**Bitcoin: A Peer-to-Peer Electronic Cash System**

**Summary:**

The main focus of this paper is an introduction of peer-to-peer version of electronic cash without introducing any third party financial institution and send directly from one party to another. The chances of frauds are unavoidable in case of conventional payment methods if any third party in involved this proposed system removes all such issues.

In this paper cryptography is used not only for the exchange of data but instead cryptographic data is used both as a digital currency and proof of trust. This paper provides a solution to the double-spending problem.

The system introduced in this paper uses a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. Network is built around timestamp server where a group of transactions form a block which is then hashed along with the previous hash which is then published publicly on the network. In this system every timestamp reinforces all the previous timestamps and this is one of the key plus points of this system as this will help to reduce the changes of fraud or any hacking attack on the system.

The proposed system defines electronic coin as a chain of digital signatures and each owner transfers the coin to the next 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 list of previous owners of the coin using the signatures. The paper also discuss the system to stop any hacking attacks.

In the proposed system the new transactions are broadcast to all nodes. Each node collects new transactions into a block. Each node works on finding a difficult proof-of-work for its block. When a node finds a proof-of-work, it broadcasts the block to all nodes. Nodes accept the block only if all transactions in it are valid and not already spent. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash. Nodes always consider the longest chain to be the correct one and will keep working on extending it.

The system encourages the participating nodes to be hones using incentives opportunity. This facility not only encourages to take part in the process more actively in fact it provide the greedy hacker a reasonable profitable valid way to earn the coins instead of doing any illegal activity.

The system also provide opportunity to reclaim the disk space. The latest transaction in a coin is buried under enough blocks, the spent transactions are hashed in a merkle tree with only the root included in the block's hash to save disk space.

This system introduces the concept of public transactions unlike traditional banking system the banks keep the transactions private between clients and bank and public can see the information about the transactions without information linking the transaction to anyone.

**Questions:**

There writer said any new needed rules and incentives can be enforced with this consensus mechanism but haven’t discussed the details of the census process w.r.t this system.

**1 -** If hackers with greater CPU power than our system attack how the system reacts to safeguard its data and structure?

**2 -** The incentive can also be funded with transaction fees. Isn’t it more costly and what is the other way to fund the incentives other than transaction fee?

**3 -** System uses a lot of computational and electronic resources. Isn’t the cost and resources increasing demand create problems for the system?

**4 -** Nodes work all at once with little coordination. Isn’t this lack of co-ordination source of problems for proposed system efficiency and consistency?