A weirder definition of Bitcoin

By Joannes Vermorel, CEO of Lokad, April 10th, 2018

Abstract: Bitcoin is best characterized as an exceedingly weird virtue-inducing artifact. Attempts at making Bitcoin less weird have only two outcomes: either the attempt fails and Bitcoin just becomes weirder; or the attempt succeeds and this is not Bitcoin anymore. The weirdest part of Bitcoin is probably that its own excess of weirdness can be reliably relied upon, as the author demonstrates by providing corollaries of practical interest out of the present definition. Anecdotally, it also explains why Satoshi Nakamoto opted to remain anonymous, as it is usually frowned upon to conjure exceedingly weird inventions.

Overview

The original Bitcoin article of Satoshi Nakamoto (2008) does not address how the maintenance of Bitcoin itself should be sorted out. Figuring out the correct answers to this question is of prime importance, because this process defines what Bitcoin will effectively become. Indeed, as Bitcoin is an active artifact, it needs maintenance, and thus, in the long run, some degree of inevitable change as well.

The truth behind Bitcoin seems to abide to the logic of the Pratchett universe. Anything that happens to be too exceedingly weird to be true, like Bitcoin, is, in fact, made true by the universe inclined to having a good laugh at human rationality. Furthermore, in the early days of Bitcoin, a few implausibly dubious characters managed - for a while - to tune the ambient weirdness one octave higher through courses of action that made the characters of the movie Fargo look like the pinnacle of human wisdom.

In this regard, quantum mechanics, which are also exceedly weird, set a good practical precedent for Bitcoin. As a community, the best course of action appears to be to conjure half a dozen impossibly challenging philosophical interpretations, and then enjoy the practical benefits of the truth, while carefully avoiding to think too much about it on a daily basis; to stay productive and to maintain a reasonable degree of sanity.

By gathering the insights detailed in the following, we can infer some conclusions of practical interest for the maintenance of Bitcoin:

1. Bitcoin dominantly attracts people of negligible sanity, as they are impervious to the excess of weirdness of Bitcoin itself.
2. Morally bankrupt actors cannot maintain Bitcoin because they will invariably degrade Bitcoin to the point that it is not Bitcoin anymore.

3. Honest but ignorant actors cannot maintain Bitcoin because they will invariably let Bitcoin be degraded to the point that it is not Bitcoin anymore.
4. There can be only one Bitcoin, because economic freedom is not additive. People are not twice as free because they enjoy twice the same freedom.
5. Academia has failed - and will keep failing - at recognising excessive weirdness as the defining trait of Bitcoin, because it's just plain embarrassing.

Bitcoin is best understood as an active artifact that enables a virtue-inducing social contract to emerge. The artifact has been purposefully and carefully engineered to deliver this emergent property. The mere fact that humanity can willingly decide to stand united around the emergence of a social contract brought by an artifact is an intriguing idea. Without Bitcoin as a living proof, the very existence of such virtue-inducing artifact would have been deemed implausible.

The security model of Bitcoin is not code-is-law, as certain early observers might have been inclined to think, but trust-and-verify recursively applied upon itself so that it can actually appear to be firmly grounded into something while being grounded into nothing at all. While trust-and-verify all the way down does induce some vertigo, it also happens to be tremendously efficient economically.

The continuous existence of Bitcoin is rooted in the proof-of-work; which is a very special kind of work with no provable use at all, except being the purest form of conversion of electricity into trust. However, the second law of thermodynamics suggests that some bizarre urban heating use case could still emerge.

Bitcoin is cash, not out of convenience but out of necessity, because cash is the most unifying social contract known to humanity to induce virtuous behaviors. The two other unifying forces were death and taxes, which had been considered, but most people were disinclined in having more of them, forcing Satoshi Nakamoto to settle on cash instead.

The maintenance of Bitcoin requires choices to be made upon Bitcoin. The author argues that the most important tool to maintain Bitcoin is a moral compass; which clearly goes against the common wisdom that Microsoft Visual Studio was the only tool truly required for the maintenance of Bitcoin.

A virtue-inducing artifact

Socrates and Meno reach two different conclusions: in the first part of the dialogue, that virtue is knowledge and can therefore be taught; in the second, that it is reliable true opinion and can therefore be acquired only by divine inspiration. Taking into account Socrates' role as a teacher

(of his interlocutors and of Plato) and Plato's role as a teacher (of us), I show that neither of these conclusions is consistent with the existence of philosophy as a human institution, and argue that, for this reason, Plato refuses ultimately to endorse either of them.

On the Teaching of Virtue in Plato's Meno and the Nature of Philosophical Authority[1]*.*
Abraham D. Stone, May 2010

While science-fiction has long explored the idea of having some transcendent intelligence taking some degree of control over mankind for its own good[2], the author isn't aware of anything remotely similar ever told that would involve a non-sentient artifact. Furthermore, the idea of having humanity willingly abiding to the emergent properties of such an artifact is probably even stranger.

Yet, Bitcoin is both an artifact and Bitcoin is virtue-inducing. As such, it gives a very compelling reason to willingly abide to its emergent properties; assuming the artifact is properly maintained.

It is an artifact because Bitcoin is clearly physical and clearly man-made. The author is wondering how much this point should simply be treated as self-evident for the sake of concision, but as it appears that many commentators incorrectly point out that Bitcoin is "virtual" or "mathematical", the author will proceed with a short demonstration: there is a whole market of devices[3] intended to become parts of Bitcoin. The skeptical reader can buy a device and assert that (a) the device is made of regular matter and that (b) the device is visibly of human origin. This concludes the proof.

As artifacts go, Bitcoin is probably among the most complex artifacts ever built by humanity right after the internet itself. As the Bitcoin artifact has grown much larger than our human senses can immediately comprehend, one can be tempted to lose sight of the artifact angle; but it's not because one stops looking at the artifact, that the artifact ceases to exist.

Bitcoin is virtue-inducing because it comes with an emergent property as the result of the human interactions with the artefact itself: additional individual economic freedom.

Individual economic freedom is a virtue desirable for humanity at large. A casual observation of the world is sufficient to conclude that countries who enjoy more economic freedom have dramatically lower infant mortality rates[4]. For any parent, this is very much obvious: unless you happen to be some kind of psychopath, you will use any way that is economically accessible to you to make sure that your children live. Any restriction on your freedom to act properly as a

[1] See https://people.ucsc.edu/~abestone/papers/short_meno.pdf
[2] Many of the robot's novels of Isaac Asimov resolves around this idea.
[3] At the present time of writing, Antminer appears to be the leading manufacturer of said devices.
[4] The author acknowledge stealing this observation from Roger Ver; but the provenance of an observation does not make it less relevant. See https://www.heritage.org/international-economies/commentary/2018-index-economic-freedom

parent is doing nothing but putting your children in danger, possibly mortal danger. As far as observations go, and despite the lingering possibility of mistaking causation with correlation, the world-wide statistics are accurately reflecting this fact[5]. The author is left to wonder how many psychopathic people it takes within the general population so that it is even possible to safely raise this very concern of causation in public, without taking the social risk of being immediately singled out as a psychopath.

For the readers who are not parents, and who would struggle to understand the first argument, the author invites you to have a careful look at all the objects present in your house, and reflect whether the objects that you enjoy the most on a daily basis have been produced by fiercely for-profit companies or by non-profit institutions. Your ongoing access to those objects depends on, first, you being free to buy those objects and, second, companies being free to produce those objects.

As the main function of Bitcoin is to let participants make secure transfers of wealth on a peer-to-peer basis, the induced economic freedom is obvious for at least one category of people: *the people who prefer a bank account, with a bank they would trust with the lives of their children* - in a literal sense. The author estimates that the present rate of people who fall in this category is about 100% of the world population, once the number is rounded to the relevant precision[6].

Bitcoin is commonly misunderstood as being a replacement for banks. It isn't. Bitcoin is an *upgrade* for banks which, if executed and maintained correctly will deliver the kind of trust presented above. The fact that any bank which will fail at taking the upgrade will be swiftly driven to extinction by market forces should not be confused with the extinction of the banks themselves. The extinction of banks remain unlikely no matter how much success Bitcoin will ultimately enjoy.

Trust and verify, all the way down

A well-known scientist once gave a public lecture on astronomy. At the end of the lecture, a little old lady at the back of the room got up and said: "What you have told us is rubbish. The world is really a flat plate supported on the back of a giant tortoise." The scientist gave a superior smile before replying, "What is the tortoise standing on?" "You're very clever, young man, very clever," said the old lady. "But it's turtles all the way down!" (apocryphal[7])

Some commentators of the Bitcoin phenomenon are still running amok and claiming that Bitcoin - sometimes the blockchain - is trustless. However, nothing is further away from the truth. On the contrary, Bitcoin is entirely build on trust, more specifically, it's entirely based on a trust-and-verify approach, with turtles all way down. It is clear to the author that this approach

[5] See https://en.wikipedia.org/wiki/List_of_countries_by_infant_and_under-five_mortality_rates
[6] Three degrees of lies are (a) the plain lie. (b) the lie under oath (c) the statistics.
[7] See https://en.wikipedia.org/wiki/Turtles_all_the_way_down

has been carefully engineered that way, in order to precisely generate the excess of weirdness that Bitcoin so absolutely requires to keep running at all.

Trust is established in Bitcoin from the maximal incentivization that is given to the miners to prove themselves worthy of that trust. Verification is made as simple as possible as it only requires an inspection of the blockchain. If Bitcoin is correctly implemented and deployed at a sufficient scale, you should be able to trust Bitcoin transactions with the lives of your children, because miners will have proved themselves worthy of shouldering such an insane trust.

To readers who may not have had the experience of successfully conducting a business, this might appear counter-intuitive. However, the essence of successful capitalism is to foster an ever growing degree of trust between participants. The more trust that can be established, the more value the parties can extract from the relationship. Contracts are signed, but every party knows that the success of the contract's execution depends on the good faith of the parties involved. Despite the fact that contracts are *designed* to be enforceable through law, contracts are very rarely enforced that way. This angle is best summarized with:

Of course I've got lawyers. They are like nuclear weapons, I've got em 'cause everyone else has. But as soon as you use them they screw everything up. Danny DeVito.

The fact that the very best contracts are the ones that you never need to contractually enforce is a positively weird idea. As such, it was clearly a worthy addition to Bitcoin to ensure the overall excess of weirdness.

Yet, sane people appear unwilling to stand on turtles all the way down. The exercise tends to generate an unease similar to vertigo, with a fear merely induced by the fact that you can't really see the turtle at the very bottom; although it's firmly there, the proof being given by the fact that you are not falling.

Considering that sane people are reasonably averse to exceedingly weird solutions, sane people prefer to collapse this arguably Byzantine trust-and-verify approach into a single step. This very idea is at the core of the code-is-law approach, which is expected to remove a lot of the trust that is demanded by the trust-and-verify approach. Unfortunately, this line of thought runs contrary to the overall principle of the exceeding weirdness of Bitcoin. If such a thing like code-is-law was actually possible, it would make Bitcoin a lot less weird, which, by now, should be sufficient to make careful readers wary whether it will still be Bitcoin.

This problem runs a lot deeper than most sane people would probably think. In real life, dumb contracts only work because of poor writing, carefully produced by pilling up business nonsense on top of legal nonsense, precisely giving the parties enough operational leeway to execute the contract. However, the smart contract approach aims at removing this much needed leeway; and by actually succeeding at doing so, it also fails at delivering anything like Bitcoin would. In summary, by virtue of a lack of excessive weirdness, smart contracts are mostly doomed.

Proof-of-work generates nothing but trust (and heat)

Gold gets dug out of the ground in Africa, or some place. Then we melt it down, dig another hole, bury it again and pay people to stand around guarding it. It has no utility. Anyone watching from Mars would be scratching their head. Warren Buffett (plausible attribution)

Sane commentators of Bitcoin have long argued that proof-of-work was an obvious flaw in the design of Bitcoin. Indeed, the neverending work performed by miners appears as carefully engineered to be guaranteed to be as close as possible to a null use case for humanity. It would be a lot less weird if the work done by miners had any kind of *material* outcome. However, if such an option were available to Bitcoin, it would make Bitcoin a lot less weird, which is in complete opposition to its principle of excessive weirdness. The work done by miners is required to be a null *material* use case, because any alternative would give the miners a potential incentive to act against the very interest of Bitcoin itself. The whole point of proof-of-work is to convert electricity into *trust* and nothing else *but trust*.

The attentive reader could object that mining devices do produce heat. Thus the proof-of-work leaves open the possibility to enable a bizarre, urban heating use case derived from proof-of-work itself. This inference is the unfortunate consequence of the second law of thermodynamics, which prevent any work from happening, *literally*, without producing heat in the process. Thus, as the flaw in the proof-of-work is unavoidable, as long as we haven't figured a way to work ourselves out of the second law of thermodynamics; which may well never happen, it is acceptable to keep this very flaw as it is.

In particular, transitioning Bitcoin toward proof of stakes would make it much more amenable to reason - plutocracy being a time-tested way to organize societies - which as the reader can now expect, goes completely against the requirements of preserving an excessive weirdness in Bitcoin, else to lose Bitcoin entirely. The proof of stakes shift the responsibility of the ongoing existence of Bitcoin, from the miners who have no incentive at all but precisely to keep Bitcoin existing forever, to its users who may well have plenty of incentives of their own, including the incentive to revert their own transactions right after completing them. Hence, in the long run, proof-of-stakes would create an endless stream of trust issues undermining the virtue-inducing property of Bitcoin itself.

Cash, out of necessity

I am not worried about the deficit. It is big enough to take care of itself. - Ronald Reagan

As a virtue-inducing artifact, in order to succeed, Bitcoin needs something that *unifies* everyone. It turns out that the world is vast, and that people have very different lifestyles, tastes or gods. It's not easy to find something all people on earth have in common, besides actually being

humans. Upon reflection, while taxes and death are a given for humanity at large, at least a sizeable portion of humanity is not inclined in the slightest in having *more* of it. Thus, Satoshi Nakamoto, without being overly specific on the case, safely ruled out those options as unifying forces for Bitcoin. Thus, Satoshi Nakamoto was left with *cash* as the only unifying thing for humanity. Even the people who trust gold above all have cash, while the converse is not true.

Thus, while governments at large are actively fighting against cash to undermine organized crime, it appears that the only way to build a virtue-inducing artifact that can federate all of humanity appears to be cash. Once, again, Bitcoin is excessively weird, and any attempt at making it any less weird prevents the artifact to be Bitcoin at all.

Morality first, Technicality second

The Ephebians believed that every man should have the vote (provided that he wasn't poor, foreign, nor disqualified by reason of being mad, frivolous, or a woman). Every five years someone was elected to be Tyrant, provided he could prove that he was honest, intelligent, sensible, and trustworthy. Immediately after he was elected, of course, it was obvious to everyone that he was a criminal madman and totally out of touch with the view of the ordinary philosopher in the street looking for a towel. And then five years later they elected another one just like him, and really it was amazing how intelligent people kept on making the same mistakes. — Terry Pratchett, Small Gods

Bitcoin is the only artifact whose maintenance has almost nothing to do with its physical integrity, but the preservation of its moral integrity. If the moral integrity of Bitcoin is compromised, then, it’s not Bitcoin anymore, as there is no point in maintaining such an incredibly nonsensical artifact any longer if it isn’t virtue-inducing in the first place. Thus, Bitcoin is probably the only artifact that can be morally compromised, and undergoing such an event, be destroyed. If the idea that a non-sentient artifact can suffer physical damage from moral compromission does not self-evidently appear to the reader as exceedingly weird, the author does not know what will.

Thus, Bitcoin is the first artifact ever invented whose maintenance requires a good *moral* compass, which is also an exceedly weird maintenance tool, as far as maintenance tools go. A moral compass offers the capacity to differentiate good from evil. The fact that a moral compass can be produced at all is an interesting concern. However, as the author would like to point out, as Bitcoin exists, and as Bitcoin requires a moral compass to be maintained, the existence of moral compasses is now beyond doubt thanks to Bitcoin. It appears that Bitcoin provides a glimpse to the origin of moral; albeit clearly not the one that either religions or philosophies have been seeking through the ages.

Various corollaries

Bitcoin dominantly attracts people of negligible sanity as they are impervious to the excess of weirdness of Bitcoin itself.

While Bitcoin enthusiasts are generally known to the public as *weird dudes*, the author thinks that this terms is oddly pejorative and non gender-neutral as well. Thus, as an act of social justice warfare, the term “people of negligible sanity” should be preferred.

The far reaching implications of Bitcoin tend to produce exceedingly weird considerations, in addition to inducing moderate headaches for the majority of the population that would be deemed clinically sane by professionals. The only people who are fully immune to the problem appear to be those who never had much sanity in the first place.

Morally bankrupt actors cannot maintain Bitcoin because they will invariably degrade Bitcoin to the point it is not Bitcoin anymore.

Con artists taking advantage of fools through get-rich-quick schemes is the oldest trick in the book, and it is not weird at all. Thus, con artists can help themselves, and through their attempt at rationalizing Bitcoin into something that serves their own interests, they invariably break Bitcoin when given the chance.

The capacity for Bitcoin to attract morally bankrupt actors is staggering, especially considering that as a virtue-inducing artifact, it goes against the very essence of said actors. The capacity for morally bankrupt actors to be publicly caught red-handed while messing with Bitcoin is also staggering.

Honest but ignorant actors cannot maintain Bitcoin because they will invariably let Bitcoin be degraded to the point it is not Bitcoin anymore.

The excess of weirdness of Bitcoin makes sane people feel worried about the fact they will look like fools in the eyes of other sane people. Thus, those people invariably try to tame the weirdness of Bitcoin by posturing for a “blockchain” perspective, which is indeed a lot less weird, but unfortunately not Bitcoin at all; as the excessive weirdness of Bitcoin cannot be diminished.

The blockchain without Bitcoin is known as Git. While Git is arguably a lot less weird than Bitcoin, it does preserve some residual weirdness, as second-order virtue-inducing artifact. Git managed the seemingly impossible feat of getting for-profit companies to give away their software code for free on GitHub.

The author observes that the vast majority of companies getting themselves into the blockchain will get exactly what can be found on GitHub: immense troves of dead code. It is unclear to the author however if this perspective truly reflects the original intents of those companies.

There can be only one Bitcoin, because economic freedom is not additive. People are not twice as free because they enjoy twice the same freedom.

As the essence of Bitcoin is to induce specific virtues, those virtues can only be induced once. This removes the need to have a second Bitcoin. Yet, the very existence of Bitcoin has somehow managed the seemingly impossible feat of convincing certain people that economic freedom, unlike any other virtue, was additive. The *additive freedom* perspective states that offering twice the same freedom make you twice as free. This process is fundamentally similar to the idea that putting a copy of the First Amendment in the United States Constitution below the original one would make people twice as free as well.

Academia has failed - and will keep failing - at recognising excessive weirdness as the defining trait of Bitcoin, because it's just plain embarrassing.

Die Wahrheit triumphiert nie, ihre Gegner sterben nur aus. - Max Planck (Truth never triumphs—its opponents just die out)

The moral imperative of professors is publish or perish. Yet obtaining publications depends on obtaining the consent of relevant peers, who also happen to be professors. Indeed, as opinions stated outside academia do not abide to *any* standard, not even of making even remotely sense, the only safe option is to stick with the opinion of professors; who have the undeniable quality of delivering a very safe form of entertainment.

Any professor who would start to defend an exceedingly weird idea would instantly become an outcast within the inner circles of academia. As such, the professor would be denied access to publication, which would lead to his death. As avoiding death is a very sensible thing to do for all living beings, which include professors; professors refrain themselves from supporting any exceedingly weird idea until the truth is so widely known to the public at large that it isn't tenable for them any more to maintain this stance.

Bitcoin, by virtue of excessive weirdness, naturally falls into this category.