Figure 1. How does blockchain work?

Blockchain allows for the secure management of a shared ledger, where transactions are verified and stored on a network without a governing central authority. Blockchains can come in different configurations, ranging from public, open-source networks to private blockchains that require explicit permission to read or write. Computer science and advanced mathematics (in the form of cryptographic hash functions) are what make blockchains tick, not just enabling transactions but also protecting a blockchain's integrity and anonymity.

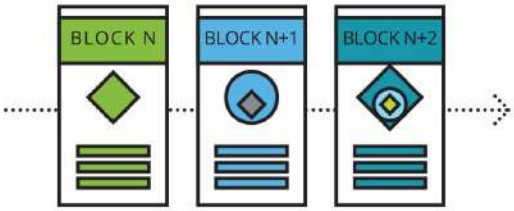
1

TRANSACTION Two parties exchange data; this could represent money, contracts, deeds, medical records, customer details, or any other asset that can be described in digital form.

2

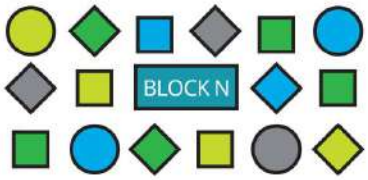
VERIFICATION Depending on the network's parameters, the transaction is either verified instantly or transcribed into a secured record and placed in a queue of pending transactions. In this case, nodes—the computers or servers in the network—determine if the transactions are valid based on a set of rules the network has agreed on.

3



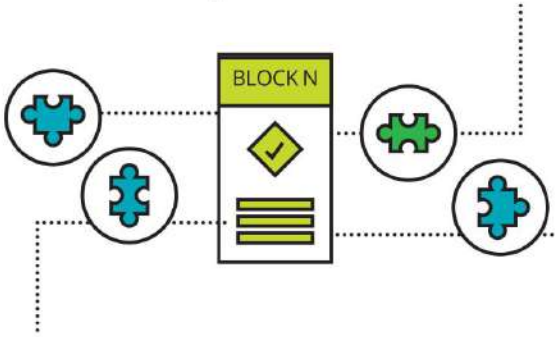
STRUCTURE Each block is identified by a hash, a 256-bit number, created using an algorithm agreed upon by the network. A block contains a header, a reference to the previous block's hash, and a group of transactions. The sequence of linked hashes creates a secure, interdependent chain.

4



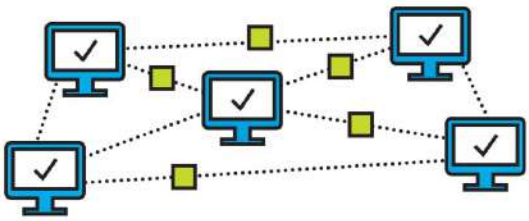
VALIDATION Blocks must first be validated to be added to the blockchain. The most accepted form of validation for open-source blockchains is proof of work—the solution to a mathematical puzzle derived from the block's header.

5



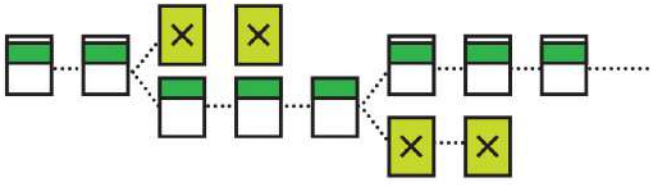
BLOCKCHAIN MINING Miners try to "solve" the block by making incremental changes to one variable until the solution satisfies a network-wide target. This is called "proof of work" because correct answers cannot be falsified; potential solutions must prove that the appropriate level of computing power was drained in solving.

6



THE CHAIN When a block is validated, the miners that solved the puzzle are rewarded and the block is distributed through the network. Each node adds the block to the majority chain, the network's immutable and auditable blockchain.

7



BUILT-IN DEFENSE If a malicious miner tries to submit an altered block to the chain, the hash function of that block, and all following blocks, would change. The other nodes would detect these changes and reject the block from the majority chain, preventing corruption.

Source: Eric Piscini, Joe Guastella, Alex Rozman, and Tom Nassim, *Blockchain: Democratized trust*, Deloitte University Press, February 24, 2016.