



Centurion
UNIVERSITY
*Shaping Lives
Empowering Communities...*

School: Campus:

Academic Year: Subject Name: Subject Code:

Semester: Program: Branch: Specialization:

Date:

Classroom Learning

(Learning by Listening and Observations)

Name of the Topic: Whitepaper- Bitcoin : Peer-to-peer electronic cash system

Learning Outcome:

Concepts learned (Mention 2/3 principles):

Based on the classwork, the principal concepts I have learned include:

1. The fundamental concept of the Bitcoin whitepaper as the foundational document that introduced the first decentralized, "Bitcoin : Peer-to-peer electronic cash system".
2. The complete architecture of Bitcoin as outlined by Satoshi Nakamoto, solving the double-spending problem without a trusted central authority.
3. The characteristics of core components described: cryptographic proof, the Proof-of-Work consensus mechanism, the incentive structure for nodes, and the privacy model.

* New techniques learned:

Additionally, I have acquired new knowledge in the following areas:

1. Techniques for understanding the Merkle Tree structure to efficiently and securely verify the integrity of transactions within a block.
2. Procedures for how the network achieves consensus through the longest chain rule, ensuring all participants agree on a single transaction history.
3. The process of generating and verifying digital signatures (ECDSA) to authorize transactions and prove ownership of funds.
4. Methods for analyzing the economic incentives that align miners to act honestly, as their computational investment is only rewarded if they follow the protocol rules.

*** Related Project/Practice work experienced and learned:**

During the practice sessions of the lab work, I engaged in and developed proficiency with programs and simulations in the following areas:

1. Mapping the structure of a Bitcoin block header and simulating the hashing process to understand the Proof-of-Work mining concept.
2. Writing a simple program to generate a digital signature for a message and then verify it, mimicking Bitcoin transaction authorization.
3. Analyzing the original Bitcoin whitepaper to trace the logical argument from the double-spending problem to the proposed solution.
4. Using a Bitcoin testnet and a block explorer to trace a transaction from its broadcast through to its confirmation in a block.

New Software/Machine/Tool/Equipment/Experiment learned:

* During the lab session, I used **Bitcoin Core** to explore the blockchain structure, **Electrum Wallet** to handle keys and transactions, and **Learn Me A Bitcoin** and other online resources to deconstruct the technical concepts in the whitepaper.

1. **Store of Value:** The robust security and predictable monetary policy defined in the whitepaper have led to Bitcoin being adopted as "digital gold," a hedge against inflation and economic uncertainty.

Application of concept(s) (preferably real life scenario):

2. **Censorship-Resistant Transactions:** The peer-to-peer electronic cash system enables individuals to transact globally without permission from banks or governments, useful for donations in oppressive regimes or for prohibited trade.
3. **Final Settlement Layer:** The concept of irreversible transactions after sufficient confirmations makes Bitcoin a powerful settlement layer for high-value transactions between institutions.

*** Case Studies/Examples:**

1. **Hyperinflation Hedge:** Citizens in countries like Venezuela and Nigeria have used Bitcoin to preserve their savings as their local currencies hyperinflate, directly applying the concept of a decentralized currency outlined in the whitepaper.
2. **The Genesis Block Message:** The text embedded in the first Bitcoin block ("The Times 03/Jan/2009 Chancellor on brink of second bailout for banks") is a direct commentary on the failure of the traditional financial system and the need for the alternative system proposed in the whitepaper.
3. **Institutional Adoption:** Publicly traded companies like MicroStrategy and Tesla have added Bitcoin to their treasury reserves, treating it as a legitimate store of value, a concept made possible by the security and scarcity mechanisms defined in the original document.

Assessment:

Marks Obtained: / 10

Signature of the Student:

Name :

Regn. No. :

Signature of the Faculty:

Page No.....

PN Archana

* As applicable according to the topic.
One sheet per topic (10-20) to be used.

240720100147