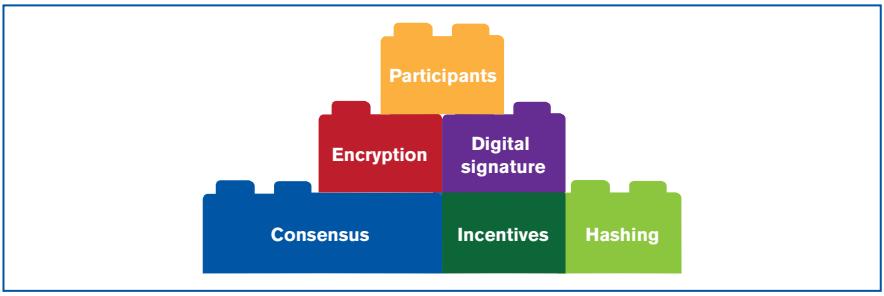
Figure A.4 Blockchain's "building blocks"



Source: Author.

The main breakthrough feature of Blockchain was that it dovetailed the properties of all these technologies and introduced minor, meticulously thought through alterations in the protocols to deliver a higher level of security. Like Lego blocks, different bricks can be taken out of the bag and put together in different ways to create distinctive features (see Figure A.4) (see Lewis, 2015).

Blockchain's immutability – the fact that records cannot easily be changed or deleted after validation – is achieved by leveraging the various properties of hash algorithms and hash pointers. However, instead of just containing the address of the previous block (as in classical protocols), hash pointers in the blockchain contain the hash of the data inside the previous block. As a result, unlike traditional distributed databases, a change in data in one block will cause all the previous blocks to change. This one small tweak is at the heart of Blockchain's immutability. It is what makes Blockchain extremely reliable.

In addition, Blockchain replaces trusted time-stamping with a distributed and tamper-proof alternative. When a block is validated and added to the chain, time-stamping provides a secure proof of the exact time at which those data were added and existed.

Some commonly used consensus protocols

Proof of Work (PoW – Bitcoin)

This consensus protocol is used by Bitcoin and several other public cryptocurrency platforms. Proof of Work requires that the participants that validate blocks – in other words the validators, also called "miners" – show that they have invested significant computing power to solve a hard cryptographic puzzle (a mathematical problem based on the consensus rule). This process is called "mining"*. Miners compete with