# **Assignment 1**

[**Uploaded @Github link:** **https://github.com/Simi-Paxleal-J/Advanced-Blockchain-Assignments/blob/main/Day1/Assignment%201**](Uploaded%20@Github%20link:%20https://github.com/Simi-Paxleal-J/Advanced-Blockchain-Assignments/blob/main/Day%201%20-%20Assignment%201)

## **Bitcoin: A Peer-to-Peer Electronic Cash System an Overview**

* Problem of the financial Cash system is the involvement as the third party to process electronic transaction, suffers trust-based model that led to casual percent of fraud but can be avoided by direct physical transaction without relying on the intermediaries but not in the case of the distance and geographic location between sender and receiver
* To overcome the defect by said (trusted) third party involvement the much-needed method will be the electronic mode with cryptographic trust and direct involvement of the parties of transaction leaving the third party not needed
* The above solution is achievable by using the defined electronic coin (to avoid the mint manufacturing that involves financial institution), replacing the symbols on currency using the digital signature on the digital coin by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership
* Another sub-solution will be timestamp introduction by wide publish of hash with the data of each timestamp of previous timestamp in the hash forming a chain enforces with each transaction containing timestamp reinforcing the ones before it.
* The cryptographic trust is by SHA-256 proof of work hash begins with a number of zero bits, solves the problem of determining representation in majority decision making. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes
* Network is established by establishing the chain of ownership to the original blockchain using the nodes in network where each node collects new transactions into a block with data of all hash, transaction info., timestamp converted to hash header to be assigned as hash signature for the next coming transaction and node that lengths the blockchain itself.
* The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins
* Most of the data corrupted due to consumption of high disk space that can be resolved by the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree. and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory that simplifies the payment verification easily
* A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced, he has the longest chain helps the trust verification individually without the involvement of the third party increases the privacy itself
* By keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone protection from unwanted manipulation from outside

## **International financial crisis of 2007-2008**

The financial crisis of 2007–2008, (the global financial crisis (GFC)), was a severe worldwide financial crisis. Excessive risk-taking by banks combined with the bursting of the United States housing bubble caused the values of securities tied to U.S. real estate to plummet, damaging financial institutions globally, culminating with the bankruptcy of Lehman Brothers on September 15, 2008, and an international banking crisis. The crisis sparked the Great Recession, which, at the time, was the most severe global recession since the Great Depression.

From its peak in the second quarter of 2007 at $64.4 trillion, household wealth in the United States fell $14 trillion, to $50.4 trillion by the end of the first quarter of 2009, resulting in a decline in consumption then a decline in business investment. In the fourth quarter of 2008, the quarter-over-quarter decline in real GDP in the U.S. was 8.4%. The U.S. unemployment rate peaked at 10.0% in October 2009, the highest rate since 1983 and roughly twice the pre-crisis rate.

While the causes of the bubble are disputed, the precipitating factor for the Financial Crisis of 2007–2008 was the bursting of the United States housing bubble and the subsequent subprime mortgage crisis, which occurred due to a high default rate and resulting foreclosures of mortgage loans, particularly adjustable-rate mortgages.

Some factors involved in the great depression were

* **Overproduction**
* **executive inaction**
* **Ill-timed tariffs**
* **An inexperienced Federal Reserve**