

BLOCKCHAIN BASICS

Zero-Knowledge Proofs Explained: ZK Technology in Crypto

By Matt Barnez

Written

Nov 15, 2026

What if you could prove you're old enough to access a service without revealing your birth date? Or verify that you have enough funds without exposing your account balance?

That's the idea behind zero-knowledge proofs (ZKPs), a cryptographic technology that allows information to be verified without revealing the private data behind it.

As blockchain technology develops, ZK proofs are becoming increasingly relevant to privacy, security, and scalability.

What Are Zero-Knowledge Proofs?

Zero-knowledge proofs are cryptographic methods that allow someone to prove a statement is true without revealing the private information used to prove it.

They involve two participants:

- Prover: Generates evidence that a statement is valid.
- Verifier: Checks whether the evidence is mathematically valid.

For example, a user could prove they're over 18 without sharing their exact age, provided a trusted system has already verified the underlying information.

This approach is particularly useful for public blockchains, where transaction information is often visible to everyone.

How Do Zero-Knowledge Proofs Work?

Zero-knowledge proofs use mathematical techniques to verify specific claims while protecting private inputs.

The process generally involves four steps:

1. Define a statement: A user wants to prove something, such as meeting an age requirement.
2. Generate a proof: Cryptographic software creates evidence using private information.
3. Verify the proof: The verifier checks the evidence without accessing the private data.
4. Confirm the result: The system accepts or rejects the claim based on verification.

For example, a digital identity service could confirm that a user meets an age requirement without revealing their birth date.

However, ZK technology does not automatically guarantee that the original information is accurate. The system must still rely on trustworthy data sources.

zk-SNARKs vs zk-STARKs: What's the Difference?

Two important types of zero-knowledge proof systems are zk-SNARKs and zk-STARKs.

zk-SNARKs

zk-SNARK stands for *Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*.

These systems typically produce compact proofs that can be verified efficiently.

Some zk-SNARK constructions require a trusted setup, although others use different approaches.

zk-STARKs

zk-STARK stands for *Zero-Knowledge Scalable Transparent Argument of Knowledge*.

STARK systems use transparent setup procedures and can support verification of large computations.

However, their proofs are often larger than SNARK proofs, potentially increasing data and verification costs.

Both technologies provide cryptographic verification, but their performance and security assumptions differ.

How Are Zero-Knowledge Proofs Used in Crypto?

ZK technology supports several blockchain applications.

Privacy-Preserving Transactions

Zero-knowledge proofs can verify transactions while keeping selected details, such as amounts or participant information, confidential.

However, privacy depends on the overall design of the application.

Blockchain Scalability

ZK rollups process transactions outside Ethereum's main network and submit cryptographic validity proofs to verify the resulting state changes.

This reduces the need for Ethereum to repeat every computation.

Importantly, ZK rollups do not automatically make transactions private.

Digital Identity

ZK technology can help users verify identity-related attributes, such as age or eligibility, without sharing unnecessary personal information.

Decentralized Finance (DeFi)

Some DeFi applications use zero-knowledge proofs to verify financial conditions while protecting sensitive data.

For example, a system could demonstrate that collateral requirements are satisfied without revealing every underlying financial detail.

Benefits of Zero-Knowledge Technology

Zero-knowledge proofs offer several potential advantages:

- Privacy: Verify information while protecting private inputs.
- Security: Use cryptographic verification instead of exposing sensitive data.
- Efficiency: Verify complex calculations without repeating all the underlying work.
- Selective disclosure: Prove specific facts without sharing complete records.
- Blockchain innovation: Support applications involving digital identity, DeFi, and scaling solutions.

These benefits depend on how securely and effectively the technology is implemented.

Risks and Limitations of Zero-Knowledge Proofs

Despite their advantages, ZK systems face several challenges.

Technical complexity: Advanced cryptography makes implementation and auditing difficult.

Computational costs: Generating proofs can require substantial processing resources.

Security vulnerabilities: Coding mistakes, incorrect verification logic, or compromised setup procedures can undermine security.

Limited privacy: Blockchain metadata or other publicly available information may still reveal sensitive details.

A valid proof also confirms only a defined mathematical statement. It does not guarantee that external information is accurate.

Zero-Knowledge Proofs vs Traditional Verification

Feature	Zero-Knowledge Proofs	Traditional Verification
Data disclosure	Can protect private inputs	May require sharing personal data
Verification	Cryptographic proofs	Documents or direct checks
Privacy	Potentially stronger	Depends on data handling
Complexity	Often technically demanding	Varies by system
Applications	Blockchain, identity, DeFi	Authentication and record verification

Zero-knowledge proofs are particularly useful when verifying information without exposing unnecessary details is important.

The Future of Zero-Knowledge Technology

Zero-knowledge proofs could play a greater role in blockchain scalability, digital identity, privacy-preserving financial applications, and verifiable computing.

However, widespread adoption will depend on lower computational costs, reliable security, and easier integration with existing systems.

While ZK technology cannot solve every privacy or security problem, it offers important tools for building more efficient and privacy-conscious digital services.

Conclusion

Zero-knowledge proofs allow information to be verified without revealing the private data behind it.

In cryptocurrency, they support privacy-preserving transactions, blockchain scaling, and digital identity applications.

Technologies such as zk-SNARKs and zk-STARKs provide different approaches to cryptographic verification, each with its own advantages and limitations.

As blockchain technology evolves, ZK proofs may become an increasingly important part of secure digital infrastructure.

Disclaimer: This article is for educational and informational purposes only and does not constitute financial, investment, or technical security advice. Blockchain technologies involve technical and financial risks.