the blockchain

Our submission to more automation and control, or the path to a more free and decentralised world?

Authentication by computers has traditionally required a centralised, one-to-many topology. A bank, for example, might hold a database of its account holders' personal details and use it to verify their identities. Passwords cannot be checked by just anybody because storing them in multiple locations would make it possible for a single user to have several different passwords. Decentralised, peer-to-peer interactions on computer networks are possible, but have typically been limited to things where trust is not important.

This is now changing. Banks, as we know them, could become obsolete. But will it empower us?

what is the blockchain?

The blockchain is a distributed public transaction ledger, originally developed for the bitcoin cryptocurrency. It consists of an indivisible chain of timestamped 'blocks' of transactions, each of which contains a hash of the previous block.

Put simply it is a method of authenticating an individual entity over an untrusted network. This is done by keeping a ledger which is stored on many computers and continuosly accessible to all, and, in the case of bitcoin, timestamped by a verifiable 'proof of work' system. 'Proof of work' refers to being able to demonstrate that an amount of computational work has been carried out, requiring time and computer resources. Each block is a function of the previous block in the chain, so in order to change something one would have to re-compute all previous blocks. If there are differing blockchains available, meaning that one of them could have been maliciously changed, the longest blockchain is assumed to be the correct one. What this means is that the system assumes that the majority of the system is honest, and the only way to undermine it would be to have more computer resources than the cooperating majority. Rather than trusting the bank, you trust the majority of the network.

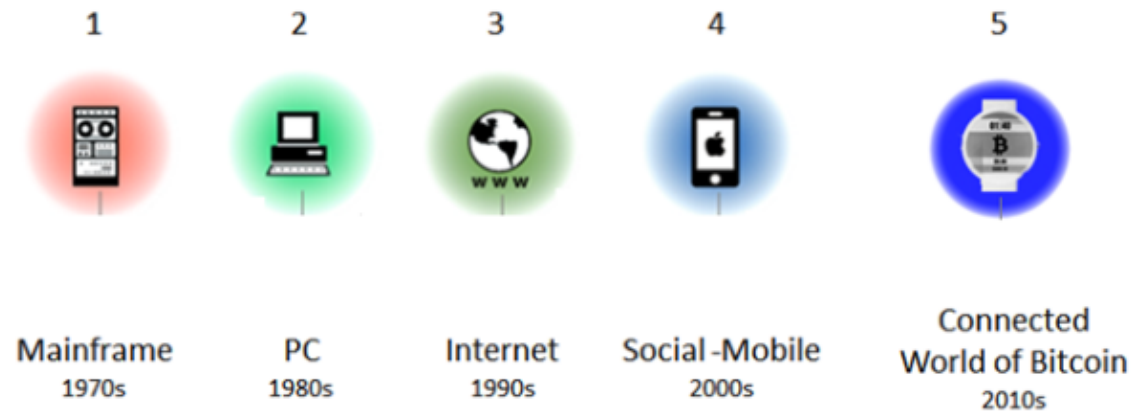
However, remember that the majority means the majority of computer resources, not majority of people. Of course it would be much better if it was the majority of people. This means there is the possibility that a superpower such as the US government might secretly have the computing resources to break the blockchain.

Or if they dont already they might think about getting such a computer. But a long as there is a financial incentive for mining and a growing number of users, we have a good chance in this strange battle.

The blockchain, as an authentication technique combining a distributed ledger with a proof of work verification system, solves a longstanding problem in computer science, thought by many to be unsolvable. It is known as the byzantine generals problem, specified by Lamport who imagined military generals camped at opposite sides of an enemy city trying to plan their attack by sending messengers. The messengers might be traitors giving incorrect information and the problem is to find the best way to interpret messages given that the majority are cooperating. Bitcoin is thought to be a solution to this problem, offering a verification system which is resilient to a certain level of corruption.

The blockchain is undoubtably an important technological breakthrough, and has potentially very many applications. Bitcoin is the original project using this technology, a distributed cryptocurrency. At the time of writing the bitcoin blockchain is the most widely used by far, although others now exist with various modifications, and it is quite possible that another will in the future prove to be more popular. The most notable emerging blockchain project is Ethereum, which is designed to be a distributed development platform, sometimes called the universal computer. Ethereum extends the application of the blockchain to authenticate not only transactions of currency, but to programmable contracts of unlimited complexity. Although the bitcoin currency has the potential to make a dramatic social impact, Ethereum takes things a big step further, and is thought by many to be a technology which will disrupt all areas of society. Ethereum's stated purpose is to decentralise the web. A decentralised topology is in its very nature, and although some believe it will be slow and impractical to use for certain tasks, the project is gaining a lot of interest. More recently another public blockchain project has begun, the 'Open Ledger Project' backed by the Linux foundation as well as IBM and other major players in the IT industry.

As interest in blockchain-based systems grows, many companies are rushing to become involved in it. Rather than seeing it as a threat they want have control it. Because of this we have to be cautious. There are many technologies which have the potential to be liberating and useful but in practice become part of a system which is competitive, individualist and environmentally destructive.



Melanie Swan thinks the Blockchain will be the game-changing technology of the decade.

Bitcoin

There are several good texts and books about cryptocurrencies and the story of bitcoin and its psudoanonymous creator, which place it in the context of the history of monetary systems. Putting it into this

context makes it not seem like such a wacky idea, or rather its not so wacky compared to the financial system we currently use. Fiat currency can be limitlessly created by banks, devaluing the money we have, meaning that by having our savings in fiat currency we put our trust in the banks. Bitcoin however has a fixed, finite supply.

Fiat currency is backed by governments and their militaries. Bitcoin is not backed by anybody. Its behaviour is determined by software that is published for all to see. You do not need to trust anybody to use bitcoin. Although many are sceptical as to whether it poses a genuine threat to banks, it is an undeniably significant achievement in the struggle of people against banks, the worlds most powerful institutions.

Because of the initial media hype around Bitcoin, it can be difficult to know whether to take the project seriously. It is not until one gets an understanding of how genuinely decentralised such a system could be, to have a secure method of authenticating payments between psudoanonymous individuals on an insecure network with no trusted third party, that it becomes clear that there is really something innovative here. Not just a new media buzzword but a tool that we now have which was previously unavailable. Just as the popularisation of encryption software such as PGP/GPG opened a new possibility for people far away from each other to communicate in secret, the blockchain lets us do things we couldn't do before.

Dominic Frisby uses the Rai stone currency used on the island of Yap as a way to explain the idea of bitcoin. On the island, beautiful Rai stones are exchanged for things. Some of them however, are too big to be moved, and stand at various places around the village. These big stones are not exchanged very often, but when they are, it is the talk of the town, and everybody knows who the stone now belongs to even though it has not moved. This could be compared to the public ledger of that is the bitcoin blockchain. Who-owns-what is stored on many different computers and is continously viewable, making the system very difficult to undermine.

Environmental concerns

Environmentalists have raised concerns about bitcoin mining. The financial incentive means that many people run powerful computers solely for the perpose of bitcoin mining. A considerable amount of electrical power is 'wasted' on verifying the blockchain, and there is no way around this as the 'proof of work' system relys on this expenditure of computing to demonstrate it was produced by a collaborating majority. One potential solution to this problem would be to use this heat produced by this computing for other things. One of the difficulties in running large Bitcoin mining computers is keeping them cool. So they could be used to heat water for example. We could have computer kettles, heaters and boilers.

However, even if this expended heat is utilised, it is still a major disadvantage, especially if we imagine to become independent of coal, nuclear, and the commercially controlled electricity grid. It seems we must find an alternative to the proof of work system.

Advantages of micropayments

One of the major advantages of bitcoin over traditional payment systems is the possibility to transact tiny amounts which are only significant cumulatively. Transaction fees associated with credit cards and bank transfers make small payments not worthwhile. Nakamoto points out that it is the possibility to reverse the transaction which makes conventional payment systems costly and uncertain, requiring trust and mediation from a third party. Physical cash transactions are unreversable, making them practical for small, casual transactions. Bitcoin was designed to be the electronic equivalent.

Wider applications

The blockchain could be used to authenticate the ownership of assets such as land, property, cars, intellectual property, as well as more complex applications such as automatically enforced 'smart contracts', for example renting or borrowing , a work contract, marriage, etc.

Being able to, for example, buy a house without any mediating authority could potentially have dramatic social implications. Cutting the 'middle man' out of internet-based interactions, changing their topology completely, to direct interactions between peers, and pulling power away from governments and institutions.

Some imagine this to mean that we could effectively work for computer programs instead of having a human as our boss. A robot boss who always follows the rules exactly and who does not need to be paid. This sounds both utopian and extremely dangerous at the same time.

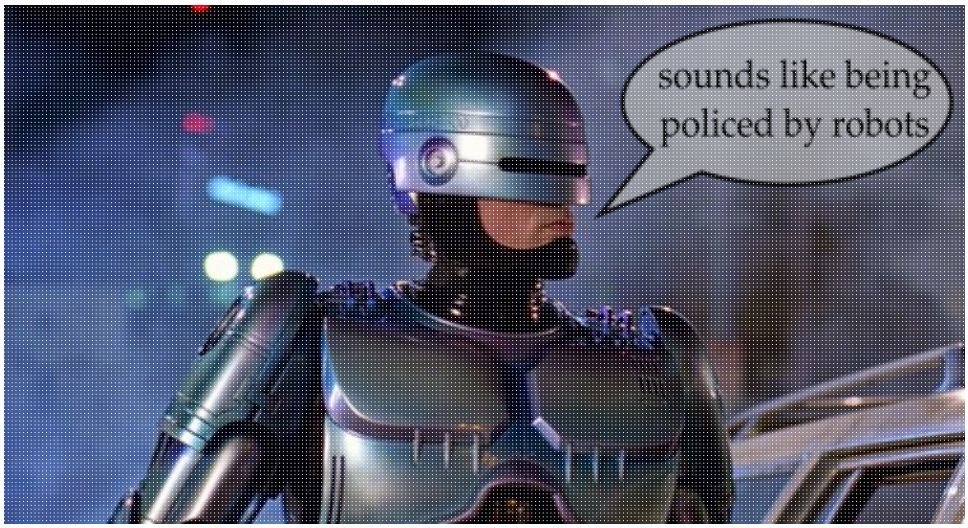
Many aspects of today's 'work' rely on paying someone just to be accountable, trustworthy and secure. This can now be automated, perhaps in a cooperative way, where corruption is visible to all. Thus pulling the rug from under the feet of many office workers, particularly in the areas of finance and law.

Ben Schreckinger claims there is a blockchain-based equity market emerging which will mean that stock exchanges and various other financial institutions loose their importance. He says that this will be considerably more socially disruptive than the adoption of bitcoin as a currency. It seems that many financial, governmental and other powerful organisations stand to loose their power and significance because of blockchain applications, and Schreckinger thinks regulating authorities are cautious to intervene for fear of being less 'progressive' than governments in other countries, and thereby loosing the edge internationally.

Security culture

It could be that 'smart contracts' while very secure from a technical point of view, could be exploited by loop-holes in their design. Melanie Swan uses the example of a grandparent using a smart contract to give an inheritance gift to a grandchild either on the 18th birthday of the child or on the day of the death of the grandparent. The death could be verified by checking some kind of reputable online newspaper orbituary or a registry of death, which perhaps only doctors are able to modify. It is easy to see how one might try to think of ways of tricking the system, and so extra levels of security are required to, for example, verify the identity of a doctor.

Another example is the idea of a 'smart' car which is bought on credit which will not start if repayments are not kept up. We can imagine other oppressive mechanisms being put in place as more control of different aspects of our lives are computerised.



Ethereum would also have applications for machine-to-machine interactions, often called the 'Internet of Things'. For example, one driverless car could compensate another for allowing it to overtake or take a less direct route.

More automation and more security culture does not seem to be a step in the direction of a more free and autonomous society.

Projects

OpenBazaar

The OpenBazaar project aims to create an online market (like ebay) which has no centralised server, it consists only of a network of individuals running the OpenBazaar software to buy and sell items from each other. The rules and regulation of how it works are determined only by the software itself, which is of course open source, making it considerably more democratic than systems like ebay. Although slightly more tricky to use than ebay, as the software must first be installed, the obvious immediate advantage over ebay is that there are no fees. This makes it possible that it will gain popularity very quickly, and its decentralised nature makes it very difficult to regulate in any way.

Also decentralised projects for announcements more similar to Craigslist, have been proposed.

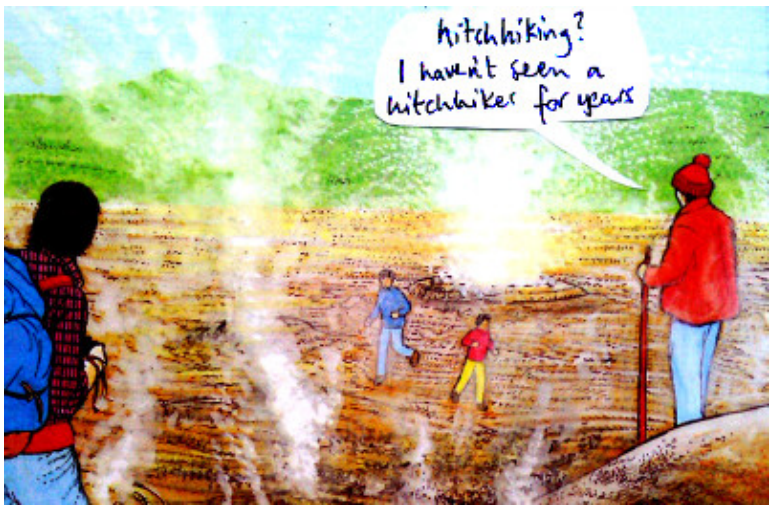
Liftsharing

Blockchain-based peer-to peer liftshare software has been proposed. This is something much needed. There seems to be a trend in european liftshare websites that they start out by allowing the driver and passenger to directly communicate for free, and payment to be made directly by putting cash in the hand of the driver usually at the end of the journey (covoiturage.fr, mitfahrgelegenheit.de). They become very popular and then introduce a fee and some regulation system which makes it supposedly more 'trustworthy' but also very inconvenient, requiring verified registration, credit card payment, etc. Then nearly all the users move to another website which is less regulated and at some point the same thing could happen.

This looks like a job for the blockchain. The only reason we use these websites is because everyone else does - the more popular a site is, the likely you are to find what you need. Whats we need is for the users themselves to talk directly to each other, removing the mediating third party.

An american software project called 'lazooz' proposes a decentralised liftshare system which aims to work in a more ad-hoc way than current systems. Currently most liftshares are organised a day or two in advance or at least a couple of hours before. With lazooz it is possible for potential passengers to be notified when a car driving in the direction they want is physically nearby. This gives the possibility for a much more spontanous liftshare system, where you can simply go when you are ready and not have to wait for a fixed appointment. One of the annoying things about taking liftshares as opposed to having your own vehicle is not being able to be flexible about when you are going somewhere.

However, this system, although it might represent a technological breakthrough, is basically a complicated way of organising hitchhiking. Does this represent a loss of trust, a loss of community, that we would only let a stranger in our car if the computer tells us to? Or is it an effective way to share costs and potentially create a decentralised public transport system?



We could extent the liftshare idea to an 'almost punk-post' system. Punk post is a genuinely anarchic postal system where you give someone a letter or package who is travelling in the direction of the recipient and they pass it along. It requires a lot of trust. In a blockchain-based system however, 'micro-payments' could be given to add incentive, and items could be tracked. You only need to move the thing a part of the journey, which maybe you are making anyway, and put it in a safe place or pass it to someone else, a step in the direction of where it needs to go. The blockchain makes you accountable for things while they are in your hands, and some kind of conflict resolution system could be devised for when things go wrong. So we could have a decentralised delivery system. It would still involve money, but there would be no centralisation, nobody in charge.

This could be extended to some logistics/distribution system. You could drive around in a vehicle (maybe your own, maybe hired, or maybe it comes as part of the collaborative distribution system) and pick up a load if it is deemed to be cost-effective to transport it. There could be some regulation and accountability system built in to the software. The software is your boss. If you don't like the rules, you can make a fork of the project and start a new system. But the new system will have to gain acceptance by others in order to be useful. Also, infrastructure such as vehicles, storage space or staff-facilities, belongs to the current distribution system itself, meaning the new system will take a long time, or have to be really a lot better, in order to become widely accepted and thus useful. Alternatively you could propose a change to the system you are using. How this works depend on the kind of open-source license the software has. Since a change would

effect a lot of people there would likely be some kind of regulation system. Although it is genuinely decentralised, this seems slowly less anarchic than our original idea. Would you really rather work for a robot boss?

Distributed digital storage

Ethereum has a blockchain-based distributed storage platform called Swarm, where users can host content in a decentralised way, making it resilient to censorship, commercialisation or other kind control by a centralised organisation. This appears similar to other decentralised content hosting projects such as 'ipfs', 'maidsafe' and 'storj'.

Ipfs (Interplanetary Filesystem), although criticised for being inherently unreliable, seems to have some very promising properties as a universal decentralised filesystem, and potentially a replacement for the web. Information is retrieved by a content addressing system, meaning popular files are faster to find, network traffic is reduced, and censorship or anyother kind of centralised control is impossible. It also has a Git-style revision control system, meaning older versions are not lost.

Distributed crowdfunding

Also using the name 'Swarm' is a crowdfunding platform which uses blockchain technology to sell equity to individuals wanting to help a project. Co-founder and CEO Joel Dietz speaks in an interview about wanting to disrupt the financial system and to empower people. He has also appeared on an anarchist webcast program 'anarchast' and said that his influences come from studying early chinese philosophy. The crowdfunding model differs from other projects like kickstarter in that investors have a financial incentive, more like shareholders. Selling these equity 'tokens' seems to be a legal grey area. Swarm promotes an alternative model for business which it calls 'Distributed Collaborative Organisations' (DCOs). Among the projects using the model is an e-health platform, 'Pointnurse' where patients can pay to contact a nurse over the internet.

While these businesses might operate in a more decentralised way and rely less on institutions, they promote casualisation of labour which can dehumanise workers, they are used like tools which are only needed in certain economic conditions.

open source design process

Using open source principles as a way of designing regulations which control our aspects of our lives is supposed to guarantee transparency and a system that everyone is happy with. If there is something you do not like you can 'fork' the project, making your own modified version of it, and in principle if you have made a genuine improvement, the forked version will gain more popularity than the original. These prinicples become more significant as software applications drift into wider areas, replacing legal structures and regulations.

What about software which favours individual users to the detriment of others? In many torrent clients it is possible to change a setting to become greedy, downloading from others but not allowing uploads. If everyone did this the system simply would not work. But of course somehow it does work.

trustless interactions

Do such 'trustless' systems represent a loss of genuine trust between humans which was once the very basis of our communities? Trust is usually built on social activity, spending time together, communicating, building emotional attachments that mean we care about each other.

Is it the case that we need this because our 'communities' have got way too big for trust or 'community spirit' to be possible? Is there a critical mass by which a society become to big for trust to come naturally?

Is there not something beautiful about genuinely trusting random people?

Compared to a moneyless utopia built on genuine community, the blockchain does not seem so great, and maybe if you have already found your way to such a community you should stop reading this. But for those of us who begrudgingly use systems which rely on a centralised trusted party, the blockchain could to some extent turn the tables on who is controlling these systems. Potentially we could create cooperative alternatives to banks, insurance companies, and many areas of government. But we are not the only ones interested. Like the internet itself, the blockchain will most likely become riddled with commercial projects.

The blockchain allows us to collaborate with a wider group of peoples as we are not limited to those we know or trust. For example we can borrow something from someone you have never met while remaining accountable, with a mechanism for resolving disputes which doesn't not rely on anything centralised.

Collaborating with a group big enough to safely pool a considerable amount of money between each, without the limit of needing to be a critically small enough group that they can all know each other well enough to give such trust. Money would not sit in storage but dynamically and effortlessly flow around to where it is currently needed.

But would this actually abstract the whole purpose of money? An abstraction of the same sort which gave rise to the financial crisis - imaginary money being pushed around? Bitcoin was developed as a response to this ridiculous situation.

Bitcoin, with its transparent underlying mechanism, remains something inherently more solid than fiat currency, where banks can limitlessly create more money, thereby devaluing our existing money.

Maybe this 'limit' of needing to know each other, of emotional contact, of human touch, is the communication tool which really binds our communities. Can we really share resources if we dont really understand each other?

It would be nice to think that a total abstraction of money brought about by such wide scale collaboration between individuals, would form part of a path towards removing the significance and importance of money in the minds of its users. Which could be the key to transforming this competitive and individualist society.

On the other hand it might just mean more time sat at the computer while our problems of food distribution and access to land remain unsolved.

http://ameba.ehion.com

References

- Cox, James - Bitcoin and Digital Currencies - The new World of Digital Freedom
- Frisby, Dominic, Bitcoin - The Future of Money?
- Lamport, Leslie, Robert Shostak, Marshall Pease, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems 4 (3) (1982): 382401. http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf
- Nakamoto, Satoshi, 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." http://Bitcoin.org/Bitcoin.pdf
- Schreckinger, Ben - Bitcoin vs. the SEC (Politico magazine article) http://www.politico.com/agenda/story/2015/04/bitcoin-money-stock-market-000026
- Swan, Melanie, 2015 - The Blockchain
- Wood, Gavin - Ethereum: A secure decentralised generalised transaction ledger