Bitcoin Summary

The paper discusses an **electronic payment system** using a digital currency (**Bitcoin**) that enables parties to transact without a intermediary. In physical currency, a third party was necessary for trust and to prevent transaction reversals. In this paper, a method will be proposed to make transactions one-way and irreversible.

The **electronic coin** is a chain of digital signatures. Each owner transfers the coin by signing a hash of the previous transaction and the public key and adding it to the end of the coin. The payee can verify the chain of ownership by signatures.

Each **transaction** has a timestamp that is stamped onto every block. The timestamp includes the previous timestamp and reinforces the chronological order of transactions.

To prevent double-spending, a **consensus** mechanism is used to agree on the transaction to be executed (PoW). The PoW is executed by incrementing a value (nonce) in the block until a hash value is found that meets the required number of zero bits.

If an attacker wants to manipulate a certain block, they would need to calculate the PoW for that block and all subsequent blocks. Compared to the trusted nodes, the attacker's attempt would be too slow to catch up and the probability of succeeding decreases with each new block added to the network.

Resource:
Bitcoin Whitepaper: https://bitcoin.org/bitcoin.pdf

مهند الحطامي

مهند الزهراني

عبد الله حجو