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

>Yes citation looks fine, I'll take a look at your paper. You maybe
>aware of the "B-money" proposal, I guess google can find it for you,
>by Wei Dai which sounds to be somewhat related to your paper. (The
>b-money idea is just described concisely on his web page, he didnt
>write up a paper).
>
>Adam
>
>On Wed, Aug 20, 2008 at 6:30 PM, satoshi@anonymousspeech.com
><satoshi@anonymousspeech.com> wrote:
>> 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 Party
>>
>> 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 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@anonymousspeech.com" <satoshi@anonymousspeech.com>

Sent: Thur 8/21/2008 6:59:49 PM (UTC+01:00)

To: adam@cypherspace.org

Subject: RE: Citation of your Hashcash paper

Thanks, I wasn't aware of the b-money page, but my ideas start from exactly that point. I'll e-mail him to confirm the year of publication so I can credit him.

The main thing my system adds is to also use proof-of-work to support a distributed timestamp server. While users are generating proof-of-work to make new coins for themselves, the same proof-of-work is also supporting the network timestamping. This is instead of Usenet.

Satoshi

>Yes citation looks fine, I'll take a look at your paper. You maybe
>aware of the "B-money" proposal, I guess google can find it for you,
>by Wei Dai which sounds to be somewhat related to your paper. (The
>b-money idea is just described concisely on his web page, he didnt
>write up a paper).
>
>Adam
>>On Wed, Aug 20, 2008 at 6:30 PM, satoshi@anonymousspeech.com
><satoshi@anonymousspeech.com> wrote:
>> 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 Party
>>
>> 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 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: "Adam Back" <adam@cypherspace.org>

Sent: Thur 8/21/2008 7:17:17 PM (UTC+01:00)

To: satoshi@anonymousspeech.com

Cc: adam@cypherspace.org

Subject: Re: Citation of your Hashcash paper

Sorry still not read your paper yet, but another related paper is by
Rivest et al called micromint, which uses k-way collisions to create
an over-time computational advantage for the bank in creating coins.
What you said about one group of players having an advantage (by
compute cycles) reminded me of micromint. In micromint the bank gets
an increasing advantage over time as there is some cumulative build up
of advantage in terms of the partial results accumulated helping
create further the partial-collisions more cheaply.

Adam

On Thu, Aug 21, 2008 at 6:59 PM, satoshi@anonymousspeech.com
<satoshi@anonymousspeech.com> wrote:
> Thanks, I wasn't aware of the b-money page, but my ideas start from exactly that point. I'll e-mail him to confirm the year of publication so I can credit him.
>
> The main thing my system adds is to also use proof-of-work to support a distributed timestamp server. While users are generating proof-of-work to make new coins for themselves, the same proof-of-work is also supporting the network timestamping. This is instead of Usenet.
>
> Satoshi
>
>>Yes citation looks fine, I'll take a look at your paper. You maybe
>>aware of the "B-money" proposal, I guess google can find it for you,
>>by Wei Dai which sounds to be somewhat related to your paper. (The
>>b-money idea is just described concisely on his web page, he didnt
>>write up a paper).
>>
>>Adam
>>
>>On Wed, Aug 20, 2008 at 6:30 PM, satoshi@anonymousspeech.com
>><satoshi@anonymousspeech.com> wrote:
>>> 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 Party
>>>
>>> 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 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@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: "Adam Back" <adam@cypherspace.org>

Sent: Thur 8/21/2008 1:55:59 PM (UTC+01:00)

To: satoshi@anonymousspeech.com

Cc: adam@cypherspace.org

Subject: Re: Citation of your Hashcash paper

Yes citation looks fine, I'll take a look at your paper. You maybe aware of the "B-money" proposal, I guess google can find it for you, by Wei Dai which sounds to be somewhat related to your paper. (The b-money idea is just described concisely on his web page, he didnt write up a paper).

Adam

On Wed, Aug 20, 2008 at 6:30 PM, satoshi@anonymousspeech.com <satoshi@anonymousspeech.com> wrote:
> 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 Party
>
> 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 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
>
>
>