

# How does blockchain support data privacy? Blockchain and Data Confidentiality

Blockchain technology offers a powerful approach to enhancing data privacy in the digital world. Unlike traditional databases controlled by a single entity, blockchain is decentralized, meaning data is distributed across a network of computers rather than stored in one central location. This makes unauthorized access or tampering much more difficult.

One key feature of blockchain is the use of cryptography. Every transaction or piece of data on a blockchain is encrypted and linked to previous records, forming a secure chain. Only users with the correct cryptographic keys can access or share specific information. This selective access helps keep personal data confidential and reduces the risk of data breaches.

Another way blockchain supports privacy is through techniques like zero-knowledge proofs. These allow someone to prove that a statement is true (for example, that they are over 18) without revealing any additional personal details. Such innovations enable users to verify their identity or eligibility without exposing sensitive information.

Additionally, blockchain users can control their own data. Instead of handing over personal details to multiple organizations, individuals can grant or revoke access to their data as needed. This self-sovereign identity model puts people in charge of their digital footprint.

In summary, blockchain's decentralized structure, strong encryption, and privacy-preserving technologies collectively enhance data privacy. By limiting unnecessary data sharing and empowering users to manage their own information, blockchain helps create a safer and more private digital environment.