Search P2P Foundation Search

- Sign Up
- Sign In

The Foundation for Peer to Peer Alternatives

- Main
- My Page
- Members
- Videos
- Forum
- Groups
- Blogs
- Chat

- All Discussions
- My Discussions
- Add

Bitcoin open source implementation of P2P currency

- Posted by Satoshi Nakamoto on February 11, 2009 at 22:27
- View Discussions

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical.

Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at http://www.bitcoin.org/bitcoin.pdf

The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.

Satoshi Nakamoto
http://www.bitcoin.org

Share Tweet Facebook

Views: 298881

► Reply to This

Replies to This Discussion

Permalink Reply by Sepp Hasslberger on February 12, 2009 at 14:44

Great stuff.

This is the first real innovation in money since the Bank of England started to issue its promissory notes for gold in the vaults, which then became known as banknotes.

I believe an open source currency has great potential. A bit like Google becoming the default search engine for many of us.

- ► Reply
-

Permalink Reply by Sepp Hasslberger on February 14, 2009 at 15:30

Dante, in an email, has mentioned a UK project called Open Coin. It seems to go in a similar direction.

Could there be synergies with bitcoin?

http://opencoin.org/