NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty
Department of Computer Science & Engineering

Lecture 01: The Model of Decentralization

CONCEPTS COVERED

- The Blockchain Myths
- Decentralization – A Use-case

KEYWORDS

- Cryptocurrency
- Blockchain
- Supply Chain Management
- Decentralization

The Blockchain Myth

- Blockchain ≠ Bitcoin (or any other cryptocurrencies)
  - If you want to take this course to trade cryptocurrencies, this course is not for you !!
  - We do not want to argue on the legal issues of cryptocurrencies -- We want to learn the technology and its applications

The Blockchain Myth

- Anything and everything in the world cannot be solved using a blockchain
  - Blockchain is good but it cannot change the society in a week or a month or a year
  - *"Want to prevent fraud and corruption? Use Blockchain"* -- **Unfortunately, you are wrong! There can be a better technology to solve your problem ...**

The Blockchain Myth

- You cannot replace a database with a blockchain
  - Blockchain is **not a distributed database**
  - Blockchain is not designed to securely store ANY data

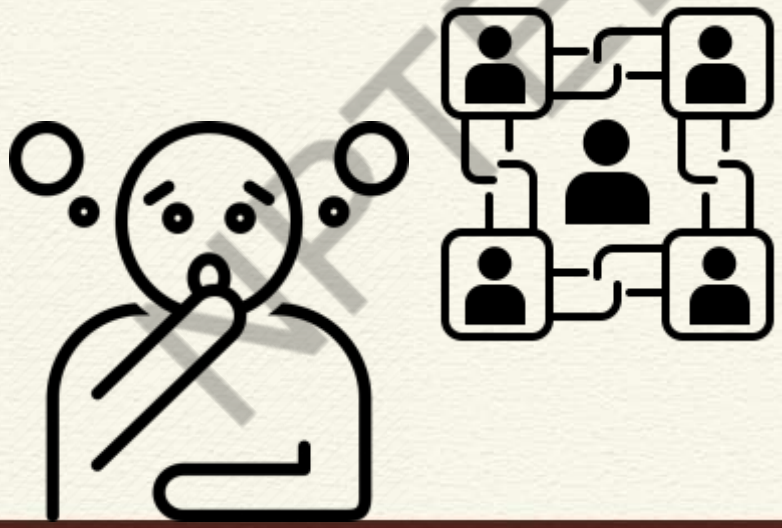
Why this course ...

- To avoid all the hypes and apply Blockchain as a solution at the right place ...

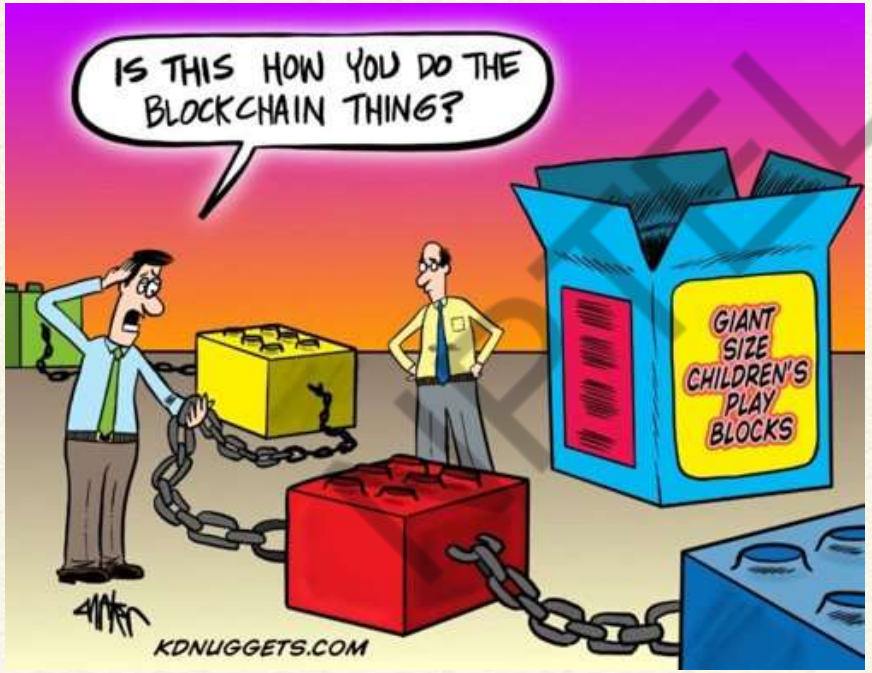
Why this course ...

- To avoid all the hypes and apply Blockchain as a solution at the right place ...

So, what is the right place?



Decentralization – When Do you Need It?



Supply Chain Management -- A Use Case

Supply Chain in Petroleum Industry

Crude Purchase

Supply Chain in Petroleum Industry

Crude Purchase

Crude Transportation

Supply Chain in Petroleum Industry

Crude Purchase

Crude Transportation

Crude Storage

Supply Chain in Petroleum Industry

Crude Purchase

Crude Transportation

Crude Storage

Refining

Supply Chain in Petroleum Industry

Crude Purchase

Crude Transportation

Crude Storage

Refining

Distribution

Supply Chain in Petroleum Industry

Crude Purchase

Crude Transportation

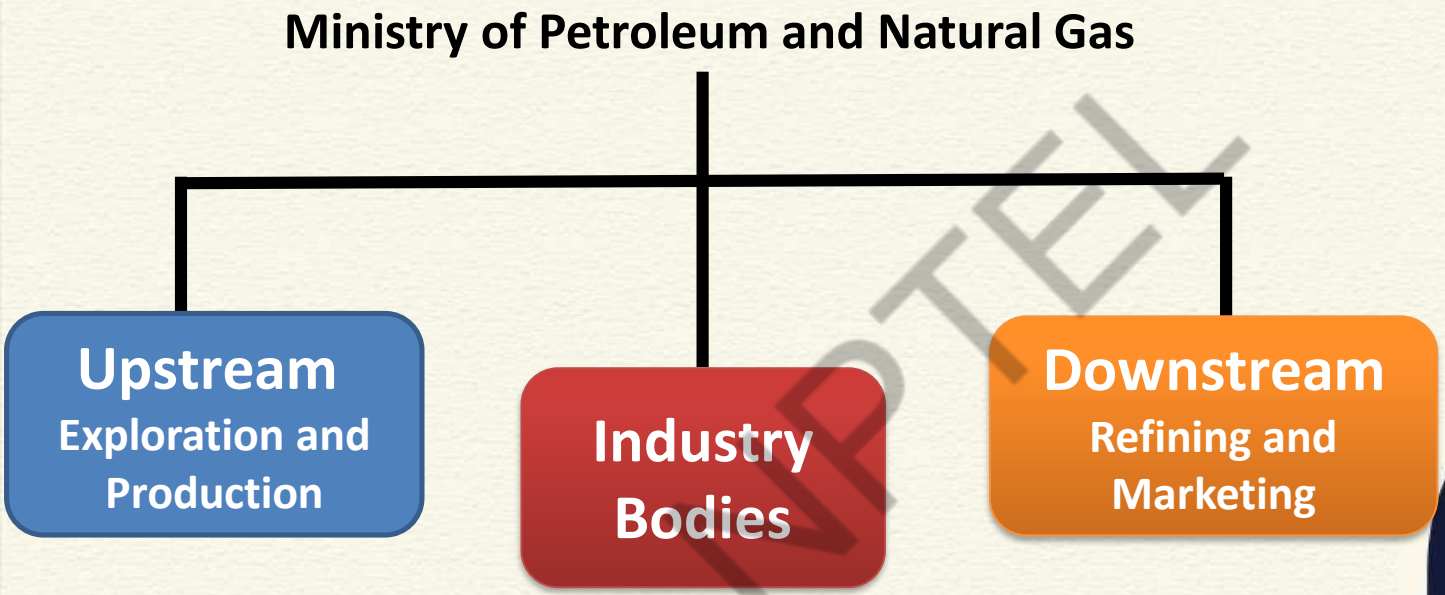
Crude Storage

Refining

Distribution

Retail

Petroleum Supply Chain in India



Petroleum Supply Chain in India

Upstream
Exploration and Production

- ONGC
- OVL
- Oil India Ltd
- Pvt E&P Co

Petroleum Supply Chain in India

Downstream
Refining and Marketing

Indian Oil	Bharat Petr.
CPCL, BRPL	NRL
Reliance Ind. Ltd	Hindustan Petr.
	MRPL

Petroleum Supply Chain in India

Industry Bodies

- Petroleum Planning and Analysis Cell
- Center for High Technology
- PRCA
- PetroFed
- Oil industry Safety Directorate
- Petroleum India International

Requirements for a Successful Supply Chain

- Minimization of material procurement
- Maximization of manufacturing capacity and sales
- Meet demand numbers
- Respond quickly to market opportunity by purchasing the production shortfall from other players
- Objective of each production unit would be to maximize the throughput and its margin
- Procurement would purchase the feedstock with not the best yields at lowest cost

Requirements for a Successful Supply Chain

- Minimization of material procurement





Needs Strong Coordination among the Players

- Procurement would purchase the feedstock with not the best yields at lowest cost

Requirements for a Successful Supply Chain

- Minimization of material procurement





How do we obtain Real-time Information from the Stakeholders?

- Procurement would purchase the feedstock with not the best yields at lowest cost

Requirements for a Successful Supply Chain

- Minimization of material procurement





How do we obtain Real-time Information from the Stakeholders?

A web-based portal?

Requirements for a Successful Supply Chain

- Minimization of material procurement





How do we obtain Real-time Information from the Stakeholders?

What is the guarantee that the information submitted is correct?

Requirements for a Successful Supply Chain

- Minimization of material procurement





How do we obtain Real-time Information from the Stakeholders?

What is the guarantee that the information submitted is correct?

What if someone denies the information later on?

Requirements for a Successful Supply Chain

- Minimization of material procurement





How do we obtain Real-time Information from the Stakeholders?

We need a decentralized solution – Noone trust each other, but they should cooperate

Requirements for a Successful Supply Chain

- Minimization of material procurement





Blockchain is the answer !!

Conclusion – Decentralization and Blockchain

- You have a network of different players (businesses, enterprises, commercial establishments, Government or Private bodies, or even the individuals)
- Everyone has their own interest – they want to fulfill their goal
- They do not trust each other
- If they cooperate, the society gets benefited
- **Trustless Decentralization = Blockchain**

NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty
Department of Computer Science & Engineering

Lecture 02: What is Blockchain

CONCEPTS COVERED

- Decentralization with a Blockchain
- Fundamental Properties of Blockchain
- Formal Definition of a Blockchain

KEYWORDS

- Decentralization
- Properties
- Definition

Requirements for a Successful Supply Chain

- Minimization of material procurement





Needs Strong Coordination among the Players

- Procurement would purchase the feedstock with not the best yields at lowest cost

Moving towards Decentralization ...

Moving towards Decentralization ...

Moving towards Decentralization ...

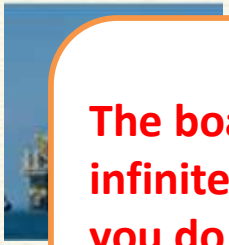
- 120432 barrels produced at Mumbai High on Dec 26, 2020

Moving towards Decentralization ...

- 120432 barrels produced at Mumbai High on Dec 26, 2020

- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

Moving towards Decentralization ...



The board has infinite space, you do not need to erase anything!

- 120432 barrels produced at Mumbai High on Dec 26, 2020

- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

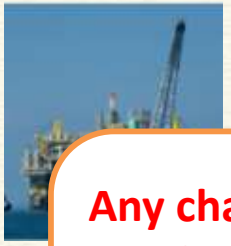
Moving towards Decentralization ...

Everyone can see all the logs and verify

- 120432 barrels produced at Mumbai High on Dec 26, 2020

- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

Moving towards Decentralization ...

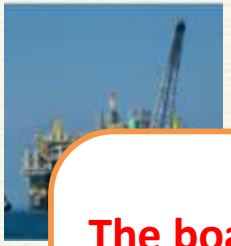


Any change in information is visible to everyone

- 120432 barrels produced at Mumbai High on Dec 26, 2020

- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

Moving towards Decentralization ...



The board is not erasable, no one can deny later

- 120432 barrels produced at Mumbai High on Dec 26, 2020

- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

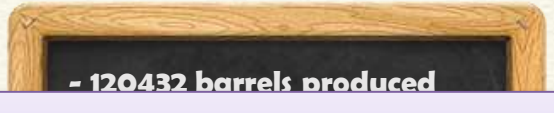
Moving towards Decentralization ...

Simple one-step auditing

- 120432 barrels produced at Mumbai High on Dec 26, 2020

- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

Moving towards Decentralization ...



Who will maintain this bulletin board?

Moving towards Decentralization ...

Who will maintain this bulletin board?

- Buy Cloud from amazon

Moving towards Decentralization ...

Who will maintain this bulletin board?

- Buy Cloud from amazon

Who will manage it and provide the cost?

Moving towards Decentralization ...

Who will maintain this bulletin board?

- One of the enterprises maintain a private cloud

Moving towards Decentralization ...

Who will maintain this bulletin board?

- One of the enterprises maintain a private cloud

What is the guarantee that it is not a fraud?

Moving towards Decentralization ...

Who will maintain this bulletin board?

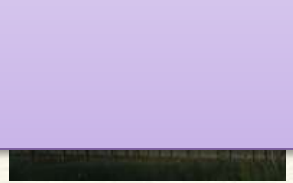
Let everyone maintain the same copy of the board individually and independently

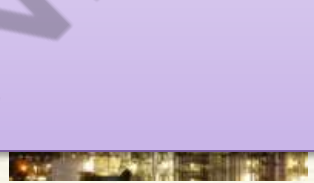
Moving towards Decentralization ...

Who will maintain this bulletin board?

Let everyone maintain the same copy of the board individually and independently

BUT HOW?





Moving towards Decentralization ...

- 120432 barrels produced at Mumbai High on Dec 26, 2020

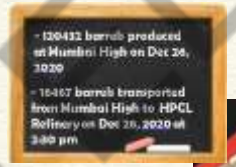
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

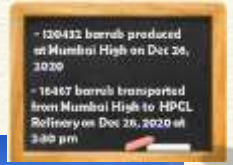
Moving towards Decentralization ...

- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm

Moving towards Decentralization ...

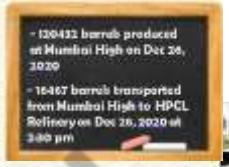
No one is the sole-owner of the data, but everyone has a copy of the data - there is no central database

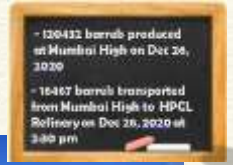




Moving towards Decentralization ...

Everyone holds exactly the same copy of the data at the same instance of the time



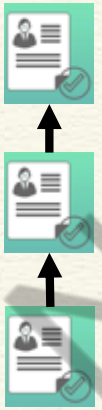


What is a Blockchain?

An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later

What is a Blockchain?

There is no central database to store the chain – everyone keeps a copy of the chain and process data locally



What is a Blockchain?

New information is added to the chain in the form of new blocks

What is a Blockchain?

Blockchain ensures that every party has the same view of the blockchain always

What is a Blockchain?

The Information is transparent to everyone – so everyone can verify and validate

Conclusion: Formally Defining a Blockchain

A decentralized immutable append-only public ledger

Conclusion

- We got a broad idea of a blockchain and its possible use cases (beyond cryptocurrencies)
- We next learn some fundamental cryptographic techniques used in the design of a blockchain ...

NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 03: Basic Cryptographic Primitives - I

CONCEPTS COVERED

- Cryptographic Primitives useful for Blockchain
- Hash Functions

KEYWORDS

- Hash Function
- SHA-256
- Puzzle Friendly

What You'll Learn

- Basic cryptographic primitives behind blockchain technology
  - **Cryptographically Secure Hash Functions**
  - **Digital Signature**
- **Hash Function:** Used to connect the "blocks" in a "chain" in a tamper-proof way
- **Digital Signature:** Digitally sign the data so that no one can "deny" about their own activities. Also, others can check whether it is authentic.

Cryptographic Hash Functions

- Takes any arbitrarily sized string as input
  Input M: The message

- **Fixed size output** (We typically use 256 bits in Blockchain)
  Output H(M): We call this as the message digest

- **Efficiently computable**

Cryptographic Hash Functions: Properties

- **Deterministic**
  Always yields identical hash value for identical input data
- **Collision-Free**
  If two messages are different, then their digests also differ
- **Hiding**
  Hide the original message; remember about the **avalanche effect**
- **Puzzle-friendly**
  Given *X* and *Y,* find out *k* such that $Y = H(X||k)$ - used to solve the mining puzzle in Bitcoin Proof of Work

Collision Free

- Hash functions are one-way; Given an x, it is easy to find $H(x)$. However, given an $H(x)$, **one cannot find** x
- It is **difficult to find** x and y, where $x \neq y$, but $H(x) = H(y)$
- Note the phrase **difficult to find**, collision is **not impossible**
- Try with randomly chosen inputs to find out a collision – but it takes too long

Collision Free – How Do We Guarantee

- It may be relatively easy to find collision for some hash functions
- **Birthday Paradox:** Find the probability that in a set of n **randomly chosen persons,** some of them will have the same birthday
- By *Pigeonhole Principle*, the probability reaches 1 when number of people reaches 366 (not a leap year) or 367 (a leap year)
- 0.999 probability is reached with just ~70 people, and 0.5 probability is reached with only ~23 people

Collision Free – How Do We Guarantee

- Birthday paradox places an upper bound on collision resistance
- If a hash function produces N bits of output, an attacker needs to compute only $2^{\frac{N}{2}}$ hash operations on a random input to find two matching outputs with probability > 0.98
- For a 256 bit hash function, the attacker needs to compute 2^{128} hash operations – this is significantly time consuming
- If every hash computation takes only **1 microsecond**, it will need $\sim 10^{25}$ years

Hash as a Message Digest

- If we observe $H(x) = H(y)$, it is safe to assume $x = y$
- We need to remember just the hash value rather than the entire message – we call this as the **message digest**
- To check if two messages x and y are same, i. e. , whether $x =$ y, simply check if $H(x) = H(y)$
- This is efficient because the **size of the digest is significantly less than the size of the original messages**

Hashing - Illustration

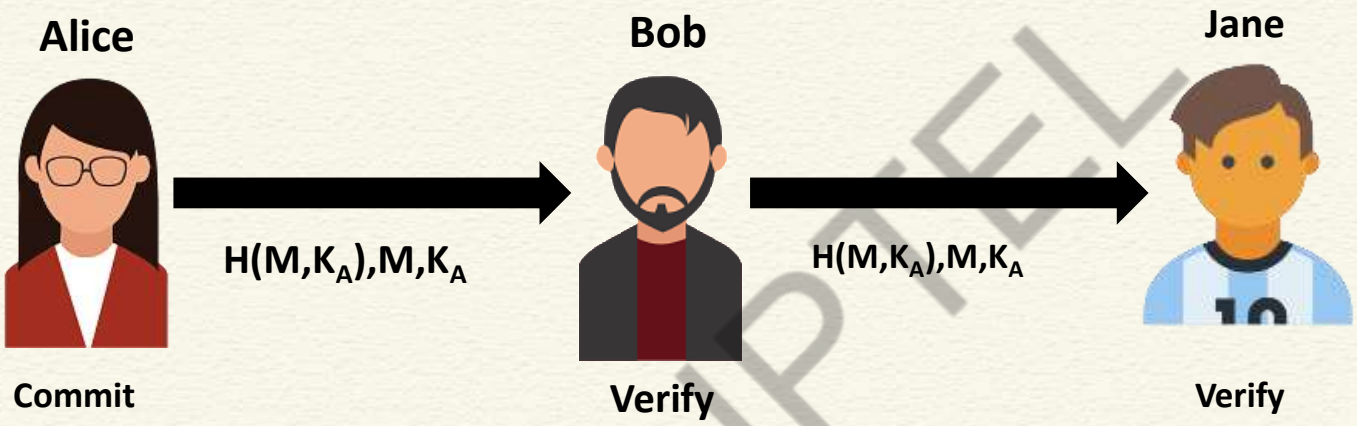
http://www.blockchain-basics.com/HashFunctions.html

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

Information Hiding through Hashing

- Given an $H(x)$, it is "computationally difficult" to find x
- The difficulty depends on the size of the message digests
- Hiding helps to commit a value and then check it later
- Compute the message digest and store it in a digest store – commit
- To check whether a message has been committed, match the message digest at the digest store

Message Commitment through Multiple Parties



K_A is the public key of Alice – A public identity that only Alice can have

Puzzle Friendly

- Say M is chosen from a widely spread distribution; it is computationally difficult to find a k, such that $Z = H(M||k)$, where M and Z are known a priori.
- **A Search Puzzle** (Used in Bitcoin Mining)
  M and Z are given, k is the search solution
  Note: It might be not exactly a particular value Z, but some properties that Z satisfies, i.e., Z could be a set of possible values
- Puzzle friendly property implies that random searching is the best strategy to solve the above puzzle

CONCLUSIONS

- Discussed what a cryptographic hash function is
- Properties of hash functions
- Uses of hash functions

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)

NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 04: Basic Cryptographic Primitives - II

CONCEPTS COVERED

- Cryptographic Hash Functions
- SHA-256
- Types of Hashing

KEYWORDS

- Hash Function
- Secure Hash Algorithm
- Patterns of Hashing Data

Hash Function – SHA256

- SHA256 is used in Bitcoin mining – to construct the Bitcoin blockchain
- Secure Hash Algorithm (SHA) that generates 256 bit message digest
- A part of SHA-2, a set of cryptographic hash functions designed by United States National Security Agency (NSA)

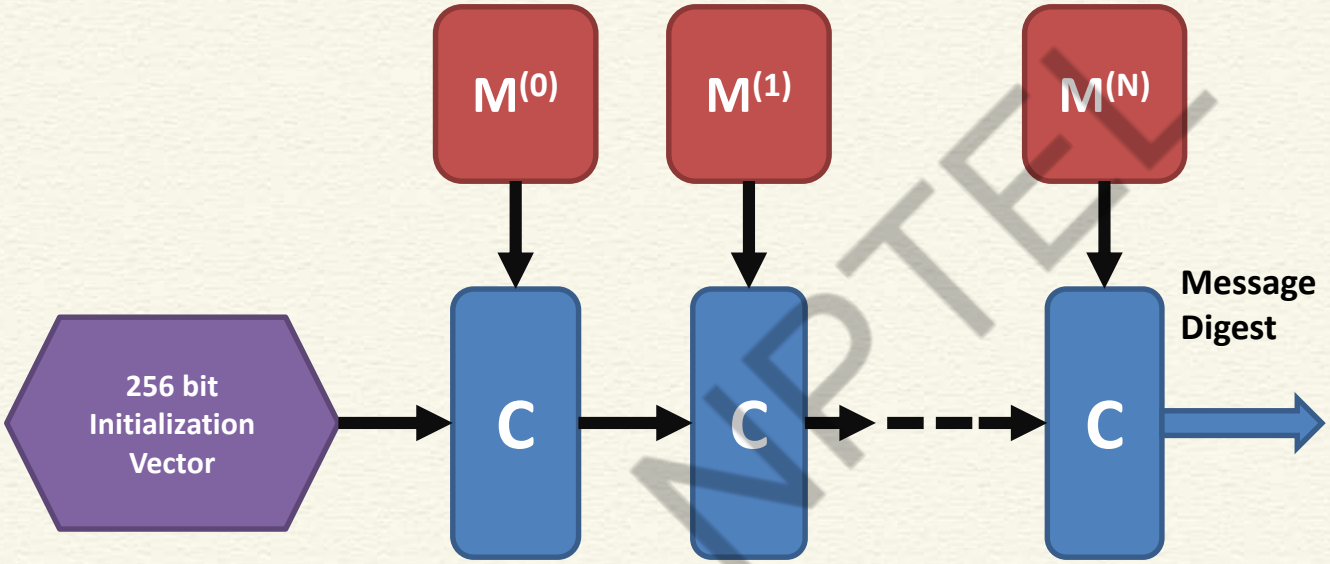
SHA256 Algorithm - Preprocessing

- Pad the message such that the message size is a multiple of 512
  - Suppose that the length of the message M is l; and $l \ mod$ 512≠0
  - Append the bit “1” at the end of the message
  - Append k zero bits, where k is the smallest non-negative solution to the equation l+1+k≡448 mod 512
  - Append the 64-bit block which is equal to the number l written in binary
  - **The total length gets divisible by 512**
- Partition the message into $\boldsymbol{N}$ 512-bit blocks $\boldsymbol{M^{(1)}, M^{(2)},\ldots, M^{(N)}}$
- Every 512 bit block is further divided into 32 bit sub-blocks $\boldsymbol{M_0^{(i)}, M_1^{(i)},\ldots, M_{15}^{(i)}}$

SHA-256 Algorithm

- The message blocks are processed one at a time
- Start with a fix initial hash value $H^{(0)}$
- Sequentially compute $H^{(i)} = H^{(i-1)} + C_{M^{(i)}}(H^{(i-1)})$; C is the SHA-256 *compression function* and + means mod 2^{32} addition. $H^{(N)}$ is the hash of M.

SHA-256 Algorithm

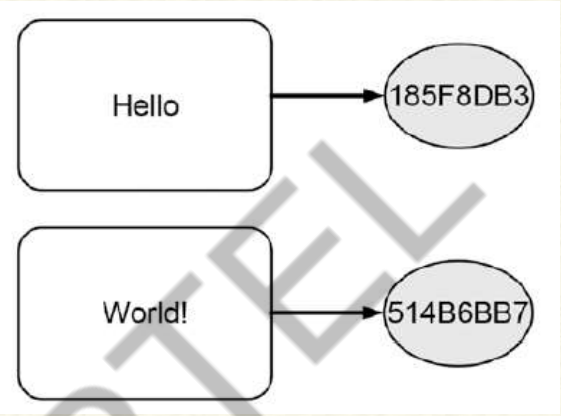


Patterns of Hashing Data

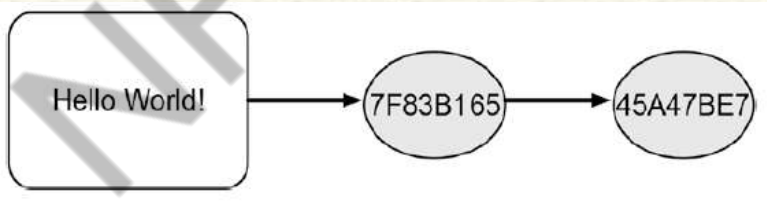
- Independent hashing
- Repeated hashing
- Combined hashing
- Sequential hashing
- Hierarchical hashing

Types of Hashing

- Independent hashing



- Repeated hashing

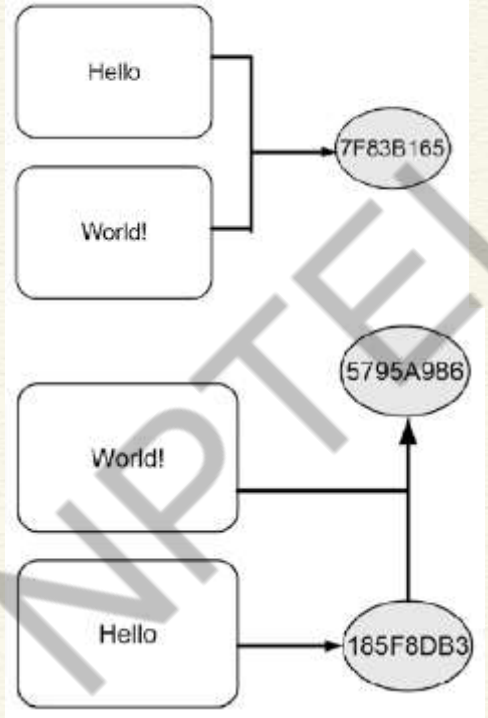


Courtesy: Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher

Types of Hashing

Combined hashing

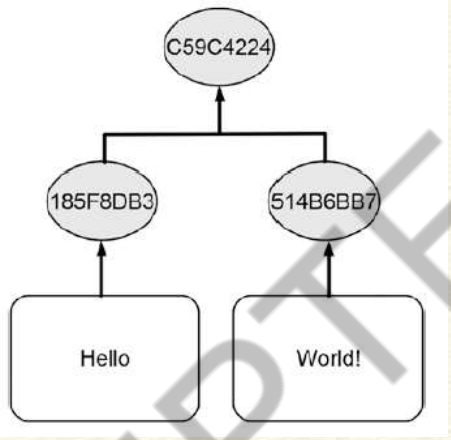
Sequential hashing



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

Types of Hashing

Hierarchical hashing



Illustration

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

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

CONCLUSIONS

- Discussed implementation of hash functions
- Types of hashing

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)

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

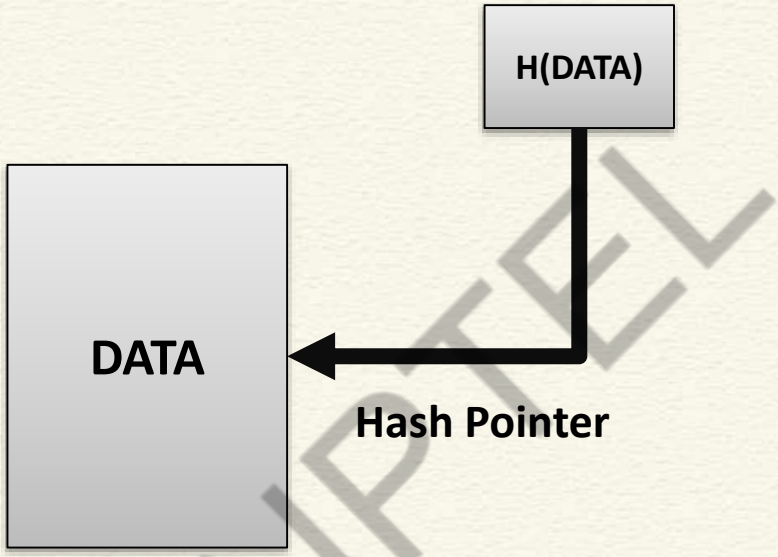
- Hash Function
- Hash Pointer
- Merkle Tree
- Blocks

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**)

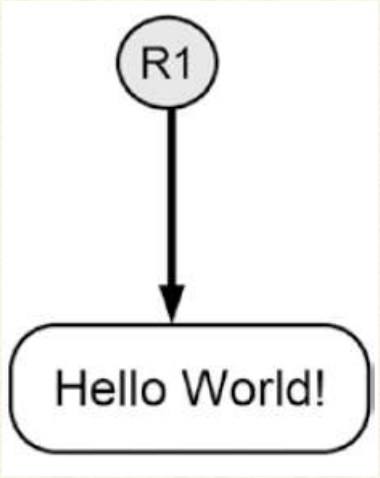
Hash Pointer

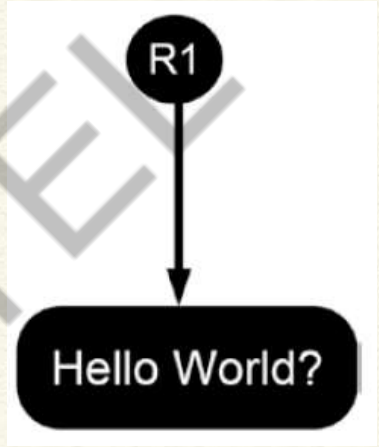


Reminds you of a linked list??

Reference: Coursera course on Bitcoin and Cryptocurrency Technologies

Tamper Detection using Hash Pointer

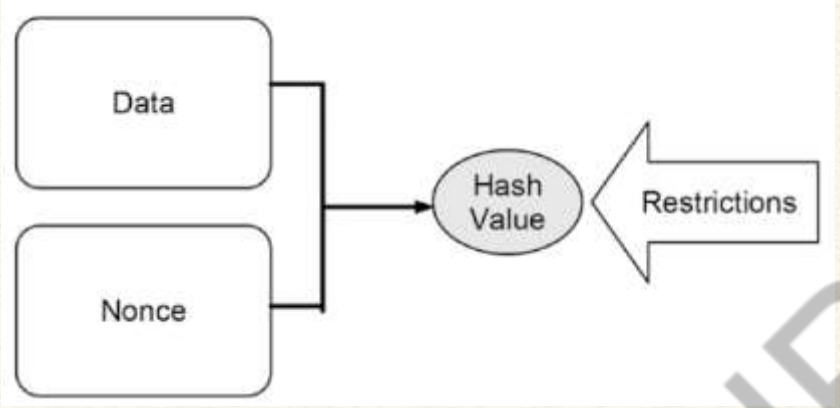




Analogies in real life??

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

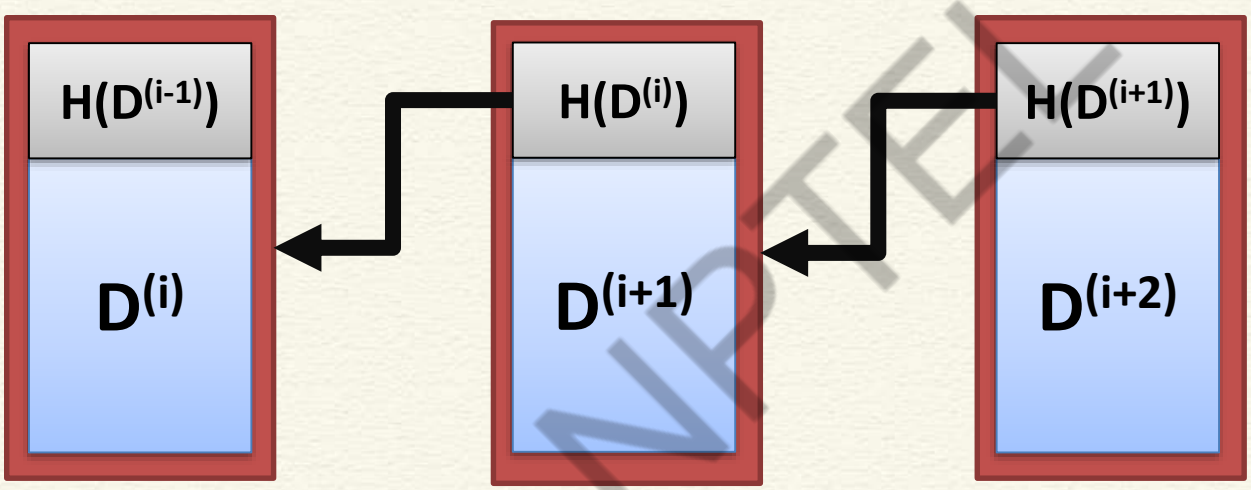
Nonce	Text to Be Hashed	Output
0	Hello World! 0	4EE4B774
1	Hello World! 1	3345B9A3
2	Hello World! 2	72040842
3	Hello World! 3	02307D5F
	...	
613	Hello World! 613	E861901E
614	Hello World! 614	**00068A3C**
615	Hello World! 615	5EB7483F

Illustration

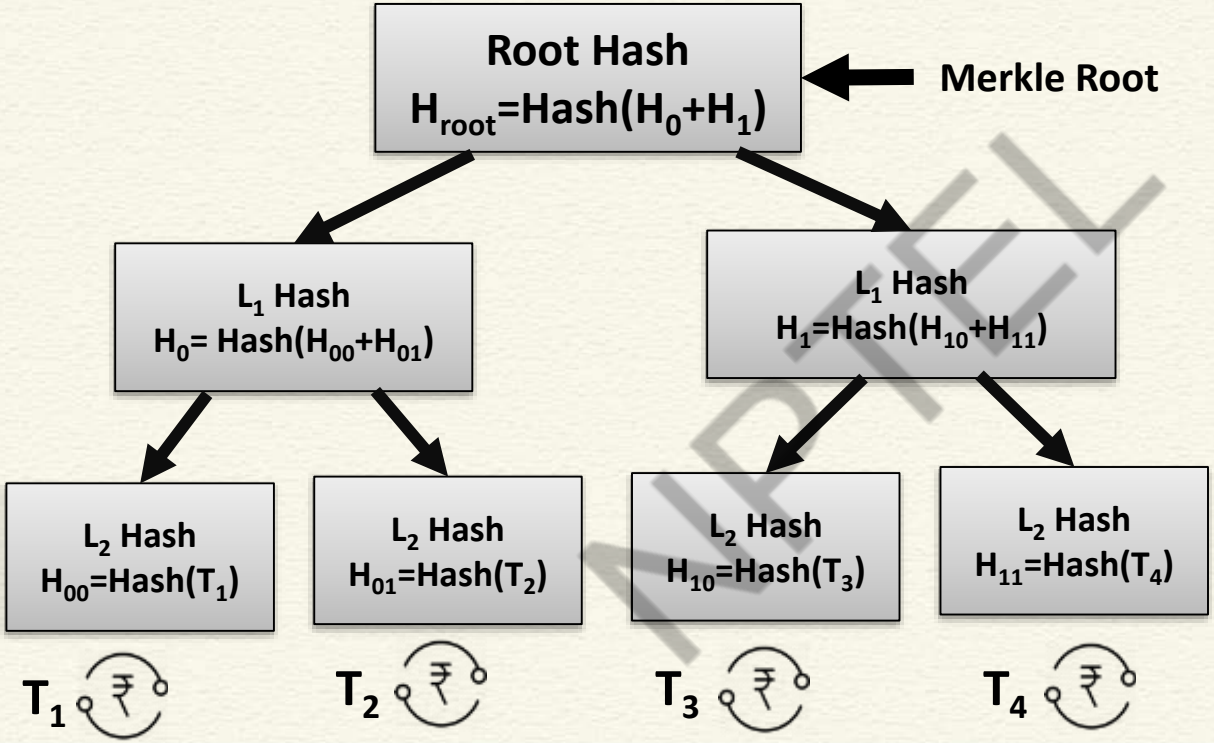
http://www.blockchain-basics.com/HashFunctions.html

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

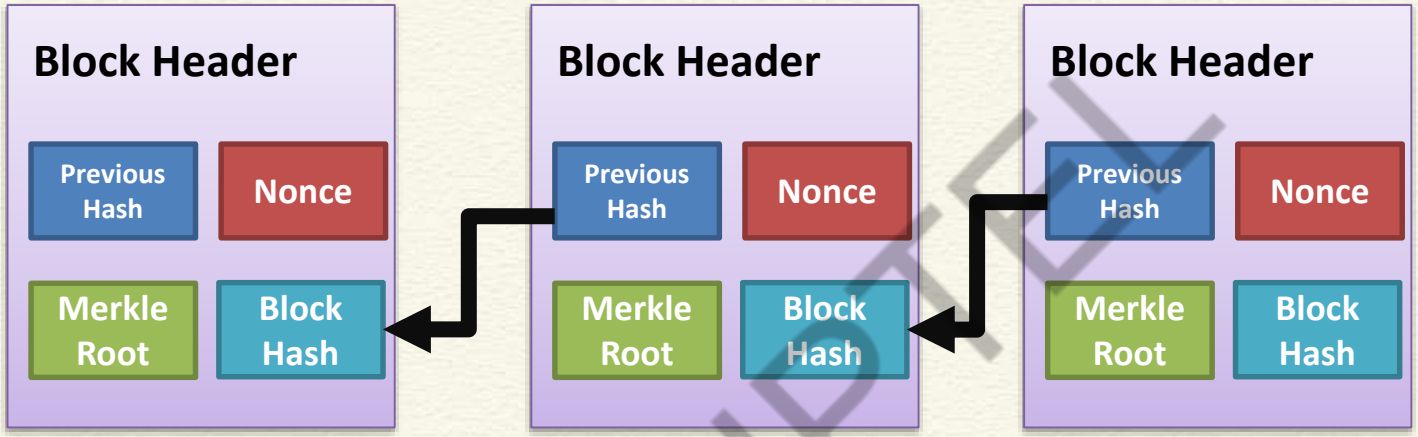
Detect Tampering from Hash Pointers - Hashchain



Merkle Tree – Organization of Hash Pointers in a Tree



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)