Blockchain Technology

BC 2304 Mid Term Presentation

Presented by
MD. RAIHAN HOSSAIN
ID No. BC-23120414

Submitted by **Shaikat Majumder**,
Faculty at Creative IT Institute,
Blockchain Developer and Researcher,

Certified Trainer ToT,

Certified Associate NLP Practitioner

Welcome!!

The Presentation of

TCP/IP Model, Peer to Peer Networks, Digital Certificates

WHAT WE WILL LEARN HERE

TCP/IP Model

- Definition of TCP/IP Model
- Layer of TCP/IP Model
- OSI Model & TCP/IP Model

Peer to Peer Networks

- Definition of P2P Networks
- Types of P2P Networks
- Application of P2P Network (Blockchain)

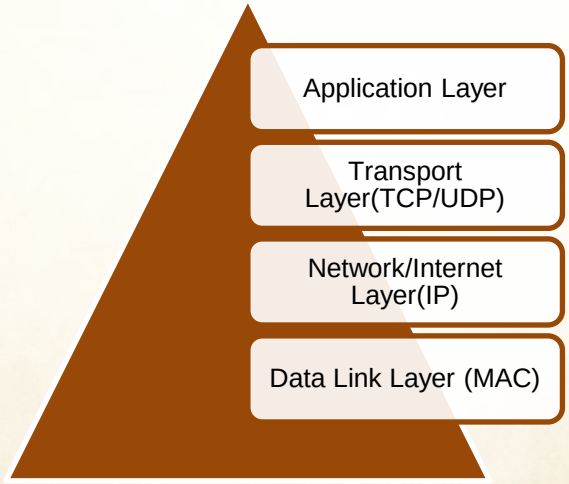
Digital Certificates

- Definition of Digital Certificates
- Encryption & Decryption
- Digital Signature & Digital Certificates

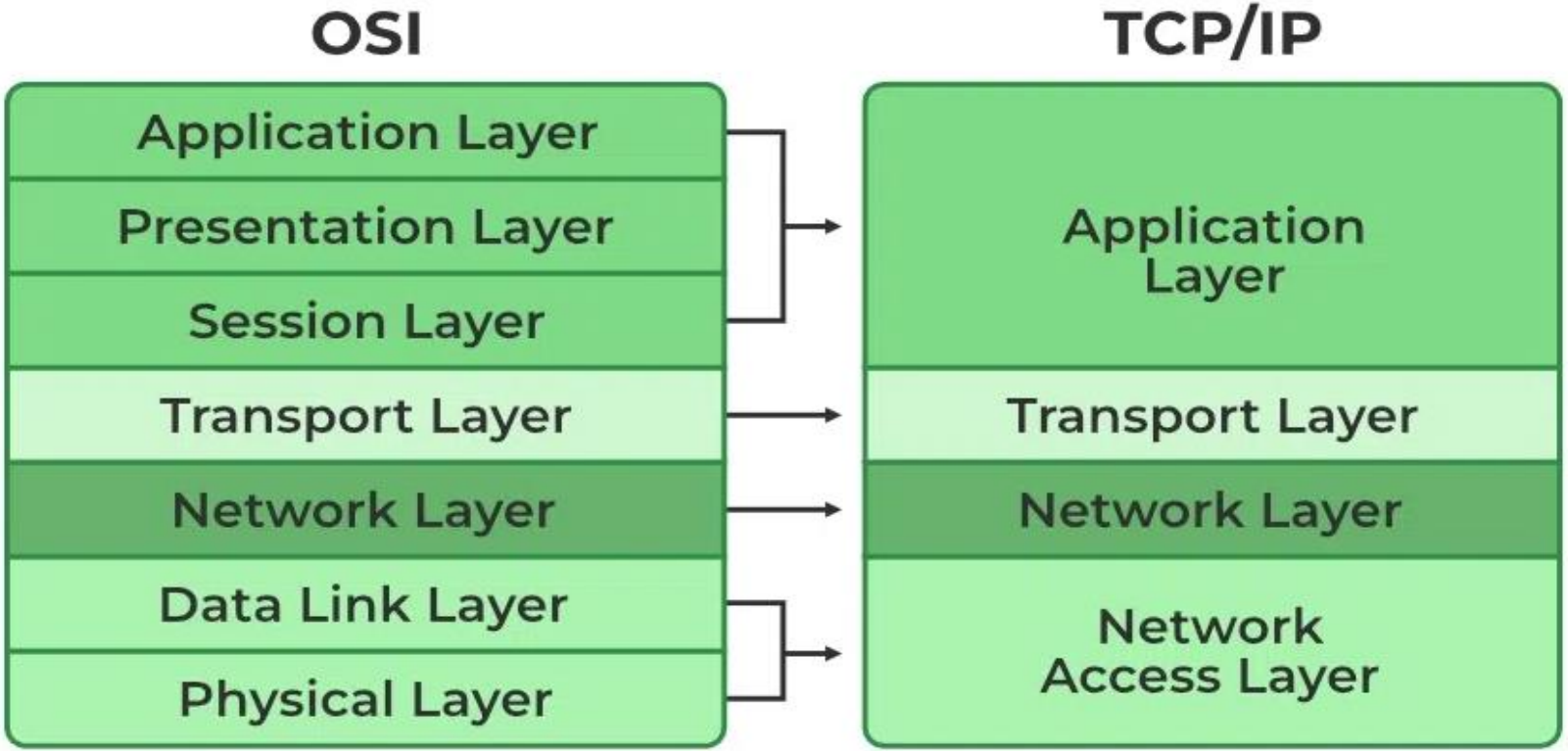
TCP/IP Model

TCP (Transmission Control Protocol) and **IP** (Internet Protocol). The main work of TCP/IP is to transfer the data of a computer from one device to another.

❑ Layer of TCP/IP Model



❑ OSI Model & TCP/IP Model



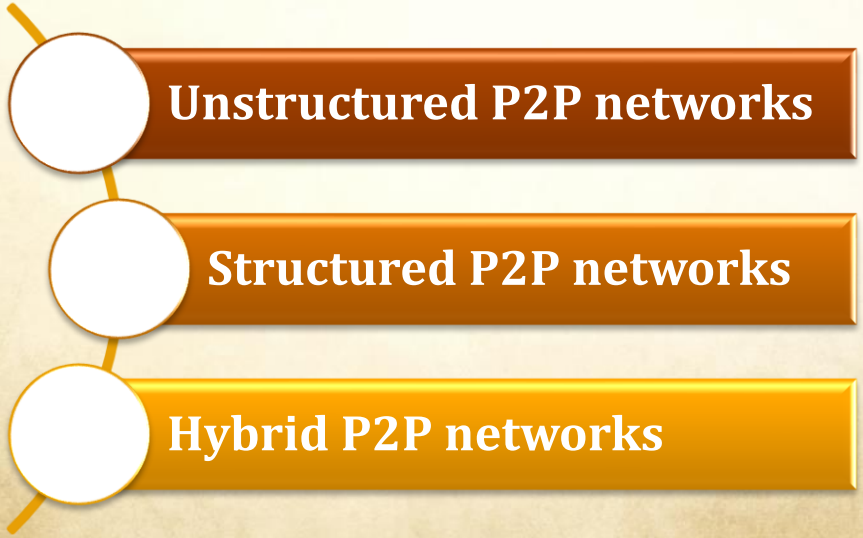
❑ Differences between OSI Model and TCP/IP Model

Parameters	OSI Model	TCP/IP Model
Full Form	OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/ Internet Protocol.
Layers	It has 7 layers.	It has 4 layers.
Usage	It is low in usage.	It is mostly used.
Approach	It is vertically approached.	It is horizontally approached.
Delivery	Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement	Replacement of tools and changes can easily be done in this model.	Replacing the tools is not easy as it is in OSI Model.
Reliability	It is less reliable than TCP/IP Model.	It is more reliable than OSI Mode

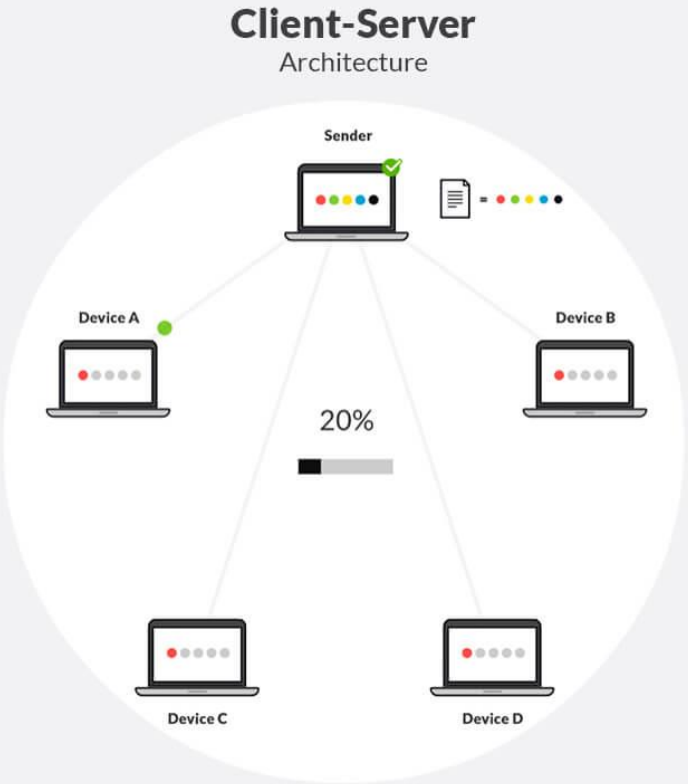
Peer to Peer Networks

In a peer-to-peer network, computers on the network are equal, with each workstation providing access to resources and data. This is a simple type of network where computers are able to communicate with one another and share what is on or attached to their computer with other users.

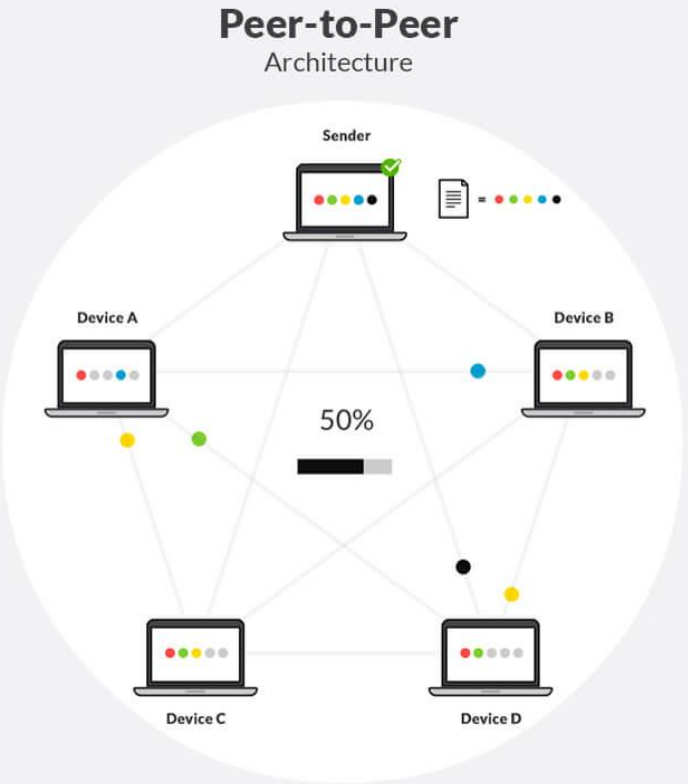
❑ Types of P2P Networks



❑ Application of P2P Network (Blockchain)



Vs.



✓ Centralized

✓ Decentralized

❑ Difference between Client-Server and Peer-to-Peer Network:

S.NO	Client-Server Network	Peer-to-Peer Network
1.	In Client-Server Network, Clients and server are differentiated, Specific server and clients are present.	In Peer-to-Peer Network, Clients and server are not differentiated .
2.	Client-Server Network focuses on information sharing.	While Peer-to-Peer Network focuses on connectivity.
3.	In Client-Server Network, Centralized server is used to store the data.	While in Peer-to-Peer Network, Each peer has its own data.
4.	In Client-Server Network, Server respond the services which is request by Client.	While in Peer-to-Peer Network, Each and every node can do both request and respond for the services.
5.	Client-Server Network are costlier than Peer-to-Peer Network.	While Peer-to-Peer Network are less costlier than Client-Server Network.
6.	Client-Server Network are more stable than Peer-to-Peer Network.	While Peer-to-Peer Network are less stable if number of peer is in crease.
7.	Client-Server Network is used for both small and large networks.	While Peer-to-Peer Network is generally suited for small network s with fewer than 10 computers.

Digital Certificates

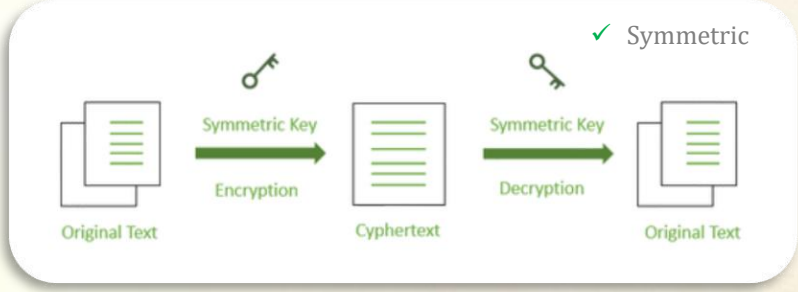
A digital certificate is a file or electronic password that proves the authenticity of a device, server, or user through the use of cryptography and the public key infrastructure (PKI).

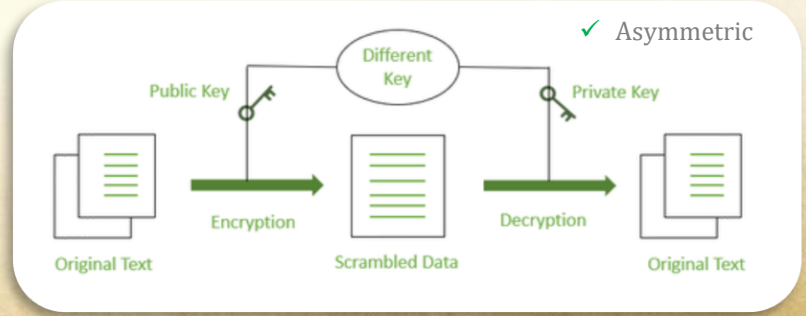
A digital signature refers to a more secure electronic signature that is generated using a digital certificate and cryptographically bound to the document using public key infrastructure (PKI).

Encryption

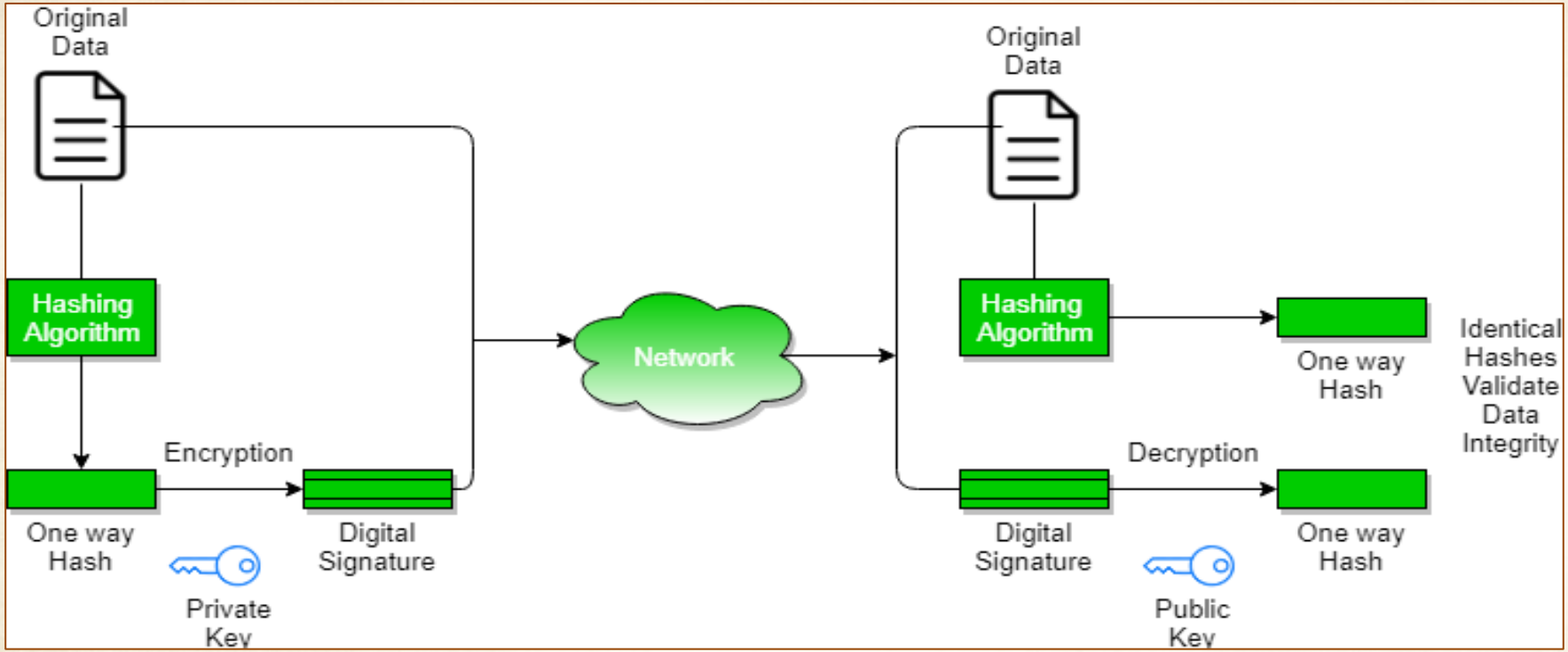
- **Symmetric Encryption**
- **Asymmetric Encryption**

Decryption





❑ Digital Signature



❑ Digital Signature & Digital Certificates

Feature	Digital Signature	Digital Certificate
Basics / Definition	A digital signature secures the integrity of a digital document in a similar way as a finger print or attachment.	Digital certificate is a file that ensures holder ’s identity and provides security.
Process / Steps	Hashed value of original data is encrypted us ing sender’s private key to generate the digit al signature.	It is generated by CA (Certifying Authority) t hat involves four steps: Key Generation, Regi stration, Verification, Creation.
Security Services	**Authenticity** of Sender, **integrity** of the doc ument and **non-repudiation**.	It provides security and **authenticity** of certi ficate holder.
Standard	It follows Digital Signature Standard (DSS).	It follows X.509 Standard Format

Thank You!!