Step 4:

Once a block is validated or, in the case of DLTs that do not combine transactions in blocks, once the transaction has been validated, it is time-stamped and linked to the preceding blocks/transactions with a "hash pointer" – a hash of the previous block/transaction – thereby forming a linear chronological chain of blocks/transactions.

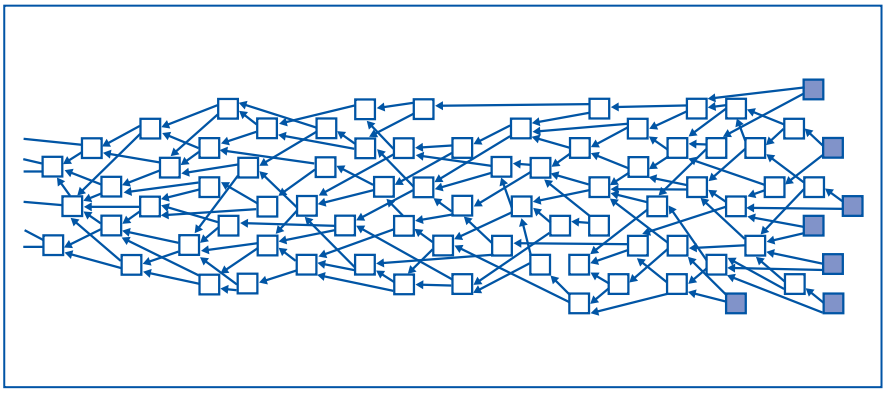
The transactions are then confirmed and the block/transaction cannot be altered or removed – thus, the block/transaction is immutable. Each time a block/transaction is added to the chain, the digital ledger is updated on all the participating nodes. The systematic update of the ledger on all the nodes is an efficient way to ensure that there are no divergent versions of the ledger in the participating nodes.

Other distributed ledger technologies follow a different process. In IOTA, for example, transactions are not grouped into blocks and each transaction is linked to two previous transactions as part of the validation process to form a "Tangle" (see Figure A.3).

What makes Blockchain so different?

While the various techniques described above – digital signatures, hashing, encryption, Merkle trees – have been the mainstay of information security for several decades, their resistance to malicious attacks has constantly been challenged, leading to a neverending cat-and-mouse game between hackers and cybersecurity specialists to develop and crack codes. Improvements were made, with no major breakthroughs until the creation of blockchain technology.

Figure A.3 The Tangle



Source: IOTA.[3]