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

Satoshi Nakamoto

satoshin@gmx.com

www.bitcoin.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-work, forming a record that cannot be changed without redoing

the proof-of-work. The longest chain not only serves as proof of the sequence of

events witnessed, but proof that it came from the largest pool of CPU power. As

long as a majority of CPU power is controlled by nodes that are not cooperating to

attack the network, they'll generate the longest chain and outpace attackers. The

network itself requires minimal structure. Messages are broadcast on a best effort

basis, and nodes can leave and rejoin the network at will, accepting the longest

proof-of-work chain as proof of what happened while they were gone.

**1. 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 really possible, since financial institutions cannot

avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

minimum practical transaction size and cutting off the possibility for small casual transactions,

and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible

services. With the possibility of reversal, the need for trust spreads. Merchants must

be wary of their customers, hassling them for more information than they would otherwise need.

A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties

can be avoided in person by using physical currency, but no mechanism exists to make payments

over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust,

allowing any two willing parties to transact directly with each other without the need for a trusted

third party. Transactions that are computationally impractical to reverse would protect sellers

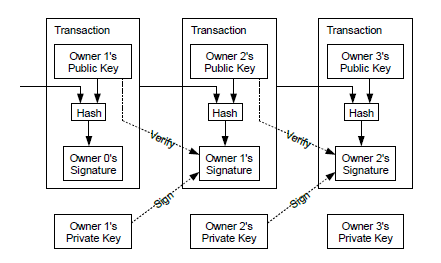
from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In

this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed

timestamp server to generate computational proof of the chronological order of transactions. The

system is secure as long as honest nodes collectively control more CPU power than any

cooperating group of attacker nodes.



What is needed is an electronic payment system based on cryptographic proof instead of trust,

allowing any two willing parties to transact directly with each other without the need for a trusted

third party. Transactions that are computationally impractical to reverse would protect sellers

from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In

this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed

timestamp server to generate computational proof of the chronological order of transactions. The

system is secure as long as honest nodes collectively control more CPU power than any

cooperating group of attacker nodes.

What is needed is an electronic payment system based on cryptographic proof instead of trust,

allowing any two willing parties to transact directly with each other without the need for a trusted

third party. Transactions that are computationally impractical to reverse would protect sellers

from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In

this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed

timestamp server to generate computational proof of the chronological order of transactions. The

system is secure as long as honest nodes collectively control more CPU power than any

cooperating group of attacker nodes.

What is needed is an electronic payment system based on cryptographic proof instead of trust,

allowing any two willing parties to transact directly with each other without the need for a trusted

third party. Transactions that are computationally impractical to reverse would protect sellers

from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In

this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed

timestamp server to generate computational proof of the chronological order of transactions. The

system is secure as long as honest nodes collectively control more CPU power than any

cooperating group of attacker nodes.