accenture

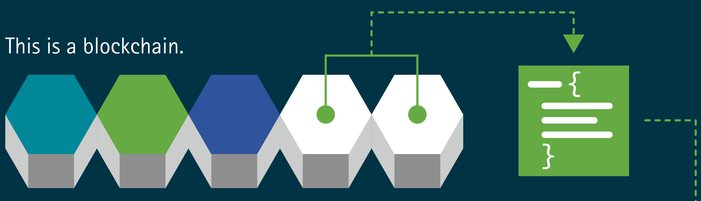
Blockchain Redaction

A new redaction capability solves a key blockchain challenge and expands its usefulness for enterprises.

Blockchain is built to be "immutable", or unchangeable. That could limit uses in financial services - because regulations might require data to be changed or removed, coding and transaction mistakes happen, and capacity and costs for retaining data need to be controlled.

Here's how redaction works.

This is a blockchain.

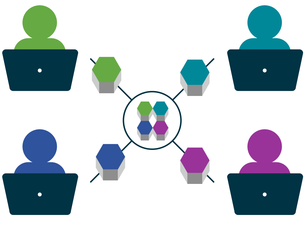


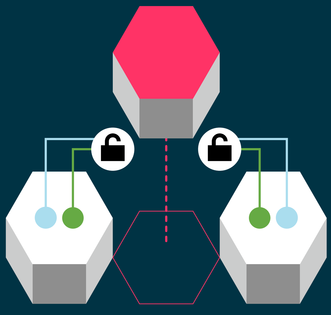
Blocks of data are linked by hashes. A hash is the output of an algorithm that turns data into a fingerprint of the data that looks something like this:

Each block contains the hash of the previous block to create the links in the chain. If the data changes, the hash changes and the link is broken.

Blocks are distributed among interested parties using a cryptographic audit trail maintained and validated by separate users that independently check the blocks.

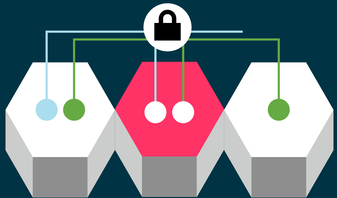
It's a shared version of the truth. If the data changes, the hash changes, and everyone involved will know.





The redaction capability is designed to work with "permissioned systems" where only designated administrators, under strict controls, are allowed to alter blocks. A special hash function called a "Chameleon Hash" is added to the standard hash that links the blocks in a chain, providing a secret key that allows the link between blocks to be unlocked so blocks may be edited and relocked.

Once a change has been made, the standard hash is broken, leaving evidence of the change. The Chameleon Hash stays intact and maintains the link between the edited and existing blocks.



Learn more about how redaction could increase blockchain use:
www.accenture.com/blockchain