Blockchain Based Decentralized Distributed Architecture

Duration: 2-3 hours

1) Theory Lecture Contents:

i. Core Concepts/Working of Blockchain ---------- 30 min. (approx.)
ii. Real World Applications of Blockchain ---------- 30 min. (approx.)
iii. Misconception/Confusions about Blockchain ---------- 15 min. (approx.)
iv. Key Research Areas in Blockchain---------- 15 min. (approx.)

i. Core Concepts of Blockchain:

Blockchain [1] may be thought of as a distributed database which keeps its records immutable and secured through its basic data structure. In blockchain, the blocks containing transactions are linked through their hashes in the form of chain which keeps on growing as more and more transactions become the part of the system through these blocks. Every block of a blockchain contains a hash function that links the block from the previous one. It also contains timestamp and the information regarding the transaction also hashed in the blocks. These hashes of blocks are responsible for holding and linking the chain through the blocks. In order to alter any record, the whole chain of blocks will have to be changed from its genesis record which is very difficult as it requires a lot of computational and hashing power to produce such a chain. Being based upon a decentralized network technology, it eliminates the risk of effectively altering and controlling the data centrally and permanently. Data reliability is maintained by multiple copies of data at each node. The fundamental nature of blockchain data structure works more or less similar to a linked list. It is shared among all the nodes of the network while every fully running node keeps its own local copy of the entire blockchain as well which is frequently synchronized among all the peers for consistency. Blockchain is secured through hashes and Proof of Work.

The major attributes of blockchain may be summarized as follow;

a) Data Structure:

Consider 3 blocks as shown in Figure 1 with the following information as given below:

- Block 1 has the information of P_1 with the hash value of Q_1
- Block 2 has the information of P_2 with the hash value of Q_2
- Block 3 has the information of P_3 with the hash value of Q_3

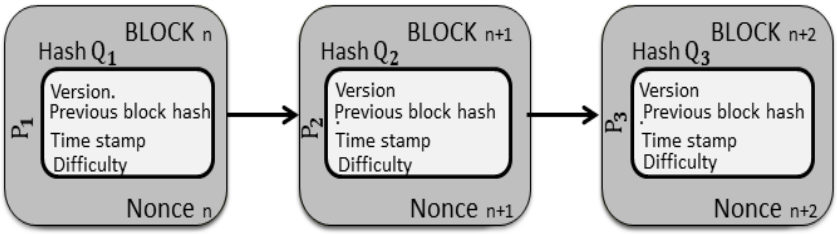


Figure 1: A Simplified Blockchain

Q_3 is created from the combination of Q_2 and $P_3$and so on while P_1comes from the default value P_0 [2].

b) Decentralized (Peer to Peer):

Referring to Figure 2, all the nodes are connected to every other node. The network is run by peers [3].

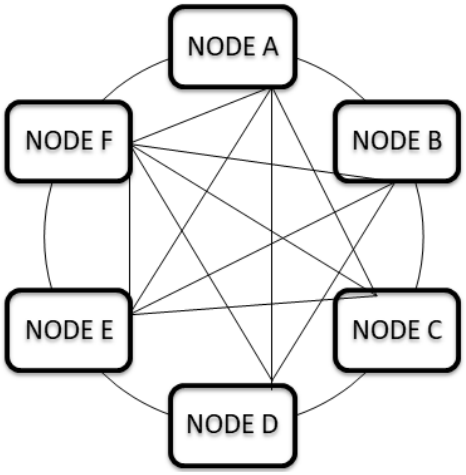


Figure 2: A Peer to Peer Network

c) Public ledger:

It is actually a series of transactions which are available publicly as it has been shown in the example of Figure 3. Every node keeps a copy of complete ledger. Therefore there is no need of having any trusted third party. The situation also poses new challenge of keeping all the copies of chain consistent and synchronized so that all nodes see the same blockchain as a distributed public ledger. New transactions are added to the chain through mining [4].

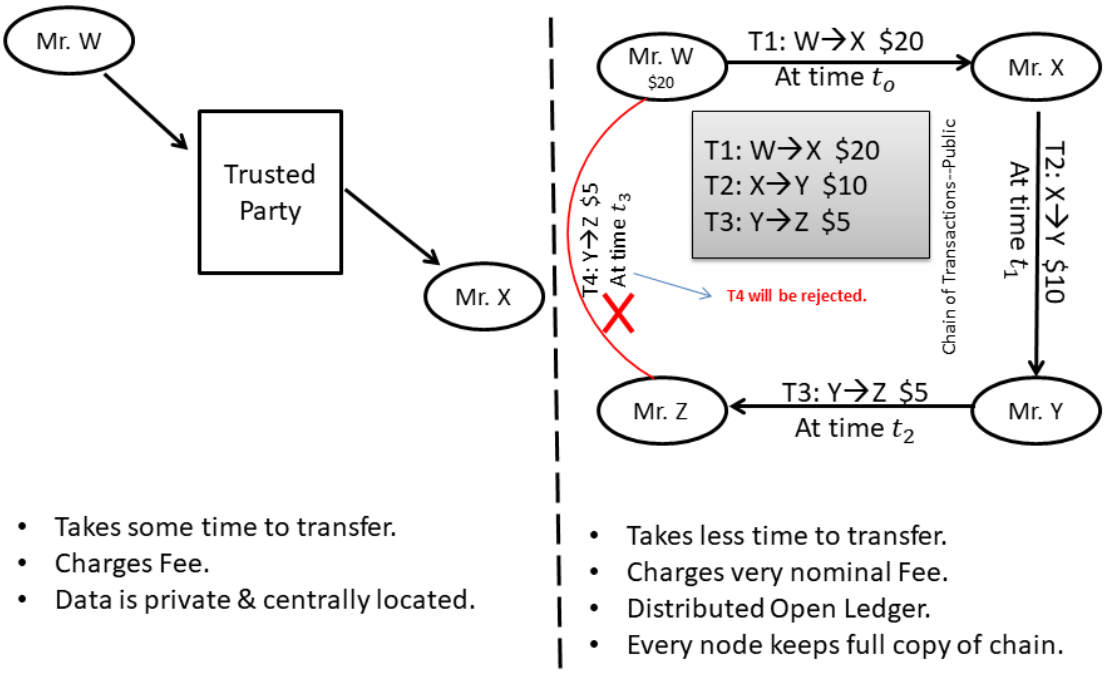
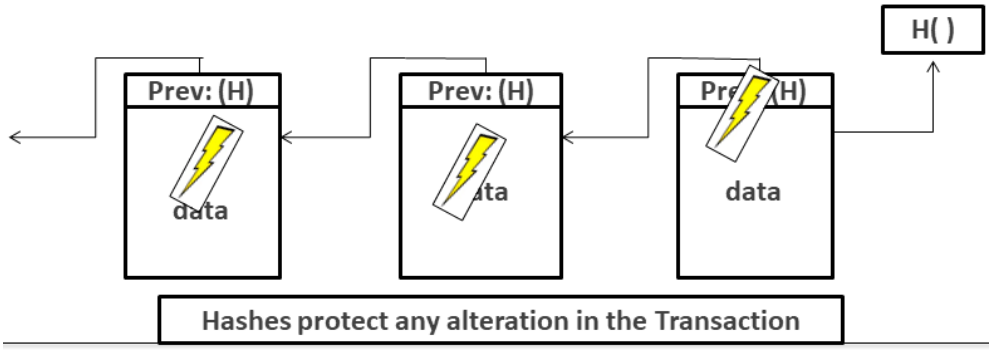


Figure 3: Centralised Vs Blockchain based Decentralised Distributed Public Ledger

d) Immutable:

Any tampering in the block is restricted by chaining the blocks through hashes [1].



ii. Real World Applications of Blockchain

a) Electronic Voting
b) Real State
c) Supply Chain Management
d) Provenance Tracking
e) Many others

iii. Clarifying Misconceptions:

a) Bitcoin is digital money.
b) Blockchain is a technology which enables Bitcoin to move from one account to another securely.
c) They are not same. But since Bitcoin has been the face of blockchain in the recent past, it would be good to build the fundamental concepts in the context of Bitcoin.
d) Blockchain attempts to solve the problem of asset transfer.
e) Transactions traditionally occur through a trusted third party in blockchain.

iv. Key Research Areas:

a) Learning Based Consensus Algorithm using Business Model Intelligence.
b) Subscription Based Mining For Private Blockchain
c) Collaborative Public Blockchain for Key Information Sharing
d) Provenance Enabled Integrated Intelligent Algorithm for Attack Protection

2) Lab: Building Blockchain Based Decentralized Distributed Architecture

Lab/Practical Demonstration:

i. Building Blockchain Decentralized Distributed Architecture -- 30 min. (approx.)
ii. Transaction Processing through Public addresses ---------- 10 min. (approx.)
iii. Demonstration of following Interesting Use-Cases ---------- 30 min. (approx.)

a) How the network would respond when one or more node goes down? (Will it continue to run since it is run by peers?)

b) How the network would respond when the receiver node goes down? (Will it affect the public ledger?)

c) How the network would respond in case when the seed node goes down as every node was initially connected through this? (Will the transaction be added to the local wallet? Will this transaction be added to blockchain?)

d) How controlling the mining power of network may impact the addition of blocks/number of confirmations to the blockchain to exploit the security of the network?

About Instructor:

Name: Dr. Kashif Mehboob Khan
Address: Department of Software Engineering, NED University , Karachi.

Short Biography:

Dr. Kashif Mehboob Khan is an Assistant Professor at NED University of Engineering & Technology Karachi. He is actively doing research in blockchain security. He has 15 years of overall experience including 5 years of experience in software analysis and development for a multinational company. He has got the publications in high impact factor journals focusing blockchain technology.

About Tutorial:

Addressing Technical Issues:
The tutorial will address the rising issue of transferring asset from one entity to another in a conventional centralised environment by proposing and implementing a distributed and decentralized architecture using public ledger.

Lecture/Hands-on Interaction:
The tutorial requires lecture as well as hand-on interaction.

Goal:
To Provide Strong theoretical and practical foundation for building and deploying distributed decentralized architecture for real world problems.

Topic Relevance:
The topic is about one of the most emerging technologies in distributed computing which is blockchain. The technology does not require any trusted party to run the system over the network and has been successful in variety of domains including well-known cryptocurrency, Bitcoin.

Target Audience:
Researchers/Students/Developers who are interested to build and deploy systems on distributed decentralised architecture.

Content Level:
20% Beginner , 70% Intermediate , 10% Advanced

Audience Prerequisites:
Basic Understanding of Networking and fundamental Programming Concepts

Two-Paged CV(Attached):

References

[1] "Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto," 2008.

[2] J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander, "Where is current research on Blockchain technology? - A systematic review," *PLoS ONE,* vol. 11, no. 10, 1 10 2016.

[3] O. Zimmermann, Q. Lu and X. Xu, "Adaptable Blockchain-Based Systems A Case Study for Product Traceability".

[4] A. L. Tsilidou and G. Foroglou, "Further applications of the blockchain," 2015.