MyCoin: A Peer-to-Peer Electronic Cash System

John Crypto
john.crypto@example.com
www.mycoin.org

Abstract

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-power, forming a record that cannot be changed without redoing the proof-of-power.

Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not possible, resulting in significant costs.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly without the need for a trusted third party.

Transactions

We define an electronic coin as a chain of digital signatures. 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.

Proof-of-Power

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-power system similar to Adam Back's Hashcash, rather than newspaper or Usenet posts.

Network

The steps to run the network are as follows:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a proof-of-power for its block.

Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with a standard framework, adding innovations like the peer-to-peer timestamp network and proof-of-power.

MyCoin could become a new standard for decentralized online commerce.