The blockchain paradox: Why distributed ledger technologies may do little to transform the economy

Author
Vili Lehdonvirta

Posted
21 November 2016

Tags
bitcoin, blockchain, Digital Economies, distributed ledger technology, Economics, economy, governance, Governance & Security

Bitcoin's underlying technology, the blockchain, is widely expected to find applications far beyond digital payments. It is celebrated as a "paradigm shift in the very idea of economic organization". But the OII's Professor Vili Lehdonvirta contends that such revolutionary potentials may be undermined by a fundamental paradox that has to do with the governance of the technology.

I recently gave a talk at the Alan Turing Institute (ATI) under the title *The Problem of Governance in Distributed Ledger Technologies*. The starting point of my talk was that it is frequently posited that blockchain technologies will "revolutionize industries that rely on digital record keeping", such as financial services and government. In the talk I applied elementary institutional economics to examine what blockchain technologies really do in terms of economic organization, and what problems this gives rise to. In this essay I present an abbreviated version of the argument. Alternatively you can watch a video of the talk below.

First, it is necessary to note that there is quite a bit of confusion as to what exactly is meant by a blockchain. When people talk about "the" blockchain, they often refer to the Bitcoin blockchain, an ongoing ledger of transactions started in 2009 and maintained by the approximately 5,000 computers that form the Bitcoin peer-to-peer network. The term blockchain can also be used to refer to other instances or forks of the same technology ("a" blockchain). The term "distributed

ledger technology" (DLT) has also gained currency recently as a more general label for related technologies.

In each case, I think it is fair to say that the reason that so many people are so excited about blockchain today is not the technical features as such. In terms of performance metrics like transactions per second, existing blockchain technologies are in many ways inferior to more conventional technologies. This is frequently illustrated with the point that the Bitcoin network is limited by design to process at most approximately seven transactions per second, whereas the Visa payment network has a peak capacity of 56,000 transactions per second. Other implementations may have better performance, and on some other metrics blockchain technologies can perhaps beat more conventional technologies. But technical performance is not why so many people think blockchain is revolutionary and paradigm-shifting.

The reason that blockchain is making waves is that it promises to change the very way economies are organized: to eliminate centralized third parties. Let me explain what this means in theoretical terms. Many economic transactions, such as long-distance trade, can be modeled as a game of Prisoners' Dilemma. The buyer and the seller can either cooperate (send the shipment/payment as promised) or defect (not send the shipment/payment). If the buyer and the seller don't trust each other, then the equilibrium solution is that neither player cooperates and no trade takes place. This is known as the fundamental problem of cooperation.

There are several classic solutions to the problem of cooperation. One is reputation. In a community of traders where members repeatedly engage in exchange, any trader who defects (fails to deliver on a promise) will gain a negative reputation, and other traders will refuse to trade with them out of self-interest. This threat of exclusion from the community acts as a deterrent against defection, and the equilibrium under certain conditions becomes that everyone will cooperate.

Reputation is only a limited solution, however. It only works within communities where reputational information spreads effectively, and traders may still defect if the payoff from doing so is greater than the loss of future trade. Modern large-scale market economies where people trade with strangers on a daily basis are only possible because of another solution: third-party enforcement. In particular, this means state-enforced contracts and bills of exchange enforced by banks. These third parties in essence force parties to cooperate and to follow through with their promises.

Besides trade, **another example of the problem of cooperation is currency.** Currency can be modeled as a multiplayer game of Prisoners' Dilemma. Traders collectively have an interest in maintaining a stable currency, because it acts as a lubricant to trade. But each trader individually has an interest in debasing the currency, in the sense of paying with fake money (what in blockchain-speak is referred to as double spending). Again the classic solution to this dilemma is third-party enforcement: the state polices metal currencies and punishes counterfeiters, and banks control ledgers and prevent people from spending money they don't have.

So third-party enforcement is the dominant model of economic organization in today's market economies. But it's not without its problems. The enforcer is in a powerful position in relation to the enforced: banks could extract exorbitant fees, and states could abuse their power by debasing the currency, illegitimately freezing assets, or enforcing contracts in unfair ways. One classic solution to the problems of third-party enforcement is competition. Bank fees are kept in check by competition: the enforced can switch to another enforcer if the fees get excessive.

But competition is not always a viable solution: there is a very high cost to switching to another state (i.e. becoming a refugee) if your state starts to abuse its power. Another classic solution is accountability: democratic institutions that try to ensure the enforcer acts in the interest of the enforced. For instance, the interbank payment messaging network SWIFT is a cooperative society owned by its member banks. The members elect a Board of Directors that is the highest decision

owned by its member banks. The members elect a Board of Directors that is the highest decision making body in the organization. This way, they attempt to ensure that SWIFT does not try to extract excessive fees from the member banks or abuse its power against them. Still, even accountability is not without its problems, since it comes with the politics of trying to reconcile different members' diverging interests as best as possible.

Into this picture enters blockchain: a technology where third-party enforcers are replaced with a distributed network that enforces the rules. It can enforce contracts, prevent double spending, and cap the size of the money pool all without participants having to cede power to any particular third party who might abuse the power. No rent-seeking, no abuses of power, no politics — blockchain technologies can be used to create "math-based money" and "unstoppable" contracts that are enforced with the impartiality of a machine instead of the imperfect and capricious human bureaucracy of a state or a bank. This is why so many people are so excited about blockchain: its supposed ability change economic organization in a way that transforms dominant relationships of power.

Unfortunately this turns out to be a naive understanding of blockchain, and the reality is inevitably less exciting. Let me explain why. In economic organization, we must distinguish between *enforcing rules* and *making rules*. Laws are rules enforced by state bureaucracy and made by a legislature. The SWIFT Protocol is a set of rules enforced by SWIFTNet (a centralized computational system) and made, ultimately, by SWIFT's Board of Directors. The Bitcoin Protocol is a set of rules enforced by the Bitcoin Network (a distributed network of computers) made by — whom exactly? Who makes the rules matters at least as much as who enforces them. Blockchain technology may provide for completely impartial rule-enforcement, but that is of little comfort if the rules themselves are changed. This rule-making is what we refer to as governance.

Using Bitcoin as an example, the initial versions of the protocol (ie. the rules) were written by the pseudonymous Satoshi Nakamoto, and later versions are released by a core development team. The development team is not autocratic: a complex set of social and technical entanglements means that other people are also influential in how Bitcoin's rules are set; in particular, so-called mining pools, headed by a handful of individuals, are very influential. The point here is not to attempt to pick apart Bitcoin's political order; the point is that Bitcoin has not in any sense eliminated human politics; humans are still very much in charge of setting the rules that the network enforces.

There is, however, no formal process for how governance works in Bitcoin, because for a very long time these politics were not explicitly recognized, and many people don't recognize them, preferring instead the idea that Bitcoin is purely "math-based money" and that all the developers are doing is purely apolitical plumbing work. But what has started to make this position untenable and Bitcoin's politics visible is the so-called "block size debate" — a big disagreement between factions of the Bitcoin community over the future direction of the rules. Different stakeholders have different interests in the matter, and in the absence of a robust governance mechanism that could reconcile between the interests, this has resulted in open "warfare" between the camps over social media and discussion forums.

Will competition solve the issue? Multiple "forks" of the Bitcoin protocol have emerged, each with slightly different rules. But network economics teaches us that competition does not work well at all in the presence of strong network effects: everyone prefers to be in the network where other people are, even if its rules are not exactly what they would prefer. Network markets tend to tip in favour of the largest network. Every fork/split diminishes the total value of the system, and those on the losing side of a fork may eventually find their assets worthless.

If competition doesn't work, this leaves us with accountability. There is no obvious path how Bitcoin could develop accountable governance institutions. But other blockchain projects, especially those that are gaining some kind of commercial or public sector legitimacy, are designed from the ground up with some level of accountable governance. For instance, R3 is a

firm that develops blockchain technology for use in the financial services industry. It has enrolled a consortium of banks to guide the effort, and its documents talk about the "mandate" it has from its "member banks". Its governance model thus sounds a lot like the beginnings of something like SWIFT. Another example is RSCoin, designed by my ATI colleagues George Danezis and Sarah Meiklejohn, which is intended to be governed by a central bank.

Regardless of the model, my point is that blockchain technologies cannot escape the problem of governance. Whether they recognize it or not, they face the same governance issues as conventional third-party enforcers. You can use technologies to potentially enhance the processes of governance (eg. transparency, online deliberation, e-voting), but you can't engineer away governance as such. All this leads me to wonder how revolutionary blockchain technologies really are. If you still rely on a Board of Directors or similar body to make it work, how much has economic organization really changed?

And this leads me to my final point, a provocation: **once you address the problem of governance, you no longer need blockchain;** you can just as well use conventional technology that assumes a trusted central party to enforce the rules, because you're already trusting somebody (or some organization/process) to make the rules. I call this blockchain's 'governance paradox': once you master it, you no longer need it. Indeed, R3's design seems to have something called "uniqueness services", which look a lot like trusted third-party enforcers (though this isn't clear from the white paper). RSCoin likewise relies entirely on trusted third parties. The differences to conventional technology are no longer that apparent.

Perhaps blockchain technologies can still deliver better technical performance, like better availability and data integrity. But it's not clear to me what real changes to economic organization and power relations they could bring about. I'm very happy to be challenged on this, if you can point out a place in my reasoning where I've made an error. Understanding grows via debate. But for the time being, I can't help but be very skeptical of the claims that blockchain will fundamentally transform the economy or government.

The governance of DLTs is also examined in this report chapter that I coauthored earlier this year:

Lehdonvirta, V. & Robleh, A. (2016) Governance and Regulation. In: M. Walport (ed.), *Distributed Ledger Technology: Beyond Blockchain*. London: UK Government Office for Science, pp. 40-45.

Note: This post was originally published on the Policy & Internet blog on 21 November 2016 5:08 pm. It might have been updated since then in its original location. The post gives the views of the author(s), and not necessarily the position of the Oxford Internet Institute.

Related posts

The Future of Work in the Global South

Added: 8 March 2018

The Future of Work in the Global South

Added: 8 March 2018

Hacking code/space: Confounding the code of global capitalism

Added: 3 March 2018

Towards a Fairer Platfo Economy: Introducing t Fairwork Foundation

Added: 16 February 2018