**Review of Bitcoin**

# **Summary**

Commerce on the Internet suffers from the inherent weaknesses of the trust based model. A certain percentage of fraud is accepted as unavoidable.

What is needed is double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.

This is a system for electronic transactions without relying on trust.

**Contributions**

① proposed a solution to the double-spending problem using a peer-to-peer network. ②The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes. ③ provided a way to initially distribute coins into circulation, since there is no central authority to issue them. ④ Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. ⑤ simplified payment verification.

**Comments**

**Flash Points:** find a way to deal with the double-spending problem using peer-to-peer network. proposed a system for electronic transactions without relying on trust. The network is robust in its unstructured simplicity.