Zero Knowledge Proofs

Aviv Zohar

Zero Knowledge Proofs are on the bleeding edge of computer science research. They act as a double-edged sword: on the one hand, allowing modern cryptocurrencies to impenetrably mask transactions, but on the other hand opening the door to new forms of collaboration between companies, individuals and governments.

I'll explain what zero-knowledge proofs are, and how they can be used to build systems that are both private and resilient to abuse.