Once a transaction is validated it is recorded on the blockchain.

• Assuming nodes follow the proof of work consensus protocol:
  - Nearby nodes invest compute power to solve a mathematical puzzle required to produce the next block within which the proposed transaction is recorded (this is mining).
  - When the first node solves the mathematical puzzle they win a fee and the pending transaction is recorded in a new block of data.
  - That new block is double checked by other members of the network until a majority agrees it is correct and then its added to the blockchain and becomes part of the database.

Transactions are sent by accounts and validated in accordance with the consensus protocol (process embedded in the blockchain software used by nodes to reach agreement on whether a transaction can be validated).

• There are different consensus protocols used by different blockchain networks. “Proof of work” is used for the Bitcoin blockchain. Proof of work involves mining.

Blockchain software installed and running by user on a machine is called a node.

• Each node stores a copy of the database (list of transactions).

• Nodes used to set up accounts (used by users to participate in the blockchain: create and send new transactions).

• Private keys (a secret number generated for an account) are used to operate accounts.

• Public keys (a public number generated for an account) identify each account on the blockchain.

Node

X and Y users want to send a new transaction to the blockchain (X user transfers Z digital currency to Y).

• X and Y broadcast cryptographically secured digital signatures (combination of their public and private keys) and the details of their transaction to nearby nodes in the network.