NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural

Department of Computer Science & Engineering

Indian Institute of Technology Kharagpur

Lecture 05: Basic Cryptographic Primitives - III

CONCEPTS COVERED

- Cryptographic Hash Functions
- Hash Pointers
- Hashchain
- Construction of Chain of Blocks

KEYWORDS

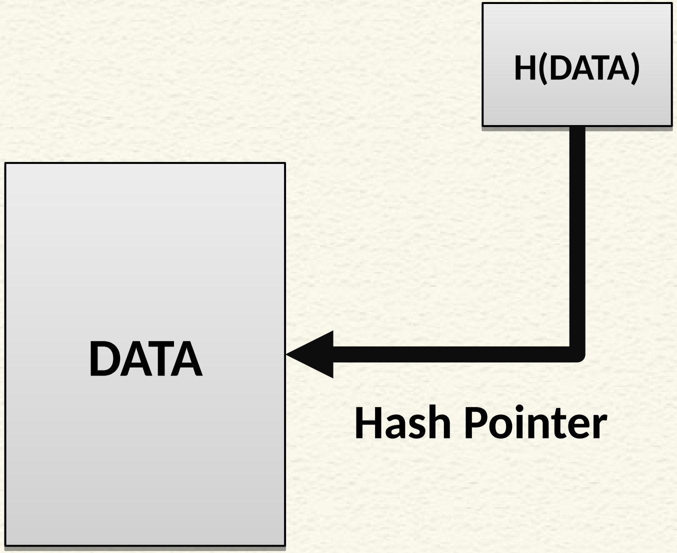
- Hash Function
- Hash Pointer
- Merkle Tree
- Blocks

Hash Pointer

- A **Cryptographic Hash Pointer** (Often called Hash Reference) is a pointer to a location where
  - Some information is stored
  - **Hash of the information is stored**

- With the hash pointer, we can
  - Retrieve the information
  - Check that the information has not been modified (**by computing the message digest and then matching the digest with the stored hash value**)

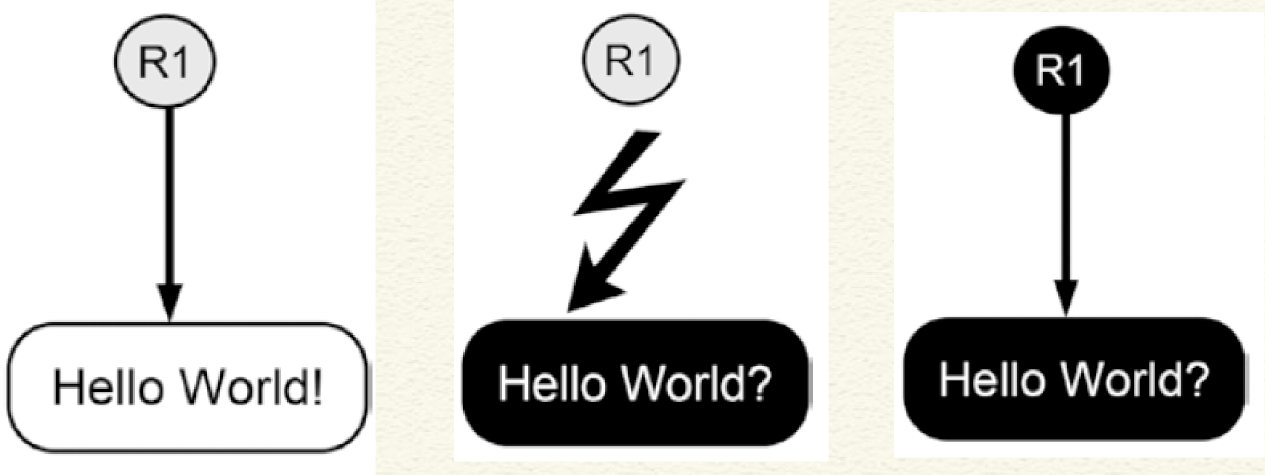
Hash Pointer



Reminds you of a linked list??

Reference: Coursera course on Bitcoin and Cryptocurrency Technologies

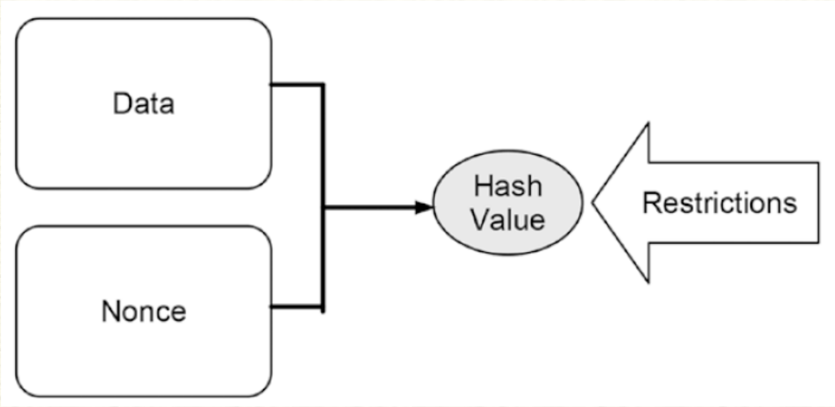
Tamper Detection using Hash Pointer

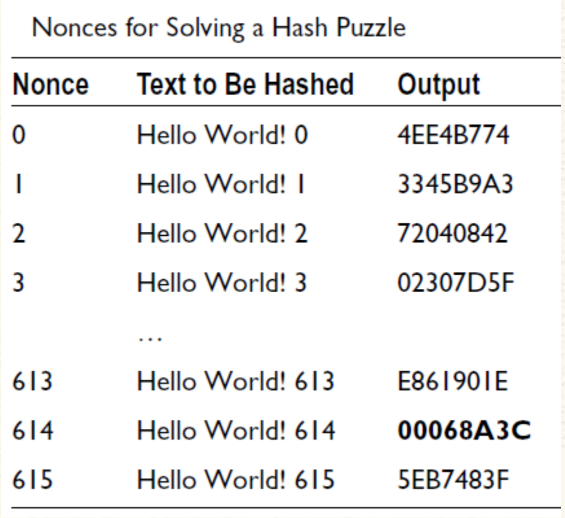


Analogies in real life??

Courtesy: Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher

Making Tampering a Hash Chain Computationally Challenging





Nonces for Solving a Hash Puzzle

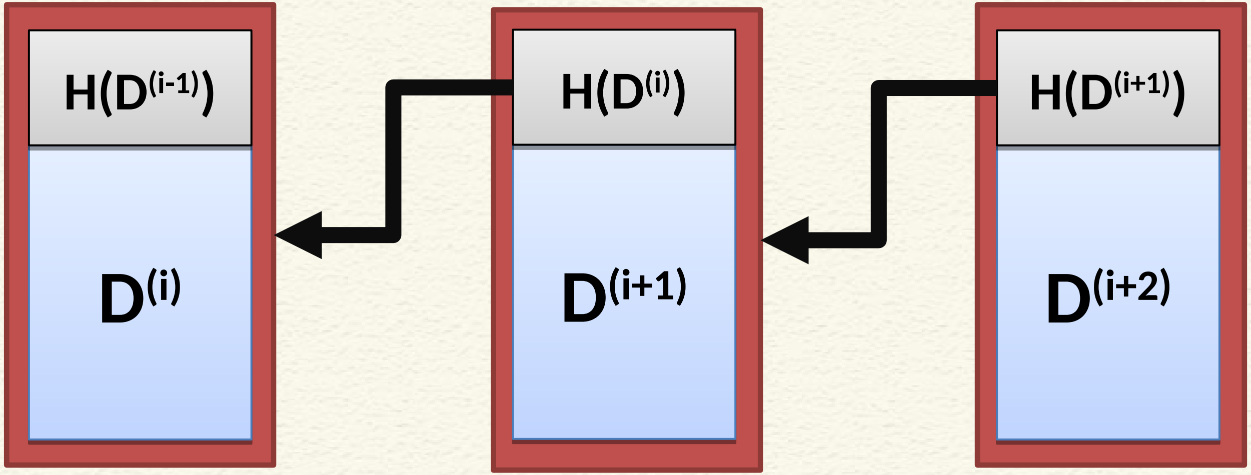
Nonce	Text to Be Hashed	Output
0	Hello World! 0	4EE4B774
1	Hello World! 1	3345B9A3
2	Hello World! 2	72040842
3	Hello World! 3	02307D5F
	…	
613	Hello World! 613	E861901E
614	Hello World! 614	**00068A3C**
615	Hello World! 615	5EB7483F

Illustration

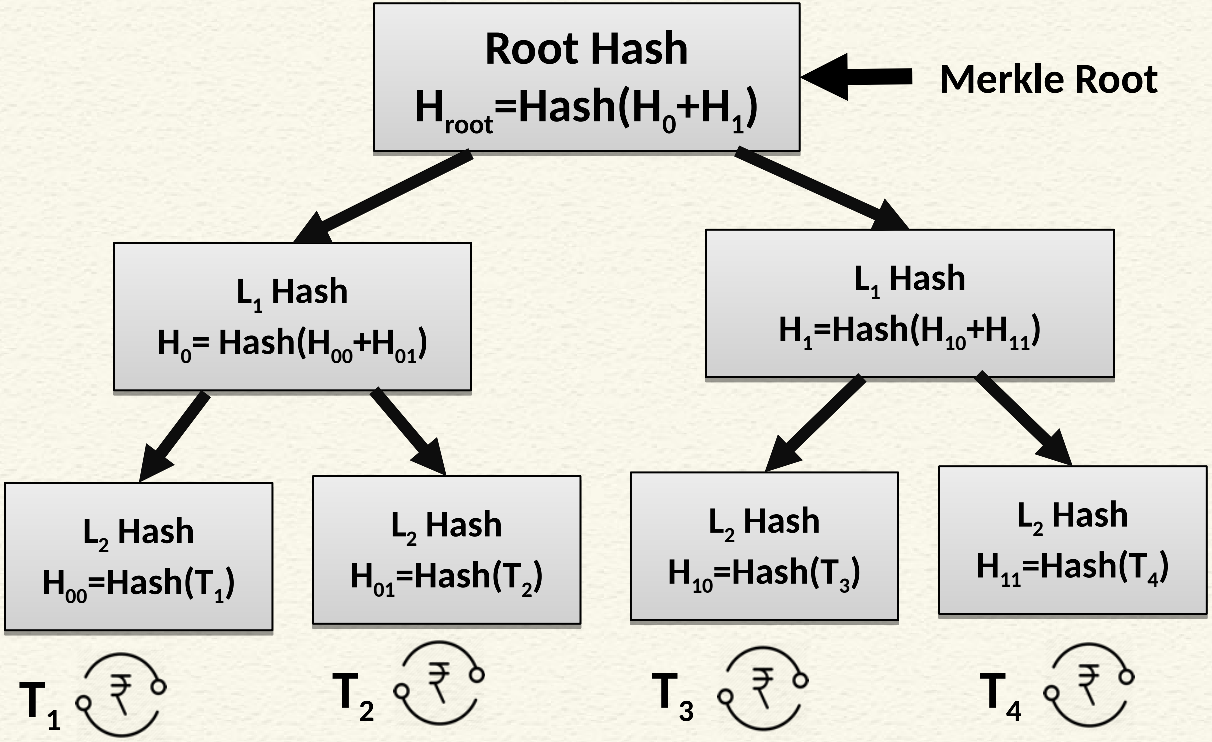
http://www.blockchain-basics.com/HashFunctions.html

Courtesy: Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher

Detect Tampering from Hash Pointers - Hashchain



Merkle Tree – Organization of Hash Pointers in a Tree



Root Hash

H_{root}=Hash(H_0+H_1)

Merkle Root

L_1 Hash

H_0= Hash(H_{00}+H_{01})

L_1 Hash

H_1=Hash(H_{10}+H_{11})

L_2 Hash

H_{00}=Hash(T_1)

L_2 Hash

H_{01}=Hash(T_2)

L_2 Hash

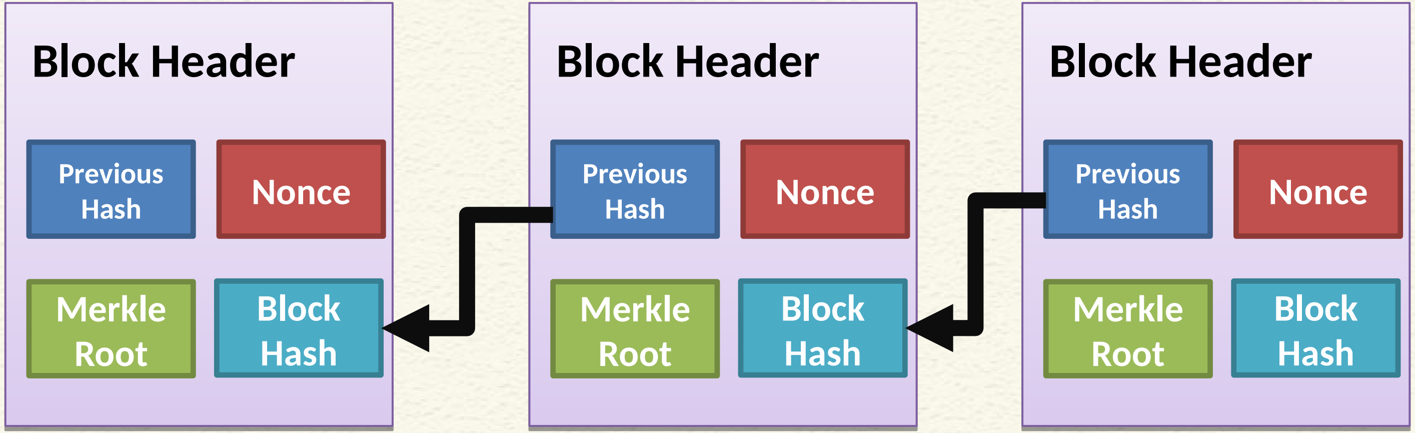
H_{10}=Hash(T_3)

L_2 Hash

H_{11}=Hash(T_4)

T_1 T_2 T_3 T_4

Blockchain as a Hashchain



CONCLUSIONS

- We have discussed the basic concepts of hash pointers
- Seen how it makes data tamperproof
- Construction of hashchain
- Merkle Tree definition
- Formation of a chain of blocks

REFERENCES

- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Cryptography and Network Security – Principles and Practice by William Stallings, Pearson (2017)

Thank you