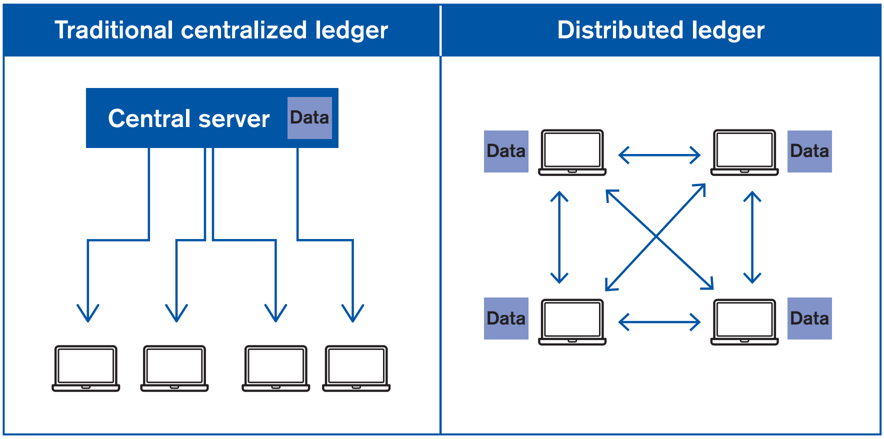
Figure 1 Centralized versus distributed ledger



Source: Author.

Data entered onto the blockchain are "hashed"*, i.e. converted into a new digital string of a fixed length using a mathematical function, and encrypted* to ensure data integrity, prevent forgery, and guarantee that the message was created and sent by the claimed sender and was not altered in transit. If the sender of the transaction does not wish other participants in the network to see the content of the message itself, i.e. the plaintext data contained in the documents submitted, he/she can choose to encrypt the message itself, thereby rendering the data unintelligible to individuals without authorized access.

Once validated, transactions are stored in "blocks" that are then "chained" to each other in chronological order using cryptographic techniques (see the Annex for a description of a typical blockchain transaction).[10] Data, once added to a blockchain, are time-stamped and near-impossible to modify. However, while blockchains can help prevent fraud on the ledger, the tamper-resistance of the technology cannot prevent false information from being fed into the ledger.

In a blockchain, each peer keeps a complete copy of the data (or as close to it as possible), and updates are shared with all participants simultaneously. Participants in a blockchain therefore all have access to the same information at any time. In other words, a blockchain is a shared, trusted ledger that all participants can access and check at any time, but that no single party can control (unless it is fully private – see next section), which allows people with no particular trust in each other to collaborate without relying on trusted intermediaries.

As data are replicated as many times as there are nodes, falsifying data or compromising the whole network would require compromising a large number of