

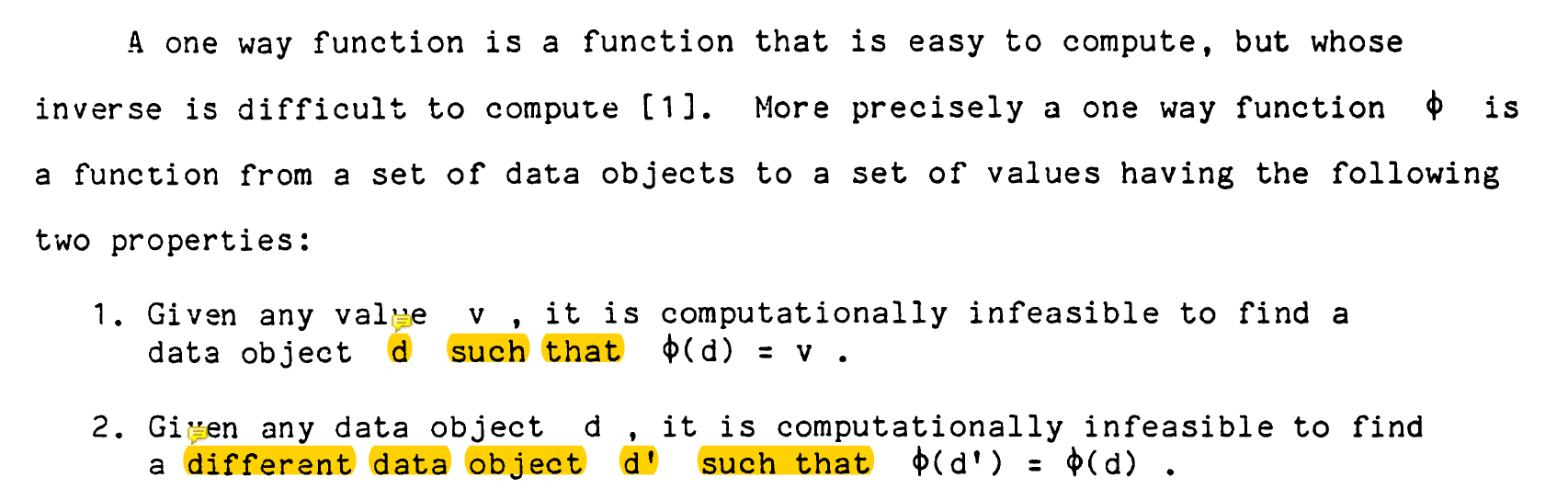
Merkle-Trees

jae Duk Seo

Jae Duk Seo | March 10, 2017

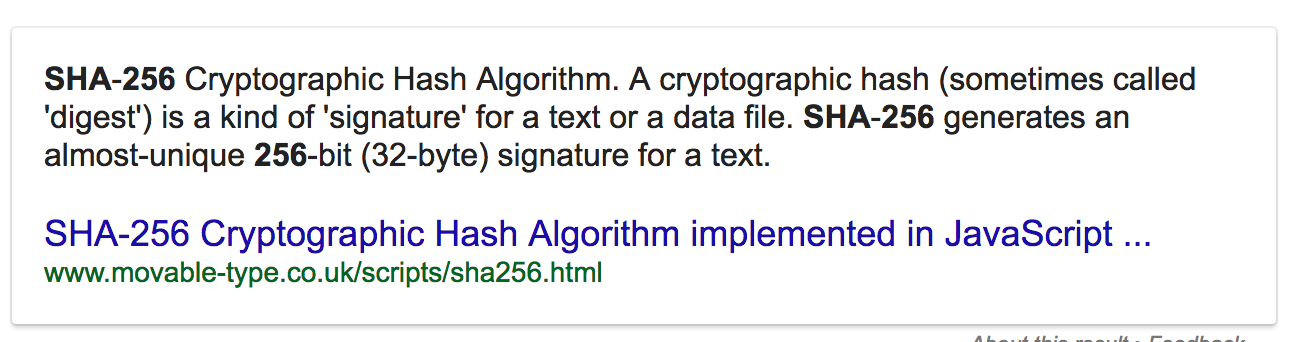
# What is a one-way function?

* Hash function is a one-way function that follow this property.

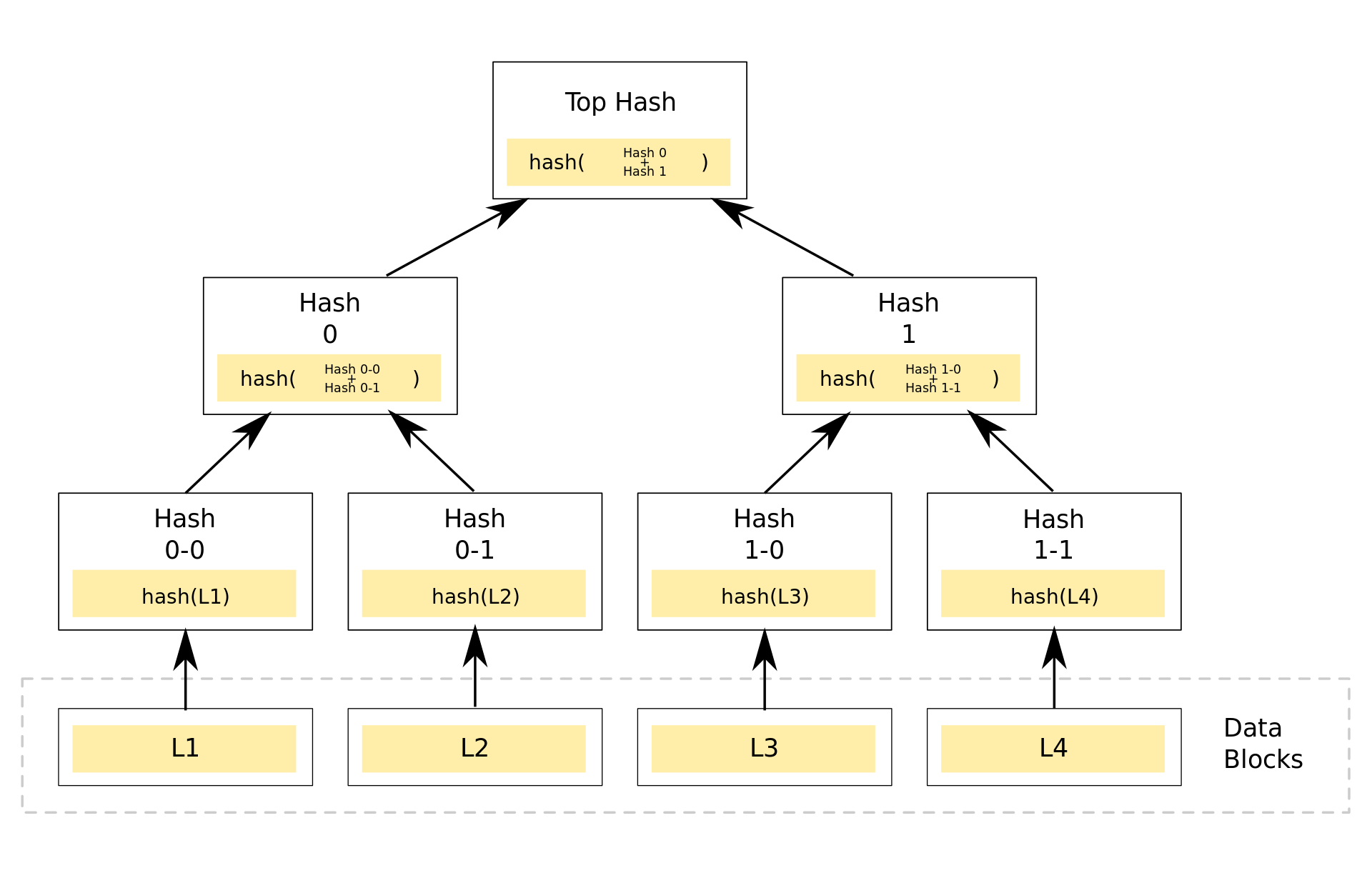


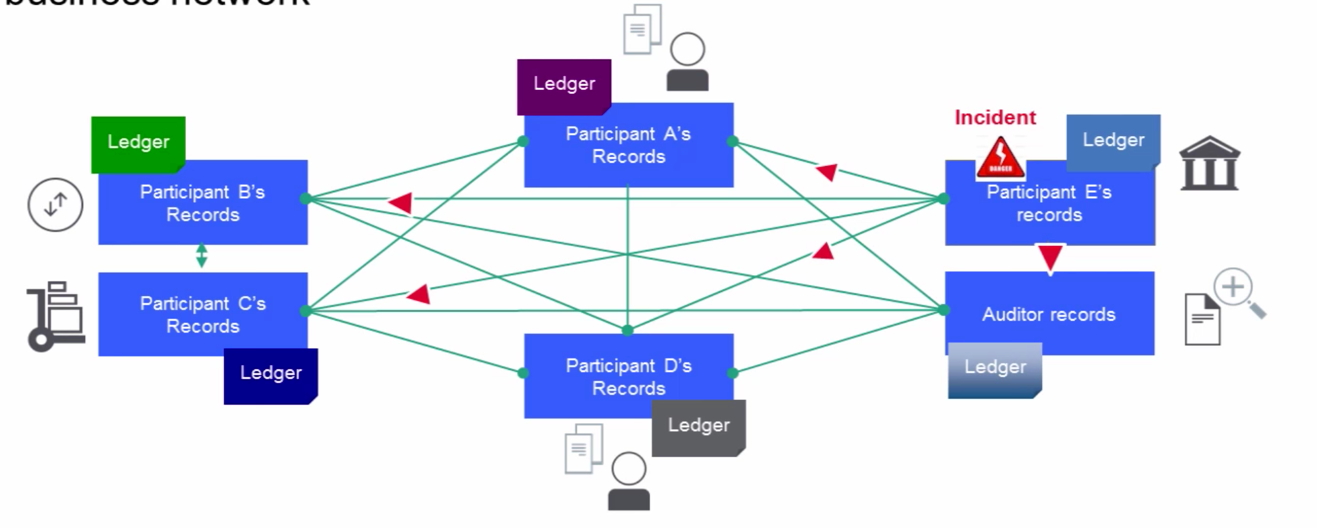
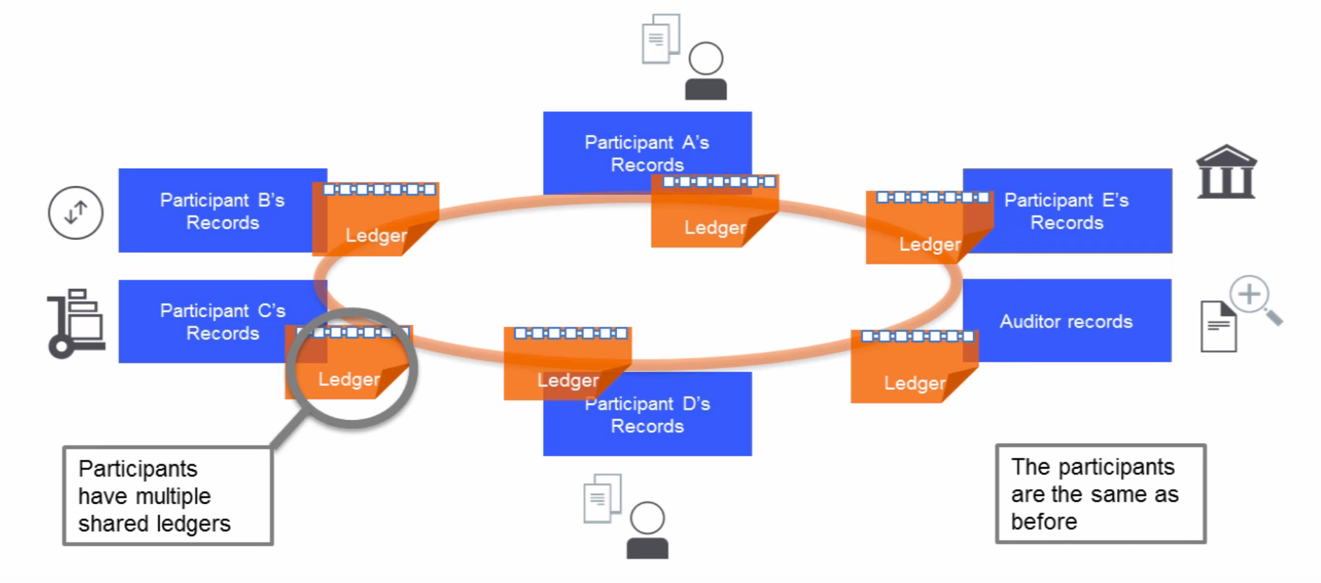
* 1. One unique input for one unique output   
  f(4) = abcd then f(3) or f(2) cannot be abcd
* 2. We cannot find the input value from the output value  
  g(abcd) = 4 <- this must not be possible!
* Source: https://pdfs.semanticscholar.org/707e/f01face0af32949eda250f2ec497a64d4231.pdf

# What is a SHA-256 hash function?

* It is the one-way hash function that ‘almost-unique’ value. But for simplicity we will considered it as 100% unique.  
  
* Example output: Since we are using Hexadecimal we need 64 digits../Desktop/Screen%20Shot%202017-03-10%20at%206.25.22%20PM.png

# What is a Merkle Tree?



* Source: <https://brilliant.org/wiki/merkle-tree/>
* In my words: A **binary tree** where, **all the leaf nodes** are data and all the **non-leaf nodes** are **combined hash results** from its two children.
* Use case: Transaction data, from company A,B, and C.
* Traditional way of keeping transaction  
  
* Using Merkle Tree a.k.a Block Chain  
  
* Source: <https://www.youtube.com/watch?v=obA0InYr0VA>

# Actual output of BlockChain

