Never Trust Bitcoin: Blockchain Technology – The Misnomer of a "Trustless" System

Palveshey Tariq
Harvard University

Mark Jamison
University of Florida

Abstract

Satoshi Nakamoto's stated aspiration was to create "a system for electronic transactions without relying on trust." He/she/they failed to do that and may have created just the opposite. The failure isn't because Nakamoto got the technology wrong, but because of humans' mental limits. Trusting bitcoin's or any other blockchain means trusting the code. Only a relatively small number of people can understand blockchain code, and an even smaller number find it worth their while to keep up with the updates. Everyone else has to trust the coders, which means trusting blockchain governance. Anyone familiar with the history of regulation knows that politics quickly imposes new regulations whenever the public loses trust in business or, ironically, government.

If blockchain technology is to avoid being overtaken by politics as usual - the very thing that Nakamoto wanted to eviscerate - members of the public have to trust blockchain self-governance systems more than they do the politicians, they vote for. This is harder to accomplish than it sounds. Such self-governance systems need to include trusted members, transparent processes, public input, nurtured critics, proven results, faithfully demonstrated public purpose, and understandable agendas. Without such self-governance systems, traditional government institutions will take over blockchain governance, with the risk that the extensive data and technical efficiency of blockchain will be used for traditional political purposes at best and, at worst, for control by authoritarian regimes.

Can we trust blockchain?

Blockchain is supposed to be trustless, meaning that it does not require a third party, like a bank, to validate payments and other asset transfers. As Satoshi Nakamoto, the creator(s) of bitcoin (which effectively launched blockchain technology) said: “We have proposed a system for electronic transactions without relying on trust.”

Did Nakamoto succeed?

No. Blockchain changes the loci of trust, but not the need for trust.

This paper intends to explain why, while providing evidence.

What are the technologies in question?

The focus will be on two technologies, in particular:

i. One is blockchain itself. For those unfamiliar with the technology, AEI provides a quick tutorial here.
ii. The second technology is smart contracts, which are software apps that execute transfers of money or other assets (although it could do other things) based on a

> trigger. For example, your credit card could be automatically charged for a hotel room stay when you use an electronic key to enter the room. Smart contracts aren't smart — there is no learning or thinking going on — nor are they contracts in the common use of the term: They don't necessarily have all of the elements of a contract, including offer, acceptance, a legally binding agreement to do something legal, an exchange of things of value, and parties of legal capacity (e.g., not minor children).

Why not trust the technologies?

They are not easily understandable to the general public. For example, according to bitcoin's website, one of the reasons people are supposed to trust bitcoin's blockchain is:

> The Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software.

But for this openness to be useful, users either have to understand the coding or trust the coders. Here is a bitcoin coding change from the week of July 30, 2018:

```
      before_install:
    - export PATH=$(echo $PATH | tr ':' "\n" | sed '/\/opt\/python/d' | tr "\n" ":" | sed
      "s|::|:|g")
    -     BEGIN_FOLD     ()     {     echo     "";     CURRENT_FOLD_NAME=$1;     echo
      "travis_fold:start:${CURRENT_FOLD_NAME}"; }
    -  END_FOLD  ()  {  RET=$?;  echo  "travis_fold:end:${CURRENT_FOLD_NAME}";  return
      $RET; }
      install:
    - travis_retry docker pull $DOCKER_NAME_TAG
    - env | grep -E '^(CCACHE_|WINEDEBUG|BOOST_TEST_RANDOM|CONFIG_SHELL)' |
      tee /tmp/env
    - if [[ $HOST = *-mingw32 ]]; then DOCKER_ADMIN="--cap-add SYS_ADMIN"; fi
```

If Gilda Radner's character, Emily Litella, tried to verify this, it is likely she would quickly say, "Never mind." Most of us are left with either trusting the coders or distrusting bitcoin. *(The above isn't the complete change, but you get the point.)*

Many blockchains have been found to be faulty

The need to trust coders was highlighted by a recent study of the fifty top-grossing initial coin offerings (ICOs). The researchers analyzed how the software code controlling the projects' ICOs reflected (or failed to reflect) their contractual promises. Our inquiry reveals that many ICOs failed even to promise that they would protect investors against insider self-dealing. Fewer still manifested such contracts in code.

How far off was real code from what the ICOs promised? For vesting requirements — which are intended to protect investors from the threat of founders deserting the enterprise — of the 30 ICOs that made promises about vesting, only 7 actually included the promises in the computer code.

Are some blockchains inherently untrustworthy?

Some probably are. Imagine if Venezuela had created a successful cryptocurrency or if China goes all crypto as some suspect. Many observers concluded that Venezuela's petro cryptocurrency was a scam. Both of these countries score near the bottom of Freedom House's political freedom index. What would keep them from using their blockchains to track everyone's economic activity? It would be perhaps one of the greatest ironies of history if blockchain —

which was created in part to reduce or eliminate government controls — becomes an instrument of choice of authoritarian regimes.

Is blockchain bad?

Absolutely not. The technology has many beneficial applications, such as bringing the unbanked into modern economies, distributing aid to refugees, managing inventories and transactions, and managing elections. But it needs trustworthy governance. For example, businesses in this space should develop standards of conduct and ways to enforce them. And businesses should standardize some aspects of the technologies. This would lower development and verification costs.

With all of this in mind, there are a few misconceptions that must be cleared up:

Know what blockchain is, but at a strategic rather than technical level

Blockchain is a technology for validating information and protecting it from tampering. But such technologies have been around for a long time. What's different with blockchain is that it decentralizes governance, which means that people that rely upon the information don't have to trust a single individual or organization to honestly and reliably validate and protect the information. Instead, people trust the software.

This has the potential for changing how businesses, customers, and regulators operate. We discuss this in more detail below. Here we recommend that regulators look for situations where it is hard to maintain and share information that people need to trust. For example, in some instances market monitoring information has been controversial. If blockchain is used to collect the information, it can be made instantly available to persons who are authorized to access it and can be protected from loss and tampering.

A slightly more technical description of blockchain

Hashing makes the data effectively tamperproof because any attempt to change the record triggers a change in the hash, which is detected by the blockchain software. We explain this next.

How do they chain the blocks? Through their hashes. Each newly created block contains the hash of the previous block. So, the new block's hash effectively includes the previous block's information (through its hash), which includes its previous block's information (through its hash), etc. Through this mechanism the software ensures that the power put onto the grid can be traced back to a corresponding amount that was taken off the grid.

So, the transactions are validated and protected by software that everyone involved has had the opportunity to inspect and authenticate, and the chain ensures that the entrepreneur sells into the grid only amounts that it has taken.

Smart contracts are not the same as traditional legal contracts.

Smart contracts can automate transactions once certain conditions are met. There is a lot of buzz about smart contracts, which are software that execute transfers of money or other actions based on triggers. A typical example is a vending machine that automatically dispenses the requested food product when the right buttons are pressed, and a credit card approved. Broadband providers could use smart contracts to subsidize rural hospitals, for example, by having the activation of a broadband connection to a rural hospital trigger a payment from an association of broadband providers to the supplier that is providing the subsidized service.

Smart contracts won't replace traditional contracts for two reasons. First, smart contracts aren't smart: There is no learning or thinking going on, only automated processes that otherwise require human intervention. Nor are smart contracts really contracts in the common use of the term. We are not lawyers, but our understanding is that agreements generally have to include the following elements to be considered contracts: Offer, acceptance, a legally binding agreement to do something that is legal to do, an exchange of things of value, and parties of legal capacity (e.g., not minor children). A smart contract may not be legally enforceable if one of the affected parties decides to object after the smart contract has been executed. There may be no exchange of value in a smart contract. For example, the water quality smart contract we described above executes without any exchange of value, an offer, or acceptance. And there is nothing to stop a minor child from executing a smart contract.

And finally, understand that the trustlessness of blockchain technology is a misnomer. A larger collective, must still be entrusted with the trust of the users in order to remain (at the very least) functional.

Bibliography

Anthony Cuthbertson, "Bitcoin Mining on Track to Consume All of the World's Energy by 2020," *Newsweek*, December 11, 2017*, https://www.newsweek.com/bitcoin-mining-track-consume-worlds-energy-2020-744036.*

Berberich, M., and M. Steiner. "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?". *https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/Edpl2&id=448&men_tab=srchresults*, 1 Mar. 2016, https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/edpl2&id=448&men_tab=srchresults.

Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa," *Power Compare* (undated), *https://powercompare.co.uk/bitcoin/.*

Carlozo, L. "What Is Blockchain?". *https://search.proquest.com/docview/1917635714?Pq-origsite=gscholar*, 29 July 2017, *https://search.proquest.com/docview/1917635714?pq-origsite=gscholar.*

Colleen Metelitsa, "*4 Predictions for Blockchain in Energy in 2018*," *Greentech Media*, March 5, 2018, *https://www.greentechmedia.com/articles/read/four-predictions-for-blockchain-in-energy-in-2018#gs.xCOeAjk (accessed August 11, 2018).*

GitHub, "bitcoin", *https://github.com/bitcoin/bitcoin/commit/566f826902cf1a1df18dba83d5302cf173b64e1d,* accessed August 7, 2018.

Hacker Noon, "*Top Blockchain Events and Conferences*, 2018," *https://hackernoon.com/top-blockchain-events-conferences-95ad281a00c1,* accessed August 7, 2018.

Mark A. Jamison, "*Can blockchain save broadband for rural healthcare?" AEIdeas*, June 6, 2018, *https://www.aei.org/publication/can-blockchain-save-broadband-for-rural-healthcare/.*

Mark A. Jamison, "Is bitcoin an energy hog?" *AEIdeas*, January 12, 2018, http://www.aei.org/publication/is-bitcoin-an-energy-hog/.

Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff, and David A. Wishnick, "*Coin-Operated Capitalism*," (July 17, 2018). Available at SSRN: *https://ssrn.com/abstract=3215345 or http://dx.doi.org/10.2139/ssrn.3215345*

Zheng, Z., S. Xie, H. Dai, X. Chen, and H. Wang. "*An Overview Of Blockchain Technology: Architecture, Consensus, And Future Trends - IEEE Conference Publication*". *www.ieee.Org*, 11 Sept. 2017, *https://ieeexplore.ieee.org/abstract/document/8029379.*