

February 11, 2021

## **1 A Little Theory on the blockchain technology**

### **1.1 The Blocks**

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

### **1.2 Verification of the blockchain**

### **1.3 The Transactions**

### **1.4 The Consensus**

## **2 Implementation of the blockchain**