Zero-Knowledge Proof

Zero-knowledge proofs or zero-knowledge protocols (ZKP) is a method by which one party can interact with another party and provide proof of knowledge without unveiling their confidential data, in other words Zero-knowledge proofs let you validate the truth of something without revealing how you know that truth or sharing the content of this truth with the verifier.

Why is ZKP important?

Enterprise businesses don't want to share proprietary information that can get into the hands of their competitors. Businesses also want to ensure that the information is securely delivered to the intended party. Ordinary blockchains can accomplish this, but with ZKP businesses can share proofs about the data without sharing the data itself.

Which industries could be impacted?

Generally speaking, ZKP could impact any industry that involves transactions, identity systems, and other proprietary information. ZKP can be used as a diligence, security, and verification tool in some of the most highly regulated industries like financial services, insurance, audit firms, and many others.

Who is building ZKPs?

The majority of cryptocurrencies expose peoples entire payment history to the public. ZEC is the first open, permissionless cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography. ZEC's shielded transactions hide the sender, recipient, and value on the blockchain. ZEC was also one of the first to implement zK-SNARKS.

ING Bank launched a modified version called zero-knowledge range proofs in Ethereum. Zero-knowledge range proofs can be used to prove that someone has a salary within the range needed to attain a mortgage without revealing the actual figure. This is key because of privacy and it reduces computational power which results in faster transactions.

What are the limitations?

ZKP is computationally expensive, performance and the level of computing power required to support trust setup can be an issue. The ability to verify sensitive information like the amount of a transaction, passwords and other identifiable data will become more valuable for everyone with the rising presence of bad actors. This technology shows great promise and it is likely that there will be more partnerships between big institutions and startups working more closely together to develop new products solving privacy problems in the near future.