COPA vs Craig Wright > Ich bin Satoshi. <

Zeugen sind u.a. Martti Malmi, Mike Hearn und Adam Back.

From: "satoshi@anonymousspeech.com" <satoshi@anonymousspeech.com>
Sent: Wed 8/20/2008 6:30:39 PM (UTC+01:00)
To: adam@cypherspace.org
Subject: Citation of your Hashcash paper

I'm getting ready to release a paper that references your Hashcash paper and I wanted to make sure I have the citation right. Here's what I have:

[5] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

I think you would find it interesting, since it finds a new use for hash-based proof-of-work as a way to make e-cash work. You can download a pre-release draft at http://www.upload.ae/file/6157/ecash-pdf.html Feel free to forward it to anyone else you think would be interested. I'm also nearly finished with a C++ implementation to release as open source.

Title: Electronic Cash Without a Trusted Third PartyAbstract: 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 offer 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.

satoshi@anonymousspeech.com

From: "Satoshi Nakamoto" <satoshi@vistomail.com>
Sent: Sat 1/10/2009 6:46:45 PM (UTC)
To: adam@cypherspace.org
Subject: Re: Citation of your Hashcash paper

Thanks for the pointers you gave me to Wei Dai's b-money paper and others.

I just released the open source implementation of my paper, Bitcoin v0.1.
Details, download and screenshots are at www.bitcoin.org

The main idea of the system is the generation of a chain of hash based proof-of-work to create self evident proof of the majority consensus.
Users get new coins by contributing proof-of-work to the chain.

There was a discussion of the design on the Cryptography mailing list.
Hal Finney gave a good high-level overview:
| One thing I might mention is that in many ways bitcoin is two independent
| ideas: a way of solving the kinds of problems James lists here, of
| creating a globally consistent but decentralized database; and then using
| it for a system similar to Wei Dai's b-money (which is referenced in the
| paper) but transaction/coin based rather than account based. Solving the
| global, massively decentralized database problem is arguably the harder
| part, as James emphasizes. The use of proof-of-work as a tool for this
| purpose is a novel idea well worth further review IMO.

Satoshi