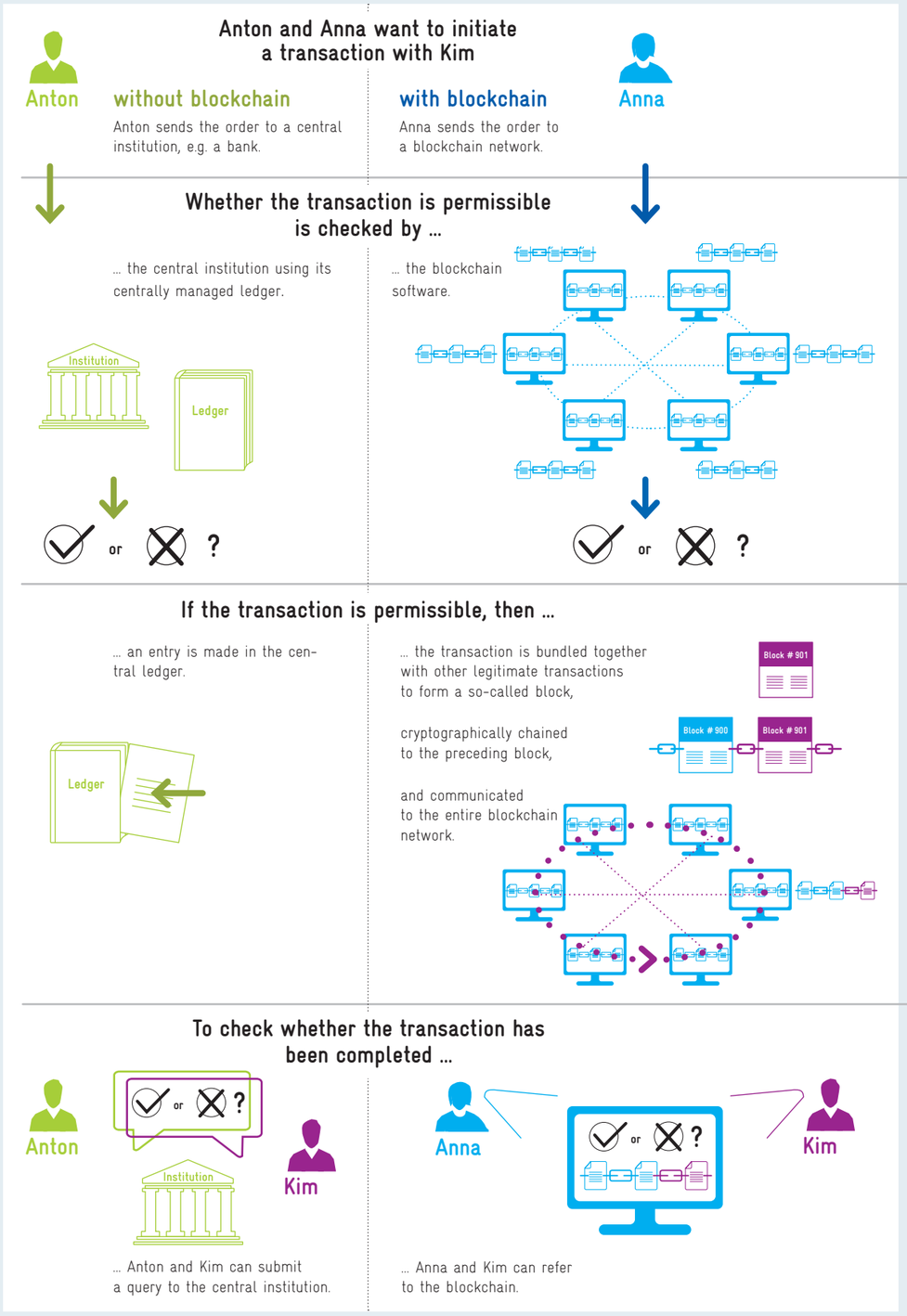
How a transaction works – both with and without blockchain technology



Transaction process

Anton and Anna each agree a transaction with Kim in which Kim is to receive €50. Anna makes the transaction using a blockchain, while Anton uses a central authority such as a bank.

Anton instructs the bank to transfer €50 to Kim. The bank uses its central cash book to check whether the transaction can be permitted. Anna sends the value of €50 via the blockchain. In the blockchain, the participants check whether the transaction is permissible.

The bank executes Anton's transaction, debiting Anton's account with the amount of €50 and crediting €50 to Kim's account. The transaction is recordedin the ledger. Anna's transaction is combined with other transactions in a block, marked with a digital fingerprint (known as a hash) and then communicated to the entire blockchain network. The new block is chained to the previous block by referring to the hash of its predecessor.

To review the transaction with Anton, Kim can check her bank account. To review the transaction with Anna, Kim can check the block with her transaction.

Differences between the transactions

In the case of transactions without blockchain technology, the central institution has to be trusted to carry out the transaction reliably, keep data secure and only use data for the authorized purposes. Such services often incur high fees. When using blockchain technologies, one has to be confident that the blockchain technology works properly.

Blockchain technologies clearly define and state which transactions are permitted. In transactions without blockchain technology, the central institution's conditions of use need to be examined and interpreted to understand which transactions are legitimate. However, the central institution might interpret these conditions differently – and can change them unilaterally.

The computers of the blockchain network have to build a consensus. The necessary consensus mechanisms, however, can consume a lot of energy, as in the case of the Bitcoin blockchain.

Transactions stored in a blockchain cannot be changed at a later date. A central institution, on the other hand, is able to change or delete transactions. In addition, a successful cyber-attack on a central institution can result in its services being unavailable. In a blockchain, the ledger is stored on many different computers, meaning that data remains available even if some computers fail.

Recording a transaction in a central ledger is a quick process that requires few resources. Recording a transaction in a blockchain, on the other hand, requires more resources because the transactions are sent to and stored by all computers in the network. This also requires greater memory capacity.

To inspect the current status of stored transactions, a request has to be sent to the central institution. Blockchain participants can directly access and view the transactions stored in a blockchain.

In addition to transactions, a central institution also stores data about its users, such as their names, passwords and credit card details. While these institutions do have security features in place to protect against theft, various hacks have shown that such provisions do not offer complete security.

Glossary:

A **ledger** records and stores transactions (potentially digitally). A transaction is a sequence of steps that form a logical unit. The nature of transactions can vary considerably – and include tasks such as transferring money from one person to another, posting on social media or sharing information between companies or authorities.

A **central institution** maintains the ledger. As a result, the institution holds sole control over the recording and storing of transactions. Examples of central institutions include banks, legal advisers and social media.

A **network** is composed of computers that are connected and therefore able to exchange information.

A **blockchain** is a digital ledger simultaneously stored on numerous different computers. A blockchain is composed of blocks connected in a chain.

Blocks bundle transactions, similar to a page in a ledger. In addition, each block contains information that connects it to the previous block and thereby renders its content immutable. This renders both the transactions within a block and the sequence of blocks immutable.

Consensus describes a situation in which all computers agree on the correct state of the blockchain and the transactions stored in it.

Consensus mechanisms ensure that the computers form a consensus, even if there might be computers within the network seeking to disrupt it, such as by sending false information.

© EFI – Commission of Experts for Research and Innovation 2019.