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

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/

- ▶ Reply

Permalink Reply by Satoshi Nakamoto on February 15, 2009 at 16:42
Could be. They're talking about the old Chaumian central mint stuff, but maybe only because that was the only thing available. Maybe they would be interested in going in a new direction.

A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system.

- ▶ Reply

 Permalink Reply by Joerg Baach on February 17, 2009 at 10:42
Hi Satoshi,

we are actually really talking about the old Chaumian central stuff. That was because a) it was there b) it was patent free (we have to think a bit about the US). I had a read of your paper on the weekend - thanks a lot for doing that work. Interesting read.

What I did not understand about your system - how would you use it for a currency of any sort?
Everybody can create a coin as they like, as far as I understood, so therefore there is no trusted supply of tokens / coins.
Or the other way around: if you don't trust the double spending database, because its a central instance,

you surely couldn't trust a central issuer to issue and redeem. How would a currency work otherwise? Would you use it for a mutual credit system in which the transactions are shown online?

Cheers,

Joerg

- ▶ Reply
-


Permalink Reply by Sepp Hasslberger on February 18, 2009 at 14:41

I have two questions, Satoshi.

the first one ties in with Joerg's doubts about the trusted supply of tokens/coins.

As far as I understand, there will be a limit of the total amount of tokens that can be created, and a changing gradient of difficulty in making the tokens, where the elaboration gets more and more difficult with time. Is that correct?

It is important that there be a limit in the amount of tokens/coins. But it is also important that this limit be adjustable to take account of how many people adopt the system. If the number of users changes with time, it will also be necessary to change the total amount of coins.

Is there a formula to decide on what should be the total amount of tokens, and if so, what is the formula?

If there is no formula, who gets to make that decision and based on what criteria will it be made?

I will keep my second question for later. One thing at a time...

- ▶ Reply
-

Permalink Reply by Satoshi Nakamoto on February 18, 2009 at 20:50

It is a global distributed database, with additions to the database by consent of the majority, based on a set of rules they follow:

- Whenever someone finds proof-of-work to generate a block, they get some new coins
- The proof-of-work difficulty is adjusted every two weeks to target an average of 6 blocks per hour (for the whole network)
- The coins given per block is cut in half every 4 years

You could say coins are issued by the majority. They are issued in a limited, predetermined amount.

As an example, if there are 1000 nodes, and 6 get coins each hour, it would likely take a week before you get anything.

To Sepp's question, indeed there is nobody to act as central bank or federal reserve to adjust the money supply as the population of users grows. That would have required a trusted party to determine the value, because I don't know a way for software to know the real world value of things. If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that.

In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value.

- ▶ Reply
-


Permalink Reply by Sepp Hasslberger on February 20, 2009 at 8:53

So in other words, "the early adopter finds the worm" in this system.

This would mean that - the earlier someone gets in on the bitcoin system establishing a node, the more chance they have of becoming lucky and being able to generate coins. Nothing against that, it would work to promote adoption of the system.

However there should also be a method of adjusting the total number of coins extant. I would propose to link the total number of coins to the number of active nods.

This way, you have two parameters that keep a balance. One is the halving of coins given per block, the other is a continual (or periodic?) adjustment of the target total of coins to the number of active users. That should self-balance the system.

The reason balance of the system is important: if it's going to be used for payments, you don't want to have large changes in the value of the coins. It would lead to distortions, I believe, by continually increasing the "purchasing power" of a single coin.

Stability of the coins' value is desirable for long term use.

- ▶ Reply
-

Permalink Reply by Russ Nelson on March 15, 2010 at 17:27

The London Mint was unable to make enough small coins in Isaac Newton's day. Private minters stepped in. If bitcoin can't make enough coins and small enough coins so that people can trade at the value they want, then it will be replaced by something that can.

- ▶ Reply
-

Permalink Reply by Jost Reinert on January 7, 2011 at 10:23

Quite interesting project. I am curator of a micro-currency in Germany called Rheingold.

It is based on cash. Therefore the problem of "trust" is not solved. However, we do not have a central bank giving money as credit, but here, every single issuer of his own money gets it printed himself. So Rheingold is rather a group of many de-central-banks. Therefore the seignorage everybody gains himself.

And our money is debt-free.

I would like to promote your project on our blog http://rheingoldblog.wordpress.com. Maybe you could even become Rheingolder yourself with your own cashbill. Since we pretend to be an art-project, the whole project will be shown in a museum in future. We already have more than 1.000 members, mostly in Germany. Our website http://www.rheingoldregio.de

Any idea about a cooperation?

- ▶ Reply
-

Permalink Reply by Robert Searle on March 20, 2010 at 11:08

As far as I can understand it we are dealing here with another glorified form of LETS, or CCs in electronic form ofcourse. The question is this. How will this help to change the big issues of our world such as global warming, food security, population, et al? This is what really matters at the end of the day. Moreover, whether we like it, or not ,we still have to deal with the "big boys" (ie. governments, corporations, banks,et al) at some point.

Ofcourse, if most people were to accept a new decentralised "made up" currency (sans banks,and bankers)then we would
have something serious to discuss about!!! As far as I am concerned energies would be better spent in improving my project known as Transfinancial Economics.

- ▶ Reply
-

Permalink Reply by Russ Nelson on March 22, 2010 at 21:08

No, nothing like LETS at all. LETS is book entry for one, and for another the total amount of currency is always zero. When you issue a credit to someone else because they've done something for you, you receive a debit. The trouble with a LETS is that you can walk away from an account which is in debit. That functions to inflate the currency -- more people have credits who want something than there are people to do or sel something for the credits.

LETS was invented by somebody who doesn't understand money, and promulgated by more people who don't understand money.

- ▶ Reply
-

 Permalink Reply by Michel Bauwens on March 24, 2010 at 7:14

Dear Satoshi,

Could you propose a text for our regular p2p blog, with eventual responses to the main questions here? Our regular blog has a lot more readers (about 10x) than our Ning community blog,

Michel