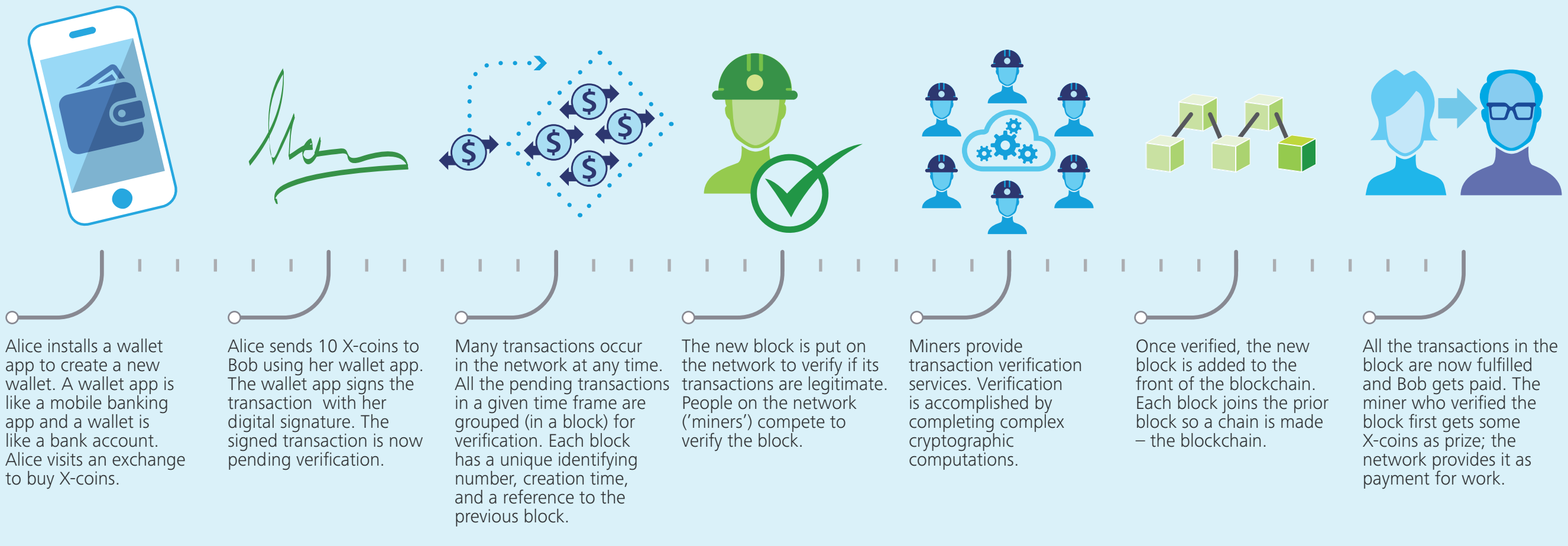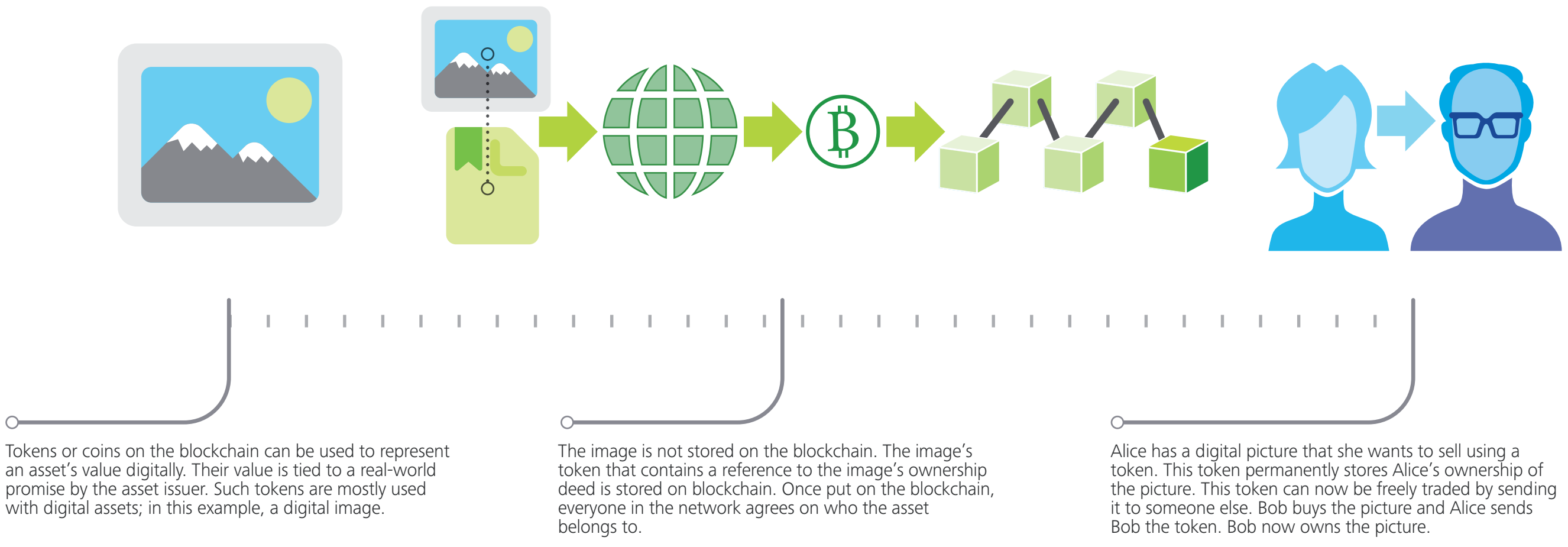# How does a blockchain work?

Below are a few sample use-cases that can be implemented using both public and private blockchains. In the case of public blockchains, the need for trusted intermediaries and central authorities can be eliminated, making the process potentially significantly more cost-effective.

## Payments example with X-coins (x could be bitcoin or other cryptocurrencies)

Alice installs a wallet app to create a new wallet. A wallet app is like a mobile banking app and a wallet is like a bank account. Alice visits an exchange to buy X-coins.

Alice sends 10 X-coins to Bob using her wallet app. The wallet app signs the transaction with her digital signature. The signed transaction is now pending verification.

Many transactions occur in the network at any time. All the pending transactions in a given time frame are grouped (in a block) for verification. Each block has a unique identifying number, creation time, and a reference to the previous block.

The new block is put on the network to verify if its transactions are legitimate. People on the network ('miners') compete to verify the block.

Miners provide transaction verification services. Verification is accomplished by completing complex cryptographic computations.

Once verified, the new block is added to the front of the blockchain. Each block joins the prior block so a chain is made – the blockchain.

All the transactions in the block are now fulfilled and Bob gets paid. The miner who verified the block first gets some X-coins as prize; the network provides it as payment for work.

## Asset registry example

Tokens or coins on the blockchain can be used to represent an asset's value digitally. Their value is tied to a real-world promise by the asset issuer. Such tokens are mostly used with digital assets; in this example, a digital image.

The image is not stored on the blockchain. The image's token that contains a reference to the image's ownership deed is stored on blockchain. Once put on the blockchain, everyone in the network agrees on who the asset belongs to.

Alice has a digital picture that she wants to sell using a token. This token permanently stores Alice's ownership of the picture. This token can now be freely traded by sending it to someone else. Bob buys the picture and Alice sends Bob the token. Bob now owns the picture.

## Smart contract example

Smart contracts are pieces of software created to perform actions based on certain inputs, for example to automate the actions in a contract between two parties.

In this example, a smart contract governs a simple wager between Alice and Bob about tomorrow's high temperature. They write a small computer program which encapsulates the details of their wager.

Alice submits a transaction to the blockchain. The smart contract code is inside the transaction's body. At the end of the day tomorrow, the smart contract retrieves the day's high temperature from a weather service.

Bob has won the bet. The contract now automatically pays Bob his winnings, as agreed upon. The contract has now been fulfilled and the smart contract stops running.

# Deloitte.

**www.deloitte.co.uk/blockchain**

Source: Deloitte Advisory Innovation, Deloitte & Touche LLP