# Blockchain privacy tools with zero-knowledge proofs emerge as key defence against AI-driven cyber threats



As the digital landscape evolves, the necessity for robust privacy tools becomes more pronounced, especially in an era increasingly dominated by artificial intelligence (AI). Eran Barak, CEO of Shielded Technologies—which is behind the innovative Midnight privacy chain—asserts that blockchain privacy solutions, particularly zero-knowledge (ZK) proofs, are set to become vital for protecting sensitive user data against escalating cyber threats.

In a recent interview at Consensus 2025, Barak highlighted the vulnerabilities associated with centralized service providers and servers that are becoming attractive targets for cybercriminals. These entities often contain troves of valuable data such as private keys, financial metadata, and even sensitive medical records, which AI-assisted hackers could exploit. According to Barak, hacking these centralized repositories promises a "massive" return on investment due to the sheer volume of records they hold. In contrast, the decentralised nature of blockchain technology can act as a deterrent: “For a hacker to get to actual data, they need to hack individual wallets, but their ROI would be one record instead of millions—not worth it. They are going to go elsewhere,” he explained.

As the demand for privacy solutions intensifies, many Web3 developers are realising the necessity of shielding metadata from AI algorithms. Large institutions are increasingly insisting on privacy protections before they consider bringing their business operations on-chain, creating a pressing demand for solutions that can maintain privacy while ensuring regulatory compliance. Notably, the Midnight chain is structured to enable users to generate shielded assets, providing a layer of anonymity in transactions while adhering to necessary regulations.

The importance of zero-knowledge proofs extends beyond the confines of blockchain privacy to mainstream applications. Google has recently enhanced its Wallet service by incorporating ZKP technology for age verification purposes. This landmark move allows users to verify their age without disclosing personal details, thus addressing concerns linked to traditional age verification methods. Similarly, blockchain-based self-sovereign identity frameworks are employing ZKP technologies to empower individuals to assert their identity without compromising their privacy, further exemplifying the growing recognition of ZKPs as essential tools in today’s digital operations.

Emerging complexities in digital interactions have underscored the use of zero-knowledge proofs as pivotal to improving data privacy protocols. These cryptographic techniques allow for verification processes that do not necessitate sharing sensitive information, effectively bolstering security for both individuals and organisations. Their application ranges widely, from identity verification to financial services, promising a more secure future.

The adoption of zero-knowledge proofs is also gaining traction in response to the broader demand for enhanced privacy across the blockchain ecosystem. As enterprises increasingly seek to leverage blockchain technology for its myriad benefits, privacy tools like ZKPs are becoming appealing features that can drive their integration. Startup RISC Zero, for instance, has secured significant funding to advance the utilisation of these cryptographic tools within various blockchain applications, highlighting industry momentum towards adoption.

In this increasingly interconnected world, where privacy concerns are paramount, the evolution of tools that protect sensitive information is critical. With AI and cyber threats on the rise, the calls for privacy-enhancing solutions will only grow louder. As Barak noted, initiatives such as those undertaken by the Midnight chain could provide the secure framework required to navigate these challenges, potentially transforming how data privacy is approached in the age of technology.

## Reference Map:

* Paragraph 1 – [[1]](https://cointelegraph.com/news/onchain-privacy-necessity-age-ai-shielded-ceo), [[4]](https://www.forbes.com/councils/forbesbusinesscouncil/2024/10/31/why-zero-knowledge-proofs-will-shape-the-future-of-data-privacy)
* Paragraph 2 – [[1]](https://cointelegraph.com/news/onchain-privacy-necessity-age-ai-shielded-ceo), [[2]](https://www.coindesk.com/markets/2025/05/02/google-adds-zero-knowledge-proofs-to-wallet-for-age-verification), [[5]](https://www.nextbigfuture.com/2023/07/why-zero-knowledge-proofs-zkp-are-the-future-of-blockchain-privacy.html)
* Paragraph 3 – [[3]](https://www.privately.eu/post/blockchain-based-self-sovereign-identity-and-zero-knowledge-proofs-the-future-of-age-assurance), [[6]](https://www.axios.com/2023/07/19/blockchain-risc-zero-funding)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://cointelegraph.com/news/onchain-privacy-necessity-age-ai-shielded-ceo> - Please view link - unable to able to access data
2. <https://www.coindesk.com/markets/2025/05/02/google-adds-zero-knowledge-proofs-to-wallet-for-age-verification> - Google is enhancing its Wallet service with zero-knowledge proof (ZKP) technology to enable privacy-focused age verification. This system allows users to prove their age without revealing personal information, addressing privacy concerns associated with traditional age verification methods. The implementation is live across mobile devices and apps using Google’s Digital Credential API, with dating app Bumble among the first partners to utilize this system.
3. <https://www.privately.eu/post/blockchain-based-self-sovereign-identity-and-zero-knowledge-proofs-the-future-of-age-assurance> - Privately SA is pioneering a blockchain-based Self-Sovereign Identity (SSI) framework that utilizes zero-knowledge proofs (ZKPs) for age verification. This approach allows users to prove their age without disclosing personal information, enhancing privacy and compliance for businesses. The system operates entirely on the user's device, ensuring data protection and user control over personal data.
4. <https://www.forbes.com/councils/forbesbusinesscouncil/2024/10/31/why-zero-knowledge-proofs-will-shape-the-future-of-data-privacy> - Zero-knowledge proofs (ZKPs) are cryptographic techniques that enable one party to confirm the validity of information to another party without revealing the information itself. ZKPs have significant potential to improve data privacy protocols, benefiting both organizations and individuals by reducing the need to share sensitive data and enhancing security in various applications, including identity verification and financial services.
5. <https://www.nextbigfuture.com/2023/07/why-zero-knowledge-proofs-zkp-are-the-future-of-blockchain-privacy.html> - Zero-knowledge proofs (ZKPs) are emerging as a crucial component in enhancing blockchain privacy. They allow for private transactions on public chains without revealing transactional details, addressing the increasing need for privacy and security in blockchain applications. ZKPs are being integrated into various blockchain projects to provide secure and private transactions, attracting enterprise customers to blockchain technology by ensuring data privacy.
6. <https://www.axios.com/2023/07/19/blockchain-risc-zero-funding> - RISC Zero has secured $40 million in funding to enhance the adoption of advanced cryptographic tools across blockchains. The funding will be used to develop Bonsai, a set of tools designed to facilitate the integration of zero-knowledge proofs into various applications, potentially attracting enterprise customers to blockchain technology by ensuring data privacy.
7. <https://en.wikipedia.org/wiki/Zero-knowledge_proof> - A zero-knowledge proof (ZKP) is a cryptographic protocol where one party can convince another party that a given statement is true without conveying any information beyond the mere fact of the statement's truth. ZKPs are fundamental in cryptography and have various applications, including secure authentication and privacy-preserving transactions.