

[Skip to site navigation \(Press enter\)](#)

# Bitcoin P2P e-cash paper

[Satoshi Nakamoto Sat, 01 Nov 2008 16:16:33 -0700](#)

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:

<http://www.bitcoin.org/bitcoin.pdf>

The main properties:

Double-spending is prevented with a peer-to-peer network.

No mint or other trusted parties.

Participants can be anonymous.

New coins are made from Hashcash style proof-of-work.

The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted 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 honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted 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.

Full paper at:

<http://www.bitcoin.org/bitcoin.pdf>

Satoshi Nakamoto

---

The Cryptography Mailing List

Unsubscribe by sending "unsubscribe cryptography" to [EMAIL PROTECTED]

- [Previous message](#)
- [View by thread](#)
- [View by date](#)
- [Next message](#)
  
- Bitcoin P2P e-cash paper Satoshi Nakamoto
  - [Re: Bitcoin P2P e-cash paper](#) James A. Donald
    - [Secrets and cell phones.](#) James A. Donald
      - [Why the poor uptake of encrypted email?...](#) StealthMonger
        - [Re: Why the poor uptake of encrypte...](#) JOHN GALT
          - [Re: Why the poor uptake of enc...](#) David G. Koontz
            - [Re: Why the poor uptake of...](#) Dirk-Willem van Gulik
            - [Re: Why the poor uptake of enc...](#) Alec Muffett

- [Re: Why the poor uptake of...](#) ji
- [Re: Why the poor uptake of...](#) StealthMonger
- [Re: Why the poor uptake...](#) Nicolas Williams

## Reply via email to



Search the site  

- [The Mail Archive home](#)
- [cryptography - all messages](#)
- [cryptography - about the list](#)
- [Expand](#)
- [Previous message](#)
- [Next message](#)
  
- [The Mail Archive home](#)
- [Add your mailing list](#)
- [FAQ](#)
- [Support](#)
- [Privacy](#)
- CHILKAT-MID-dd013ecc-8c7f-fc14-b1c5-cc9fd0181098@server123