Markle Root Tree

Dr. Preeti Chandrakar
Assistant Professor
Department of Computer Science & Engineering

Contents

- Introduction
- Merkle Hash function
- Basics - Cryptographic Hash
- Merkle Tree
- Merkle Root In Header

Introduction

- **Markle tree is introduced by the Ralph Markle in 1979**
  - As **classic** cryptographic construction
  - **It involves combination of hash functions in binary tree structure**
- **It is an efficient Data Structure for many applications**

Markle Tree Data Structure

- Binary tree nodes are assigned (160 Bits) values
-

Interior Nodes $v=Hash(V_{left}||V_{right})$

Leaves $V_i = Hash(s_i)$

Secret Si

Computing Tree and Root Hash

-

Complexity Analysis

-

Authenticating A Secret

•

Merkle Hash Function

- Ensures Authenticity of the document as well as the schema
- Associate a hash value with each node in the graph representation
- The hash value of a node is obtained by applying a hash function over the concatenation of its children
- The hash values are computed using the Merkle Hash Function

Merkle Hash Function

Example : Alice and Bob

- Bob stores a set of items for Alice
- Alice keeps a single value
- Alice can validate the Items returned to her

First Solution

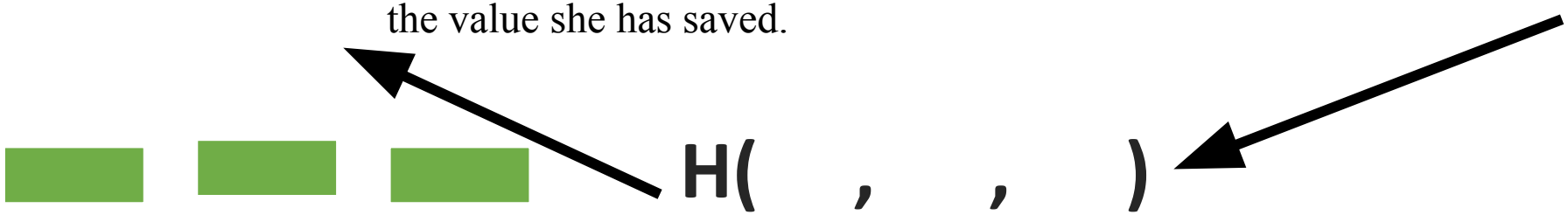
- Alice keeps the hash of the entire set

Validation Of An Item

Bob sends all of the items to Alice

Alice computes the
hash of the items

Alice compares the result to
the value she has saved.



Problems With First Solution

- Bob must send Alice the entire set for validation

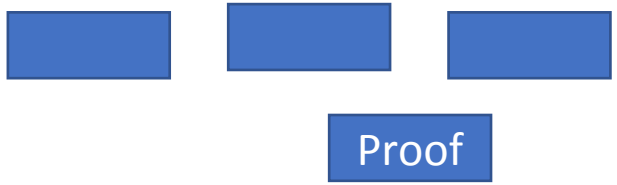
OK

Problems With First Solution

OK

- Bob must send Alice the entire set for validation
- Denote m to be the size of the set
- We have O(m) network traffic for validating a single item.
- Can we do better?

Validating An Item



Bob sends Alice an item d and a logarithmic size proof

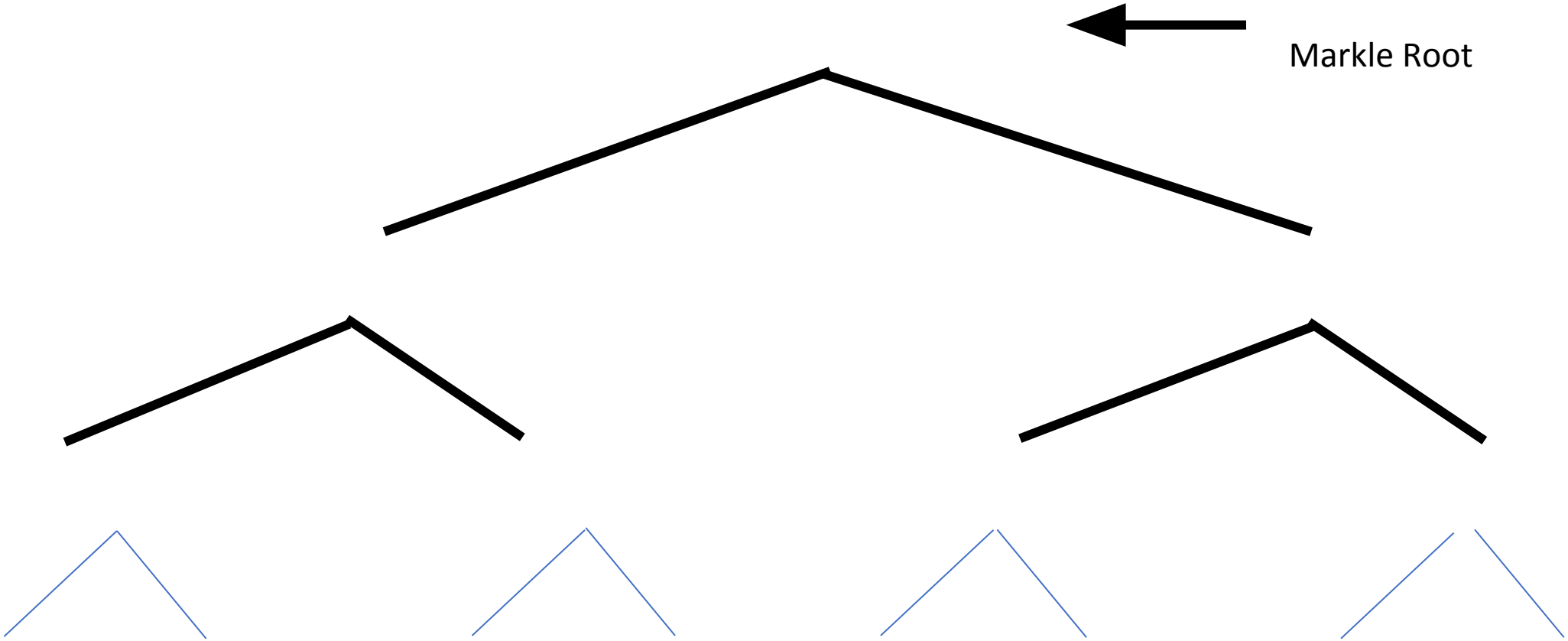
Alice computes a function of
the item and proof

Alice compares the result to
the value she has saved

Cfcdhgasv57654738390/……..

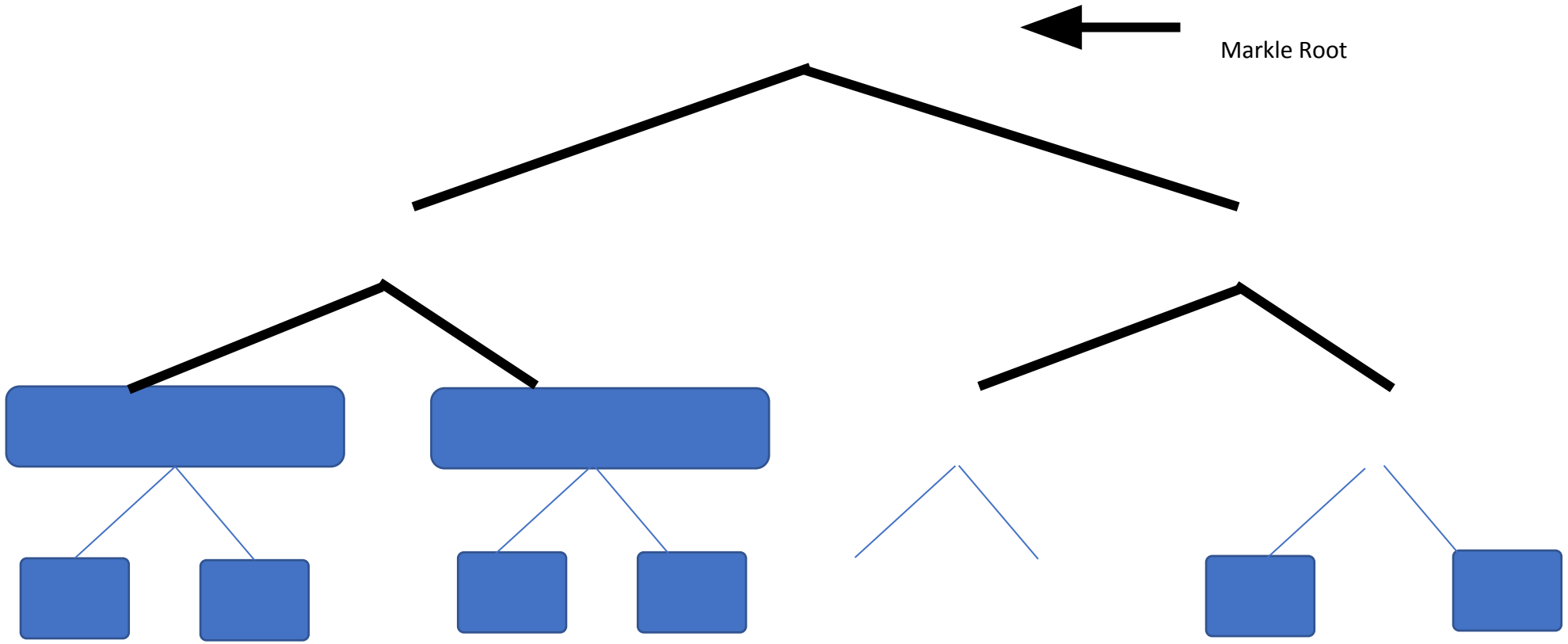
F(, ,)

Markle Tree



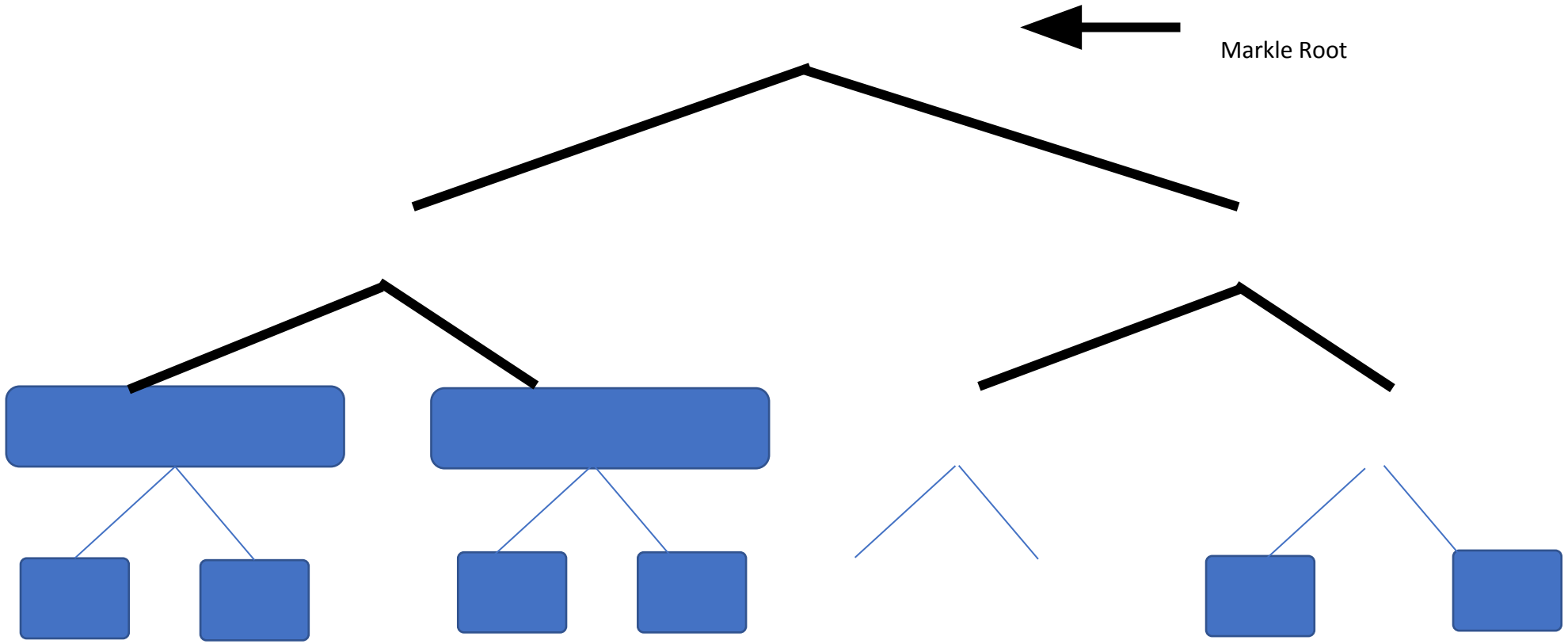
Alice Computes The Root

Given an item d and H1,H2,H3 hash values

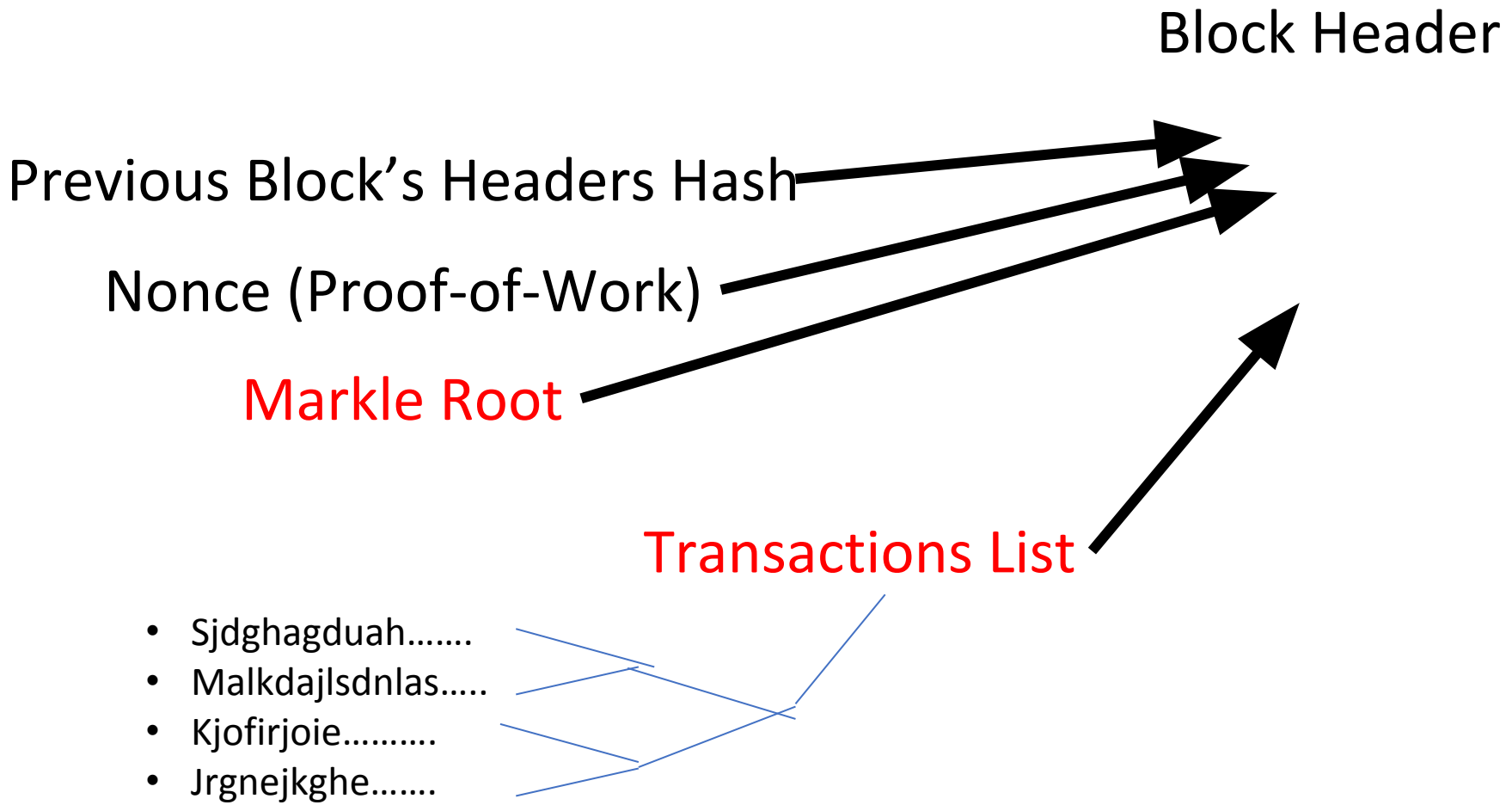


What if d is not valid

Given an item d and H1,H2,H3 hash values



Merkle Root In Header



Advantages of Markle Root in Blockchain

- Merkle trees are a smart way to hash.
- They allow for easier storage of Blockchains, allowing headers to represent the entire block in a concise way.
- They even allows us to forget the transaction IDs of spent transactions.

Questions