coincide, the receiver has the guarantee that the data were not altered in transit. The transaction can then thus be validated.

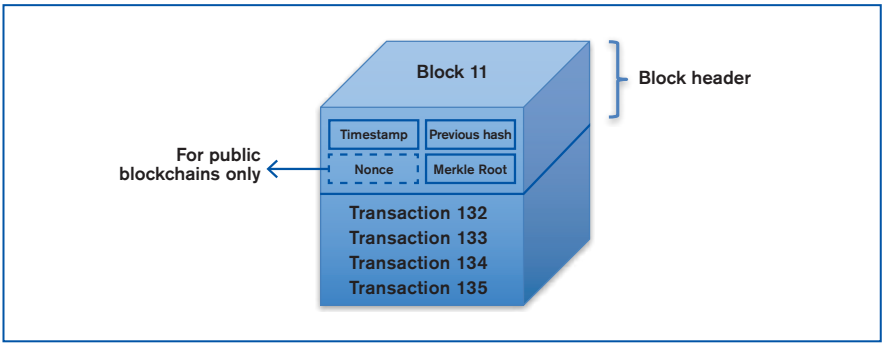
The chain is then updated via the "consensus protocol". Consensus protocols ensure a common, unambiguous ordering of transactions and blocks, and guarantee the integrity and consistency of the blockchain across geographically distributed nodes (see below for a presentation of the most frequently used consensus protocols).

In the case of blockchain technology, validated transactions are first combined with other transactions to create a block that is then validated[2] based on the consensus protocol of the blockchain. If validated, the new block is linked to the chain as the "true state of the ledger". Each block contains several transactions (see Figure A.2). A block is composed of a block header and of records of transactions. The block header contains the following elements:

- The block number.
- The current time-stamp* that captures the date and time to ensure a record of the chronological sequence.
- The hash of the previous block – also referred to as a hash pointer – to link the blocks together.
- The hash of what is called the "Merkle Root"*, which allows easy comparison and verification of large data sets of transactions without the need to include the complete set of data of every transaction in the block header, thereby making the size of blocks more manageable.

In addition, for public blockchains such as Bitcoin, the block header includes the "nonce"* – i.e. a random sequence of numbers that the miners* have to find in order to validate the block and the difficulty target associated with it.

Figure A.2 Composition of a block



Source: Author.