Blockchain and privacy

How do you protect data that's distributed?

Traditional databases store data in one place, where security systems can control access.

Blockchain copies the same data to many places, creating what we call a distributed ledger. All of these places communicate with each other to validate the data. That ensures data accuracy.

To ensure the data privacy that regulations and users require, blockchain solutions need to take non-traditional approaches. Here are three security challenges that are unique to blockchain, and how you can approach each one.

Ownership

By its nature, blockchain data is equally owned at each place where it's distributed. But, for personal data, regulations require one owner who is accountable for all data privacy.
So, instead of storing personal data in a blockchain, consider storing index numbers that tie to personal data in a separate database. Then, one organization can own and secure that database while still sharing the blockchain. Another reason to store personal data in a separate database is the need for data deletion.

Deletions

Blockchain records are permanent. If data changes, there is still a record of what it used to be. But many users want to be able to entirely delete their personal data from a system. And privacy regulations require that capability. Deletions are another reason to store personal data in a separate database. While there are statutory exceptions that let you store personal data in a blockchain, you would need to have encryption, user agreements and other statutory requirements in place.

Smart contracts

A blockchain can include little bits of code that automatically act upon the terms of a contract, such as transferring funds when an event occurs. These are called smart contracts. Privacy regulations require smart contracts to provide a way to report and correct any errors. Since blockchain transactions are permanent, you might even need to nullify and replace a smart contract. Make sure you have the appropriate rights to take that action.

Blockchain solutions can include reasonable, appropriate and compliant protections for privacy. But, you need to ensure those protections are built into your solution and your contracts. Be sure to know the regulations and the roles that technology needs to play. For more details, see our white paper: Can data privacy be achieved in blockchain?