Defining BlockchainBefore delving further into the details of the technology, we first define the  
main concepts. Blockchains maintain a ledger and implement a specific kind of  
distributed ledger technology.

**Definition 1 (Distributed Ledger)** A *distributed ledger* is an append-only  
store of transactions which is distributed across many machines.

Being ‘append-only’ is important: new transactions can be added, but old  
transactions cannot be deleted or modified. A new transaction might reverse a  
previous transaction, but both of them remain part of the ledger to allow auditability  
and ensure long-lasting integrity. We define the *concept* of a blockchain as follows.

**Definition 2 (Blockchain)** A *blockchain* is a distributed ledger that is structured into a linked list of *blocks*. Each block contains an ordered set of  
transactions. Typical solutions use cryptographic hashes to secure the link from  
a block to its predecessor.

A graphical representation of this concept is shown in Fig. 1.1. Cryptographic  
hashes ensure that a previous block cannot be changed. If the previous block was  
changed, its new hash would not match the originally recorded hash, so the link  
between the two blocks would break. We explain this mechanism in more detail in  
the next chapter, where we discuss specific blockchain platforms.  
Some ingredients are necessary for the blockchain concept to work in practice as  
a system.

**Definition 3 (Blockchain System)** A *blockchain system* consists of:  
(i) a *blockchain network* of machines, also called *nodes*;  
(ii) a blockchain data structure, for the ledger that is replicated across the  
blockchain network. Nodes that hold a full replica of this ledger are  
referred to as *full nodes*;  
(iii) a network *protocol* that defines rights, responsibilities, and means of  
communication, verification, validation, and consensus across the nodes  
in the network. This includes ensuring authorization and authentication  
of new transactions, mechanisms for appending new blocks, incentive  
mechanisms (if needed), and similar aspects.

For the verification of transactions, consider the example of Alice spending 2  
Bitcoin (BTC), by transferring them to Bob. The system needs to ensure that the  
party initiating the transaction has Alice’s authority and that Alice has the 2 Bitcoin  
available.  
The above definition is still relatively broad and can capture blockchains of  
various sizes, degrees of openness, for various purposes, etc. The most well-known  
blockchains are Bitcoin and Ethereum, which are *public blockchains*.

**Definition 4 (Public Blockchain)** A public blockchain is a blockchain system  
that has the following characteristics:  
(i) it has an *open network* where nodes can join and leave as they please  
without requiring permission from anyone;  
(ii) all full nodes in the network can *verify* each new piece of data added to the  
data structure, including blocks, transactions, and effects of transactions;  
and  
(iii) its protocol includes an *incentive mechanism* that aims to ensure the correct operation of the blockchain system including that valid transactions  
are processed and included in the ledger and that invalid transactions are  
rejected.

Public blockchains are often open leaderless peer-to-peer systems that manage  
the ownership of assets of value. Examples of such assets on Bitcoin and Ethereum  
blockchains are Bitcoin (BTC) and Ether (ETH) cryptocurrencies and digital tokens.  
In a public blockchain, there is not a high degree of trust in information from other  
nodes. Therefore, all full nodes verify everything, to reduce the risk of integrity  
violations jeopardizing the value of their own work. While this leads to redundant  
computation across the network, it is a direct consequence of the community of  
nodes collectively safeguarding the integrity of the blockchain.

In other settings, for example, within a large enterprise or in a consortium  
of companies, all blockchain nodes might be known and governed by other  
organizational or contractual mechanisms. These applications can be served by  
adopting a more relaxed trust assumption.  
Finally, we define the term blockchain platform, which refers to the software  
used to run a blockchain.

**Definition 5 (Blockchain Platform)** A *blockchain platform* is the technology  
needed to operate a blockchain. This comprises the blockchain client software  
for processing nodes, the local data store for nodes, and any alternative clients  
to access the blockchain network.  
Note that any blockchain platform must have client software with which  
processing nodes can operate the network, including for transaction propagation and  
block creation. Light clients may additionally exist, e.g. to enable mobile devices to  
read and write transactions to the network; these typically do not hold a full copy  
of the blockchain data structure. Alternative clients, both for processing and light  
nodes, may exist, particularly if the protocol is specifield well

Smart Contracts and Decentralized ApplicationsThe transactions stored on a blockchain can be more than simple records of the  
exchange of assets—emerging blockchain systems also allow computer programs  
to be stored and to execute as part of transactions on the ledger. These are often  
called ‘smart contracts’, although the programs are typically not very smart and are  
often not related to legal contracts

**Definition 6 (Smart Contract)** *Smart contracts* are programs deployed as  
data in the blockchain ledger and executed in transactions on the blockchain.  
Smart contracts can hold and transfer digital assets managed by the blockchain  
and can invoke other smart contracts stored on the blockchain. Smart contract  
code is deterministic and immutable once deployed.

***Cryptocurrencies and Tokens***Cryptocurrencies are the base currencies of blockchains. *Ether* is the currency  
of the public Ethereum blockchain, and Bitcoin is the currency of the public  
Bitcoin blockchain (thereby highlighting a source of confusion due to overloaded  
terminology). The respective blockchain keeps track of the ownership of portions  
of that currency. Say, Alice owns 2 Ether and announces a transaction to transfer  
1 Ether to Bob, offering a fee of 0.01 Ether. Once the transaction is included in a  
block mined by Charly, Alice has 0.99 Ether, Bob has 1, and Charly received the fee  
of 0.01 Ether. The sum of the money is not changed by these transactions, but the  
ownership of portions of it is.  
Fees for transaction inclusion are paid in the base currency of a blockchain,  
although the client can choose to offer a fee of 0 (typically reducing the speed  
and/or likelihood of inclusion). Fees often relate to the *size* of a transaction, not  
its *value*: more data (including larger smart contracts to be deployed) incur higher  
fees. Similarly, more complex computations as a result of smart contract invocations  
incur higher fees. Transfers of 0.01 Ether incur the same fees as transfers of 100  
Ether.  
Digital *tokens* can be created and exchanged on blockchains. Usually tokens are  
created using smart contracts. Similar to a cryptocurrency, each token is controlled  
by an actor on the blockchain. Tokens might represent shares in a company, the right  
to benefit from future earnings, or perhaps virtual gold in an online game. The use  
of tokens has become widespread, and tokens can be seen as the first ‘killer app’ of  
using blockchain for things other than cryptocurrency