# A Simple Blockchain Documentation

Flavien Chamay

February 19, 2021

## 1 A Little Theory on the blockchain technology

A blockchain is a distributed data storage composed of containers which are connected.

### 1.1 The Blocks

A container is represented by a block that can contain any type of data (In the case of a cryptocurrency, the data is a list of transactions). In a blockchain, the order of each block matters and each block know something about each other (via a hash).

### 1.2 The Hash

A hash is a string of text corresponding to a bunch of data. When you hash a data, it generates that string that uniquely identifies the data (for the same input you get the same hash). In a blockchain, each block has a hash that uniquely identifies it. Also, each block (except the first one) stores the hash of the previous block. The security mechanism of a blockchain appears when you change the previous blocks, the last block (with the true hash) will detect that the hash that it stores doesn't match the hash of the hacked previous blocks.

### 1.3 The Transactions

Three informations are necessary to define a transaction: the sender, the recipient and the amount. Each block contains a nested list of transactions. This nested list contains the transactions for the current block and the nested list of all of previous blocks.

### 1.4 The Mining

Coins are created via mining. It is a result of the effort (a reward) in creating new coins. It is also how new blocks are added to the end of the blockchain. For a new transaction to be confirmed, it needs to be added into a new block in the blockchain. This process is supposed to take time and needs to solve complex algorithms but, for this project, we simplified this process without implementing this complex algorithm. Instead, we simply implemented a button (in the frontend) when clicked it generates 10 coins to the properitary of the wallet.

### 1.5 The Node

A node is simply a machine hosting the whole blockchain. Nodes are broadcasting the blockchain to all their neighbors (via a consensus) and are also broadcasting the transactions of each wallet. After a bunch of transactions have been completed, one node will bundle them up in a newly generated block (via mining). After an update of the blockchain, this node broadcast the updated blockchain according to the consensus.

### 1.6 The Wallet

For simplification in this project, we will say that a wallet is a node that has an adress for receiving or sending coins. This wallet is capable of identifying its holder.

### 1.7 The cryptocurrency

A cryptocurrency is based on the blockchain theory to operate. The coins transferred via the transactions form the cryptocurrency. Inside the blockchain, it is not possible to change coins into other currencies. Only via a platform (Coinbase, Binance, ...) you can exchange the coins into fiat currency. And the worth of each coin is what people think it is. Because this technology is new, the volatility is very high, we have not properly assessed the true value of this technology.

### 1.8 Verification of the blockchain

The security mechanisme on which the blockchain is based is, when the whole chain is ongoing verification, if the list of transactions of one block is changed then the next block will detect the forgery and the whole blockchain will be rejected. To ensure this mechanism we use the hash of each block. Each block contains a hash that identifies uniquely the data of its previous block.

### 1.9 The Proof of Work

The proof of work is another security mechanism for the blockchain. The equality of a hash from a block to its next one is not enough to secure the blockchain. If an attacker edits the transactions stored in a block and then also updates the blocks after it (and therefore the rest of the chain). The resulted blockchain after validation will be considered valid. The proof of work solves that issue. The proof of work is simply a number (also referred to as "Nonce"). For this project, we use simply the string ’00’ and concatenate it at the beginning of our hash.

### 1.10 The Consensus

## 2 Implementation of the blockchain in Python