Totalizing a Partial View

Jacob Hjortsberg
May, 2019

Bitcoin is the world's first and most successful digital currency. It is based on a protocol that was first proposed in a white paper authored under the pseudonym Satoshi Nakamoto – to date the identity of the author is still unknown. The main

technical problem that the paper solves is the so-called “double-spend problem”, which up until that point had stood in the way of any decentralized digital currency. The problem is this: If money only exists as digital information in online bank accounts, what stops a person from spending the same amount of money twice? While physical money for obvious reasons makes that impossible, there is in principle nothing stopping digital money from simply being copied and added to two different accounts, at the same time. Nothing, after all, is ever “transferred”. Therefore, a so-called “third trusted party” is needed to keep a ledger of all transactions that are made, to make sure that money is never spent twice. Usually, this is done by banks.

Bitcoin’s revolutionary innovation is to do away with the need for a trusted third party. Instead of entrusting banks to keep private ledgers of all transactions that are made, Bitcoin operates a public ledger that is kept and maintained by all users collectively. So how does it avoid money being spent twice? This is where the Blockchain enters the picture. In order for a certain transaction to become a part of the public ledger – and thereby confirmed – it has to be bundled together with other transactions in what is called a “block”.

> *Each new block is connected to the previous one, together forming a chain that goes back to the very first transactions ever made. The people who create blocks are called “miners”, since the successful creation of new blocks releases new Bitcoin to its creator; this is how new Bitcoin are created.*

The process of creating a new block, however, is not easy. Bundling together new transaction into a block results in the creation of a “hash”, a specific value corresponding a) to the information contained in the new block and the one before it, and b) to a random number called a “nonce”. The hash is the answer to a mathematical equation resulting from the combination of these two values (the blocks and the nonce), but the miners only have access to half the information and have to find out the nonce value on their own. Due to the complexity of the equation, the nonce can only be figured out by repeated guessing – often millions

of times.

Stickers on display at the Bitcoin Embassy in Tel Aviv. Photo by Matan Shapiro.

The chance of figuring it out first, and thus being rewarded with the new Bitcoin that is given to the one updating the Blockchain, is therefore determined by the processing power of the miner's computers, and the system is set up in such a way that the more processing power is applied over the whole system in trying to guess the hash, the harder the equation gets – in general, it should take about ten minutes for a new block to be generated. When a new block is created, all other users can easily determine if it is valid, because while it is difficult to guess the nonce, it is easy to determine if it is correct – all one has to do is test if it results in the proper hash. When the validity of the new block has been confirmed, all miners start working on creating the next block in the chain, and so on. In this way, the system constantly produces a consensus regarding the current state of the ledger/Blockchain – a *single source of truth* that the whole system has agreed upon.

To a large extent, Bitcoin was developed in response to what was seen as the excessive power of central banks and governments to control currencies in their favour, specifically following the policies of the 2008 financial crisis when big financial banks were bailed out, leaving thousands of people in severe financial hardship. What many Bitcoin advocates argue is that, in a globalized world where digital currency is unavoidable, it should not be controlled by centralized institutions that have to be "trusted" not to misuse their power.

> *Trust, after all, signifies that the relation in question is open-ended, not governed by necessity but human will.*

One very vocal supporter of Bitcoin, Stefan Molyneux, has for example argued that this technology, if implemented universally, will put an end to wars, as wars are financed through money printing by governments controlling fiat currencies – as a point in fact, he argues, the gold standard was abandoned in order to finance the Vietnam war. Therefore, a shift to peer-to-peer based decentralized currencies like Bitcoin, he claims, will once and for all put an end to oligarchic money power, giving power back to the people.

Leaving aside the validity of these proclamations, it's interesting to note that Bitcoin in this way has a certain ideal-type vision of the free market written into its code. Whatever problems there might be with the free market, according to Bitcoin enthusiasts, those problems are understood to be external to the market logic itself – governments and central banks misusing or exploiting the "trust" that (unfortunately) have to be put in them in order to constitute market logic. Bitcoin solves this problem by replacing trust with cryptography. Typically missing from this picture, then, is class – by which I mean concentrations of wealth that arise out of market competition, but also undermine it. Instead, from the point of view of this technology, the "freedom" of market exchange is only ever subverted by excessive government control coming from the outside, and never concentrations of private wealth within the market system itself.

Now, while this particular vision of the free market is not new, and indeed has

been debunked countless times – perhaps most powerfully by Polanyi and Marx – what's new about Bitcoin, it seems, is that it manages to turn this misrecognition of market logic into the only recognizable reality. That is, in seeking to realize "pure" market logic as envisioned by neoclassical theories – which according to Bitcoin advocates has always existed as something of a supressed reality – Bitcoin actually represents something entirely new: a market logic that is able to constitute itself. In this way, while the dichotomy between states and market has up until now only been a phantasmagorical projection from the partial point of view of markets, Bitcoin represents *a technological means of totalizing this projection as real*.

> *Rather unsurprisingly, Bitcoin has been unable to do away with private concentrations of money power. It has, however, transformed the ways in which such concentrations emerge, and how they are organized.*

Soon after Bitcoin was launched, individual miners realized that their chances of mining new Bitcoin would increase if they coordinated their computational power into so-called mining pools. Most of the new Bitcoin that is mined today is mined by such pools, the majority of which operate from China where electricity is cheaper. Currently, no one mining pool controls the system (i.e. control more than 51% or more of the processing power), yet they have severely reduced the possibility for individual miners to update the Blockchain.

While Bitcoin has in this way not been able to avoid accumulated money-power from controlling large parts of the system, it has been able to severely reduce the possibility of anything resembling economic class struggle. For this reason, it might be worthwhile to consider what it is that Bitcoin actually replaces, or seeks to replace. I noticed that, for many of its advocates, the main point about Bitcoin is to get rid of the element of "trust" in maintaining market rule. On closer inspection, however, this appears like a rather dubious formulation.

Is the relation between banks and citizens really one of trust? The answer ultimately depends on what one means by the term. Still, it would seem that

regardless of definition, if we say that we “trust” banks, we will have a different dynamic in mind than when we say that we trust our friends. In fact, we would have to refer to two quite opposite dynamics. On the one hand, when I say that I trust a friend, this means that our relation does not need to take the form of a contract; in fact, for most people, making a friend sign a contract would be taken as *a clear sign of mistrust*. With banks, the opposite goes. Our “trust” in them is purely contractual: we trust them not to break the contract that both of us are bound by.

> *From this point of view, I believe, a better way to understand the kind of shift that Bitcoin represents is as a shift from politics to necessity.*

Rather than trust, what Bitcoin removes is *the gap or tension that has previously existed between the logic of the market and the process of establishing it.* While market systems have previously always had to co-exist with a logic that defies its principles, Bitcoin allows the establishment of market logic to be a function of market logic itself. As we’ve seen, within Bitcoin, the continual establishment of market logic, as well as the process of changing its rules, is a function of the same principles that govern market activity. Hence, while there has previously always existed a tension between the act of instituting markets and the logics of markets themselves, Bitcoin imagines a seamless relation between the two, in which money functions as its own constitution.

'Bitcoin to the Moon' at the Bitcoin Embassy in Tel Aviv. Photo by Matan Shapiro.

Still, what disappears in this process is not trust, I would argue, but rather the possibility of thinking about politics as distinct from economics. Instead of market logic being established through a process of political contingency and will – subject to various forms of collective and class based struggle based on conflict of interest (and not trust) – politics is reduced to the necessity of market logic as inscribed in the Blockchain source code.

This is interesting to note, as it speaks to a wider issue that seems to permeate many solution that go under the name "smart" – many of which are based on the same Blockchain technology as Bitcoin. This is *the fusion or integration of systems of law or rule with their actual implementation*. In Bitcoin, the integrity of money is not guaranteed by some external agency keeping track of all transaction – it is written into the money itself. What's further striking is that the Blockchain

technology can be extended back to the physical world. This is the principle of the Internet of Things (IoT).

The Internet of Things

IoT has emerged as one of the most important areas of research within "smart city" planning. What it means is putting sensors on objects in the physical world, allowing them to communicate with each other, as well as whoever has control of the information that is generated by them. We are already surrounded by such objects; the swipe cards that we use to get onto the metro is one example. As IoT technology becomes increasingly applied in cities, however, more and more objects will be equipped with sensors that determine how they can be used, and by whom. 5G telecommunication networks are primarily set-up to enable this.

Within the IoT community, this has spawned a lot of discussion regarding the relation between safety and security, a new dichotomy that partly mirrors the one between markets and governments. The idea is that, while security in the smart city means putting sensors on everything in order to detect actions that might be deemed security threats, this will imply a breach of privacy as more people than those guilty of crimes will have their every movement surveyed.

> *Like the dichotomy between markets and governments, the basic problem with this formulation is that privacy and security are not necessarily opposed to each other.*

It is not as if the more you privilege security, the more you automatically have to disregard people's privacy, nor vice versa. Instead, as many people within the smart city community actually acknowledge – typically without noticing how it clashes with the security/privacy dichotomy, however – the very lack of privacy that many security regimes involve might be a security problem in its own right, insofar as "the wrong people" might gain access to the surveillance apparatuses

that are set up in order to “protect” people.

Likewise, the very notion that security is always a matter of surveillance, and thus naturally stands in opposition to privacy, forgets that surveillance may in many cases be experienced as a form of insecurity for the people being surveyed. After all, the meaning of “security” is not necessarily the same for those who are surveyed as it is for those doing the surveying – especially not in authoritarian states like China, which has unsurprisingly been very interested in “smart city” development. Hence, what any simple opposition between surveillance and privacy will inevitably hide is the fact that the relation between the two can never be understood outside of the particular social arrangement in which both surveillance and security take on specific meaning. Whether security and privacy are contradictory or versions of each other can therefore only ever be socially determined. From this point of view, the real problem that is emerging within the smart city landscape is not that it constantly has to weigh security concern against privacy concerns, but that it seeks to resolve this issue in a technical rather than social/political way.

> *In the smart city, surveillance itself is largely becoming a matter of automation: for example, computers can now independently analyse video-feeds to determine whether or not someone or something is deemed a security threat.*

Privacy, here, simply becomes the flip side of the law, as it is codified in computer algorithms; it comes to represent the other side of the law-as-necessity. Still, what disappears here is not privacy, I think, but public life as we know it. If public life is ruled by security cameras that enforce the law through algorithms, there can never be any true social interaction, understood as open-ended relations between people whose perspective can never be more than imperfectly coordinated. After all, when law enforcement is automated, something different happens than when the production of, say, shoes is automated.

It loses something essential. Shoes were never essentially social; the law is a social relation. If its enforcement is automated, therefore, it becomes what it

never was: a thing, a necessary logic that is codified not only in writing but also in its execution as an algorithm. It can no longer be negotiated, only followed or not followed (mirroring the binary logic of the algorithms that enforce it). Within such a regime, the fact that privacy is seen as the opposite of the law is only to be expected: if the only thing that protects us is the law, the only thing that is *not* the law is a private non-social individual. The notion that the only threat to this neat opposition is the danger of "wrong people" gaining access to surveillance information, is a point in fact – it is the end of politics as negotiation, replaced by the binary and absolute logics of zeroes and ones.

Featured Image by Marco Verch (flickr, CC BY 2.0).