AI & SOCIETY (2018) 33:291–292
https://doi.org/10.1007/s00146-018-0808-x

CURMUDGEON CORNER

In *mod* we trust? Human trust, Bitcoin, and the burning waste of time

David Morris[1]

Published online: 2 February 2018

Bitcoin is strikingly beautiful in its abstract cryptographic design but a nightmare on earth regarding concrete environmental realities. It is also a symptom of a sci-fi libertarian tendency to find clever technological solutions to problems that we do not need to have. We could instead work to find better ways of humans living together, so as to build shared institutions of trust.

Bitcoin's goal—keeping a transparent, tamper-proof, decentralized ledger—hinges on a Proof of Work verification step, the cost of which, in terms of electricity, computers, and computing time, must ramp up with the value of what is recorded in the ledger. Otherwise, a cheater would find it worthwhile to invest in enough computers, computing time, and electrical energy to forge the entire blockchain, or build a computer setup powerful enough to forge a fork that catches up with the most recent N blocks.

Either way, electricity is a limit factor: by design, Proof of Work *must* require an enormous amount of computation and huge electrical expenditures, including removal of waste heat. These costs and wastes must go up as the value of bitcoin and the ledger goes up. More, to allow decentralization, *multiple* miners or consortia must work to solve the problem. But only the first to solve it wins back bitcoin. All the others just waste heat and electricity for the sole purpose of demonstrating that one cannot produce results fast enough to forge the chain. This computational time wasting must be repeated for each transaction—which also limits transaction volume and instead of cutting out middleman charges, transactions fees are rising to cover this waste.

Imagine we coined a currency out of Damascus steel, where the newest coin is accepted for circulation if and only if its randomly produced striation pattern is similar enough, by some absurdly hard-to-satisfy metric, to the previous coin. Miners burn up energy forging coins until one is lucky enough to produce a winning, certifiable coin. And then everybody else throws away their result. This allows a decentralized minting process, but it is totally wasteful and inefficient. It is intolerable as a design for physical coins: just have a central mint produce coins with hard-to-forge features.

If you want a decentralized ledger, the design of Bitcoin is elegant. If energy and time per currency exchange were a consideration, the design is terrible. But this terrible design is precisely what lets us prove and secure an identity in an abstract realm of numbers that do not have identities—if you do not want to trust a central authority. In physical coinage, when the cost of producing a coin (e.g., a penny) converges too closely with the monetary value it represents, it is removed from circulation. In contrast, Bitcoin's security hinges on this convergence: the cost of producing bitcoins and adding transaction blocks must track the increasing value of bitcoins.

This result is something of a novelty, or even a regression, in the history of information technology: the great power of numerical notations is that the cost of writing them down does not notably increase with the quantity the numbers represent. That is why we use Arabic rather than Roman numerals, why we start using exponential notations when numbers get very large: it is only marginally more difficult to write 2×10^{340} vs. 2×10^{3}, even though they represent vastly different values. Bitcoin is a very strange informational institution that in effect prevents people from stealing numbers by making it very costly to write them down or change them. This is why the cost of recording has to track upward with the quantity and value of what the numbers represent.

Is it worth it? Why not solve the human side of the equation: Figure out how to build human institutions that one can trust, instead of bending numbers to purposes they do not serve well. That is it in a nub: Bitcoin coins numbers we can trust by stamping them with the energy, time, and computing cost of computations.

Bitcoin should be branded with the logo "In *mod* we trust." (Information loss under the *modulo* operation is irreversible; this is crucial to the irreversibility of hash

✉ David Morris
david.morris@concordia.ca
https://www.concordia.ca/artsci/philosophy/faculty.html?fpid=david-morris

[1] Department of Philosophy, Concordia University, Montreal, Canada

functions, as key to securing Bitcoin. In fact, there is a profound connection between irreversible heat production, and irreversible information loss: Bitcoin is forged in the intersection of physical and informational entropy.)

But really it is not *mod* we trust: it is the energy and computing costs of calculating *mod*. Bitcoin is really Heatcoin: it secures trust through a burning waste of (computational) time. (But be prepared for trouble when quantum computing gets to the point of computing hashes or finding prime factors quickly.) And imagine something we might have computed with all the computations burnt up so far, e.g., some sort of medically important protein-folding problem.

At present Bitcoin is also a platform par excellence for the purest sort of financial speculation we have yet invented. It is not for nothing that some governments see cryptocurrencies as securities—although it is not clear what they are securities *in*. Blockchain might be great as a ledger for other sorts of information. But once it is seized by currency speculation it blows up into the biggest bubble yet, one that is not limited by tulips to grow, or houses to build and fob off on buyers. Its limit is burning up energy to produce numbers we can trust to value. So, this bubble will not, e.g., savage housing stocks, it has no underlying reality. But it wastes time and energy, and any bursting bubble of investment will have its ripple effects.

Why have this sort of currency then? Yes, it allows for exchange that is not subject to government or centralized authority. But why must governments not be trusted? Why begin with the view that they must be inefficient or mendacious? Why not work together for better governments and for systems whereby we cultivate trust without needing to secure it through a burning waste of time?

Indeed, we find something like this approach in Estonia, which is building efficient, transparent, and sensible systems for sharing and exchanging information in secure ways—by trusting governments to build things. Perhaps we could find a midway point. Or, in a perverse twist, what if, e.g., it were possible to set the Proof of Work step as calculation of cells in a weather prediction or climate modelling system at some international level? Then the time would not be wasted, but would help us manage our burning up of this planet.

In any case, instead of speculating in a currency secured by a burning waste of time, we might want to find other ways to build trust together, despite and in face of demonstrable and repeated failures of our humanity. If we are to survive, it is in humanity, not *mod*, that we must put our trust.