AI & SOCIETY (2019) 34:161–162
https://doi.org/10.1007/s00146-018-0870-4

CURMUDGEON CORNER

Burning down the house: bitcoin, carbon-capitalism, and the problem of trustless systems

David Morris[1]

Published online: 7 December 2018

Bitcoin is built to bypass governments, which can fail, and central banks, which can print and thereby devalue currency. In many ways it's designed to be *money* (a 'store' of value), versus a *currency* (backed by government fiat and people working and paying taxes). Bitcoin, therefore, cannot trust any centralized authority to keep its books. The transaction data is kept in the open—yet no one person or power can unilaterally add to or tamper with them.

How can this work? Bitcoin uses mathematical *hashing* functions to chain blocks of transaction data together, via numbers, *hashes*, that in effect seal the transactions, so anyone can detect tampering. But you could compute these on an iPhone. If this is all it took, you would be able to forge slightly skewed books that look legit, but double spend, or rip people off. Bitcoin, therefore, carefully calculates an added, arbitrary difficulty, which forces "miners" using computers to make thousands of random guesses to make a hash with special characteristics. The first to compute this hash is awarded (some) bitcoin. The losers' computations are thrown away—wasted. This ends up being very energy intensive.

That computational waste is just what secures bitcoin. Wasting calculations on computing such hashes costs a *lot* in real-world electricity (and equipment). The algorithm adjusts the difficulty so that the cost of forging bitcoin runs higher than the value of the bitcoin you would gain.

Bitcoin mining rigs are, therefore, more effective at converting electricity into heat—at being radiators—than converting electricity into useful computational work. Or rather, the real work of rigs is proving they are wasting enough electricity to not profit from ripping off the system, whilst also occasionally calculating a winning hash.

When I was growing up this would have been a sci-fi scenario: explorers land on distant planet whose priestly caste offers burnt sacrifices, ritual waste, to create fictive value; explorers shake their heads, wondering how long these people will survive, since their sacrifices pollute their planet.

In the real world, the wasteful cost is carbon release right amidst the climate change crisis. Yes, renewables and hydroelectric alter that a bit—but that just means Bitcoin sucks up renewable electricity that could replace carbon energy sources for *real work* that needs to be done. Useable energy degraded into waste heat to secure Bitcoin means carbon is released somewhere else to do real work. Bitcoin miners know their main product is waste heat: in Québec, one argument they advance in favor of providing them electricity is they can heat unused buildings in winter.

At the very same time, as money deliberately cut off from the real currency of countries and labour, it fosters speculation that detaches more and more from real world flows. It is a disembodied 'Cartesian money machine', moving counter to economies taking into account externalities: it offers a possibility of trade solely within a number-money system, that need not be linked to anything—except the wasting of real-world energy to secure a money without trust.

In a nutshell, or a heatsink (let's say), Bitcoin is carbon-capitalism purified: extracting wealth from pure number as value, by burning carbon as proxy for trust. There are efforts in crypto-currency to address this: to shift from the enormous waste of Bitcoin's proof-of-work step described above, to proof-of-stake systems. But there are going to be inefficiencies, driven up by profit and speculative motives, whenever you try to secure such a system without central authority.

All this broaches further issues. It's not as if there are not actual human authorities making just the sort of decisions that Bitcoin does not trust central banks to make. A notorious example is rolling back the books to write off the Mt. Gox theft of huge amounts of bitcoin. Other cryptocurrencies share this seemingly paradoxical weakness. Vitalik

✉ David Morris
david.morris@concordia.ca

[1] Department of Philosophy, Concordia University, 1455 de Maisonneuve Blvd. W, Montreal, QC H3G 1M8, Canada

Buterin, lead of Ethereum, is aware of this paradox, how the shaping power of founding gurus runs counter to trustless cryptocurrencies—so he is trying to vanish from his creation.

But here's another strange head-spin, via an MIT Technology Review newsletter item (MIT Technology Review 11.20.2018) titled "The Bitcoin Cash hard fork has created a confusing mess". Basically, competing groups are advancing different versions of Bitcoin: the original; and a new one that would be more efficient in enabling cash-like transactions (all the computational overhead in fact makes Bitcoin very slow).

Quelle surprise! A money system built to obviate the need to trust a central authority, and that has generated huge speculative investment cash flows… is now battling about which human authority is the authority! And, since the money is not backed by governments or *humans negotiating matters of trust*, but by trustless algorithms, the battle is turning into a "hash war" "in which both sides have spent massive amounts of computing power in attempt to wrestle control of the original chain from the other".

Lesson 1 In monetary systems, you will never be able to trust math alone, without humans involved. Any money that has value is about humans valuing it, not numbers alone.

Lesson 2 In a monetary system that seeks to be secured by math, and not trust in authority (or what humans themselves give to the system), the real security, the real trust, ends up grounded in electrical power for computation. So electrical expenditure becomes proxy for trust in authority.

Corollary 1 Smart contracts are going to open disasters. Contracts contract *trust*. The assessment of fulfilment of contracts is always a human and legally binding affair; there will be no way to fully adjudicate this in an automated fashion. The issue is already known to the cryptocurrency community, e.g., under the heading of the 'oracle problem': how to ensure trusted sources of information, re., e.g., even something as simple as airplane flight cancellations, to trigger automatic refunds. At the place where numbers and trust meet, there are irreducible human interests that by definition are not subject to any algorithm.

Corollary 2 Trust, promise, debt, and written contracts (when they arise), are close to the heart of human societies. Ask an anthropologist, sociologist, political scientist, historian, scholar of law (or literature or philosophy). Mediating knowledge, social relations, or stock markets, with computer algorithms has…. not gone so well for us humans. Ought we trust human built algorithms to mediate contracts? Imagine hash wars to settle contracts. Imagine algorithms that wirelessly repossess the family car right as they head to the hospital for a baby being born (because the collateral in their house just vanished in a housing bubble). What does it mean to 'sign' such contracts, when fewer will understand their workings than understood CDOs? We should base our monetary systems on the study of the human reality of trust—which shows that contracts are inherent exposures to unstable meanings and unpredictable circumstances. Human futures do not compute. Pretending they do leads to flash crashes… which may now turn into cash crashes, trust crashes, and crashes of new, unanticipated sorts, with real world impacts.

Curmudgeon Corner Curmudgeon Corner is a short opinionated column on trends in technology, arts, science and society, commenting on issues of concern to the research community and wider society. Whilst the drive for super-human intelligence promotes potential benefits to wider society, it also raises deep concerns of existential risk, thereby highlighting the need for an ongoing conversation between technology and society. At the core of Curmudgeon concern is the question: What is it to be human in the age of the AI machine? -Editor.