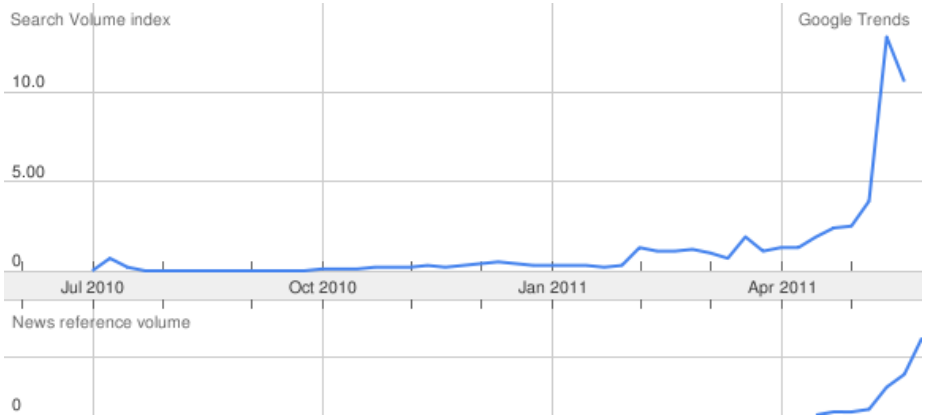
Bitcoin, lure or cure

Many people got attracted to bitcoin the last couple of months. This explosion of interest probably caused the monetary value of bitcoins to show the same shape as the google trend-line chart pictured below.

In this article I will ignore the exponential increase in monetary value since its inception and focus on some intrinsic properties of bitcoin and why those are valuable as such.

The sudden interest in bitcoin is not coincidental in my opinion. The bitcoin *ecosystem* tries to solve a number of problems with the current systems of trade, currencies and the economical structures in general we have in place for them, like our national banks, the currency and stock exchanges and the IMF. The last couple of years we have been confronted, sometimes in very painful ways, with the shortcomings of those systems and, not in the last place, the shortcomings of the people involved; all of us.



The financial crisis is obviously a complex issue and no single cause can be determined. Whatever these causes are however, they have provided a trigger for many to look for alternatives to create wealth or, more important, create ways to hang on to wealth, especially if there is not a lot of it to hang on to.

For the rest of this article I'm going to assume you know how bitcoins work. You will not have to be an expert in economics, cryptography or computer programming, but a basic understanding of the workings of bitcoin will be

necessary. The websites http://bitcoin.org en http://weusecoins.com are good starting points. Some of the points below won't make sense if you do not have at least a rudimentary understanding of how the system operates.

The trust issue

Most people will worry (a lot) if they have money issues. This alone dictates that you absolutely want to trust all parties involved with handling your money.

These parties include the people you receive money from, like your employer, the local banks you trust to keep your money safe for you, the government which monitors the usage of it, but also the 'coins' that represent the money. All of these need your continued trust, and that is a lot to ask. Especially if things do go wrong at times.

Employers need your trust that they possess enough of the 'stuff' to be able pay you for work, local banks need your trust so you let them keep your savings, governments and central banks need your trust that they won't screw up (by printing too much money for example) and the coins also need your trust that they are the real deal. All of the examples in some way betrayed our trust in the past. That has an effect on people. It may not be visible for a while, but broken trust *sticks*.

Bitcoin tries to address some of the trust issues people have; I think it was one of the main motivations for creating a system like bitcoin. It does this, amongst other things, by shifting a few of the trust items from people/institutions to verifiable technology.

For example, instead of trusting a bank to verify transactions to be valid, because they are the only party who can oversee all transactions, trust is placed in hashing techniques to demonstrate that, for example, double spending is very, very unlikely. These techniques are easier verified and proven to be right than the bank which is now responsible for it, if only because we don't have access to these verifications. The major goal of both verifications is to prevent the same coin to be spent multiple times. (fraud)

Another trust shift is the 'keep-save' mechanism. If you keep your savings on your savings-account at your bank, the combination of the banks trustworthiness and, should that fail, the (limited) guarantee the government gives on your savings makes that you can feel comfortable on parking your money there. With bitcoin, your trust will be in cryptographic tools and *the network* so you keep all your savings in a computer file. The mechanism you could use to keep it safe is to encrypt that file and spread it all over the network to many places

to minimise the chances of losing all copies of it. There is no-one to trust but yourself, but there's also no-one which can protect you in case you screw up yourself.

Distance is not important, value is

Another property of the bitcoin system, not unique to it but especially well implemented I think, is the way it makes the distance to receivers irrelevant and allows value to be put to use effectively. I'll give an example below.

Say I want to transfer 2 euros to someone which is in a country far away from mine. The amount of time and money it takes to get this modest amount into the hands of that someone distant is ridiculous in the current financial system. My bank does provide a service but it will cost me at least 10 euros, double that amount if I want to get it done 'fast'. Fast, in this case meaning within 24 hours! For larger sums, the cost may be acceptable, but for small amounts both time and cost are ridiculous.

There are many services which try to solve at least part of the problem outlined above. Services like paypal with on-line accounts to make things go faster, or proxy companies which gather up all the small amounts and transfer to the real supplier when things have piled up. Up until bitcoin I did not encounter a service which chose the simplest concept for this problem: "Set up a secure, verifiable, immediate non-refundable transaction between the involved parties."

I do not believe the technology to do this has not been available to banks and/or credit card companies, so that can't be the reason they have not implemented a cheaper and more efficient system. It's not very hard to imagine what their reason is though. Distance used to be a major hurdle, it is not anymore.

The key differences bitcoin provides here are:

- the receiver and sender communicate directly, trust is a lot easier to maintain if there are less parties involved. "No middle man needed, nor wanted"
- the 'act' of payment is almost immediate, the receiver can check almost immediately that a transaction has been made. (Verification for validity by the network can take a while though) In relation to the 24 hours described in the first paragraph this can certainly be considered very fast, near *real-time*
- a transaction fee is optional. If you specify one, you make it more attractive for others in the network to check your transaction and have a go at collecting that fee. If swift transaction handling is not important, but transferring, say 0.05 euro, to a certain person **is** important, bitcoin is about the only way I know to do that effectively.

Remember, the amount of 0.05 euro may not be much to you and me, but there are parts in the world where it can buy you a meal or a bottle of water. The fact

alone that bitcoin makes these kinds of transactions possible is enough reason to give it more than a casual look.

Bitcoin increases the value of my € 0.05 by allowing effective use.

No unreasonable control

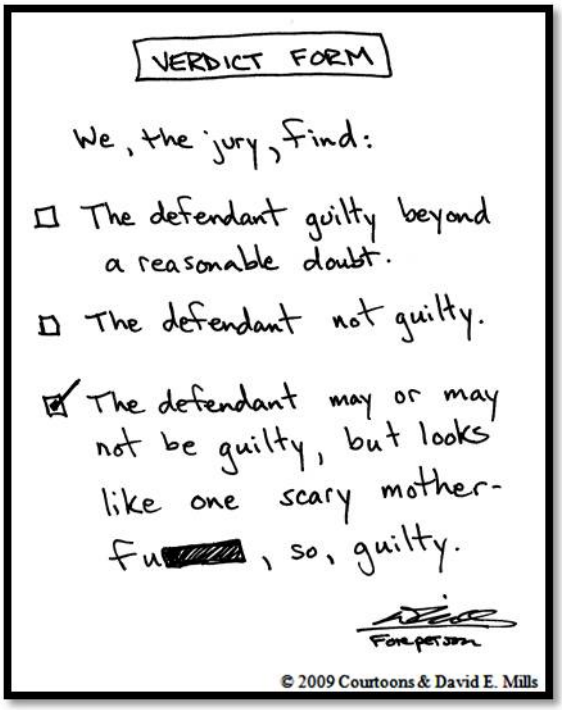
It's probably true that bitcoin, or systems like it, scares financial companies and governments and therefore will have a rough time ahead. This scare is in part caused by a fear of decreasing control over the system compared to the *classic* system. Almost all economic commentators or government representatives will argue that 'some form of control' is needed to correct and stabilise the system. I'm not very convinced of that being effective or wanted anymore.

Recently, the unreasonable control over money flow in the wikileaks dry-out attempt confirmed this once again for me. It doesn't really matter if companies like mastercard and paypal decide not to handle transactions for wikileaks themselves or that they have been put under pressure to do so. The fact that it happens shows they have control over where I spent my money. I don't want that. Bitcoin offers a system where this type of control is impossible by means of the system itself; personal threats will be effective I'm afraid with any system.

Next to the self-control over spending purposes, anonymity is also important for some people. The example often used, mostly in critical pieces on bitcoin, are criminals. Bitcoin makes it possible, when used in certain ways, to bring money from A to B without exposing identities to each-other and to third parties. This is obviously attractive for criminals, including people who want to evade taxes. This is a valid concern and should be addressed properly, but I don't think it has anything to do with bitcoin as such. With regard to **this** aspect, bitcoin has no other properties than cash, it's just more effective and easier to use than exchanging bits of paper money. The real use-case here is the non-criminal people who want to perform semi-anonymous transactions for valid reasons.

So, what's the verdict?

Bitcoin is a good idea, generally speaking. From a technological viewpoint it's excellent. It's trivial that libertarians and anarchists will be attracted by bitcoins, we don't need to argue the case for them. The challenge is to present the extra-, not the replacement-, values of bitcoin for all the other people out there. I have touched on three of the most important ones to me. There are more properties which make it very attractive as an alternate choice for exchanging value.



There are really three possible verdicts.

Many 'digital cash' systems have been presented before bitcoin, but for all of them I could point out critical weaknesses within a very short time. For many of them this was not even a technical weakness, but an organisational (like a paranoid initiator, looking for patent protection) or an economical issue (creating a metal backed currency in the hands of a private company). With bitcoin there are certainly weaknesses in the system, but I have not been able to find a critical one upfront.

The goal of bitcoin is not necessarily to take over existing currencies or existing financial systems, although I would love to see that play out. I would like it to augment the current systems with new ways to trade, more effective ways to put wealth to use, more transparent ways to work together. It needs to put banks and governments on the edge of their seats and keep them a lot more aware of their obligation to reasonably deal with their control over over money.

Having a transparent, technologically sound system for exchanging value is in the interest of many. I'm sure bitcoin has many things that can be improved. Its its complexity of use and the rather clumsy exposure of meaningless addresses come to mind, but the foundation is solid and the issues I found are by no means critical or unsolvable. The fact that bitcoin, the program, is open source does help to understand and validate the system and thus gain my trust. This contrasts on many levels with the services offered to me through financial companies.

When was the last time you validated your bank's software?