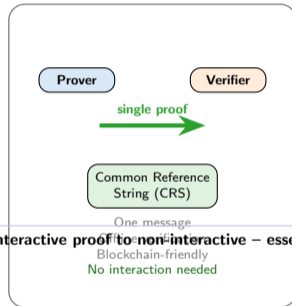
Zero-knowledge proofs are one of the most powerful tools in modern cryptography – proving truth without information

Interactive vs Non-Interactive Proofs

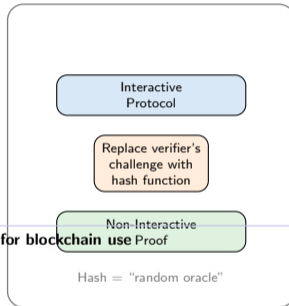
Interactive ZK



Non-Interactive (NIZK)



Fiat-Shamir Transform



The Fiat-Shamir heuristic (1986) converts any interactive proof to non-interactive – essential for blockchain use

Proving Without Revealing

Discrete Logarithm Problem

Given g , p , and $y = g^x \bmod p$
Finding x is computationally hard

Alice can prove she **knows** x
without ever sending x to anyone!
This "hardness assumption" is the
foundation of ZK proof security

Key idea: Easy to verify ($g^x \stackrel{?}{=} y$)
but hard to reverse (find x from y)

Commitment Schemes

Pedersen Commitment

$$C = g^v \cdot h^r$$

g, h = generators, v = value, r = randomness

Hiding

Cannot recover
 v from C
(info-theoretic)

Binding

Cannot change
 v after commit
(computational)

Mathematical hardness assumptions (discrete log, pairings) make zero-knowledge proofs possible

Like a sealed envelope: you commit to a value
without revealing it, but can't change it later

zk-SNARKs

Succinct
Non-interactive
ARgument of
Knowledge

Proof size: ~200 bytes
Verification: $O(1)$
Very fast to verify!

Requires trusted setup
Not quantum-safe

zk-STARKs

Scalable
Transparent
ARgument of
Knowledge

No trusted setup!
Post-quantum secure!
Proof: $O(\log^2 n)$

Large proof (STARK)
Heavier prover cost

Head-to-Head

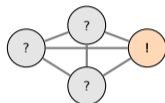
| | SNARK | STARK |
|---------|---------|--------|
| Setup | Trusted | None |
| Proof | ~200B | ~45KB |
| Quantum | No | Yes |
| Verify | Fast | Fast |
| Prover | Fast | Slower |

SNARKs: Zcash, zkSync
STARKs: StarkNet, Cairo

Choose based on your
trust & quantum needs

SNARKs trade trusted setup for tiny proofs; STARKs avoid trust assumptions but produce larger proofs

Monero (XMR)



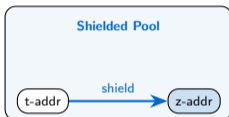
Ring signatures:
real signer hidden
among decoys

+ Stealth addresses

+ RingCT (hidden amounts)
+ Dandelion++ (network)

Default privacy for all

Zcash (ZEC)



zk-SNARKs prove
valid transactions
without revealing details

Transparent (t) or
Shielded (z) addresses
Opt-in privacy model

Monero vs Zcash

| | XMR | ZEC |
|---------|----------|----------|
| Privacy | Default | Opt-in |
| Crypto | Ring sig | SNARKs |
| Setup | None | Trusted |
| Tx size | ~2KB | ~2KB |
| Audit | Hard | Possible |

Both achieve strong
privacy but via very
different approaches

Different philosophy:
always-on vs opt-in

Monero uses ring signatures for default privacy; Zcash uses zk-SNARKs for optional shielded transactions

ZK-Rollups Simplified

The Problem



Ethereum L1:
~15 TPS
High gas fees
Congested

ZK-Rollups batch thousands of transactions off-chain and post a single proof on-chain – the future of scaling.

Cannot scale to
millions of users

ZK-Rollup Solution



ZK
Proof

Single proof
on L1

The Result

1000x throughput
Thousands of txs
verified with one proof

Low gas cost
Proof verification
is cheap on L1

Projects:
zkSync, StarkNet,
Polygon zkEVM, Scroll

Private Voting



Anonymous but verifiable elections
Prove eligibility without revealing identity
Prevent bribery & coercion (MACI)

Identity Verification



Prove age ≥ 18 without showing ID
Self-sovereign identity (SSI)
Selective disclosure of credentials

DeFi Privacy



Private trading (no front-running)
Hidden balances & amounts
Railgun, Aztec, Penumbra

Supply Chain



Prove product authenticity
Without exposing trade secrets
Verify compliance privately

ZK proofs enable "verify without revealing" across voting, identity, finance, and supply chains

ZK Evolution Timeline

- 1985 GMR: ZK proofs defined
- 2012 SNARKs constructed
- 2016 Zcash launches
- 2018 STARKs published
- 2020 PLONK universal setup
- 2023 ZK-Rollups go live

From a 1985 theory paper to production rollups in 2023 – ZK technology is accelerating rapidly

ZK Ecosystem Map

Research: Universities, IACR, Ethereum Foundation
Zero-knowledge theory, new proof systems

Infrastructure: Circom, Noir, Cairo, Halo2, SP1
Proving systems, compilers, developer tools

Applications: zkSync, StarkNet, Zcash, Worldcoin
Rollups, privacy, identity, compliance

“ZK is the most important cryptographic breakthrough since public-key cryptography” – many researchers

1. ZK proofs prove knowledge without revealing it – completeness, soundness, zero-knowledge

2. SNARKs are small but need trusted setup; STARKs are transparent and quantum-safe

3. Privacy coins (Monero, Zcash) use different cryptographic approaches to hide transactions

Zero-knowledge proofs are transforming blockchain scalability, privacy, and identity – the future is provable

4. ZK-Rollups are scaling Ethereum by orders of magnitude using validity proofs

5. ZK powers private voting, identity verification, DeFi privacy, and supply chain integrity

Coming Next: Deep dive into proof system math, circuit design, privacy coin internals, and ZK-rollup architecture