Next Generation Internet

Position Paper on:

Bitcoin, Blockchain, and the future of the Internet

Primavera De Filippi
CERSA / CNRS — Berkman Center at Harvard Law

Bitcoin is widely known as a decentralized payment system, which allows for the transfer of funds across borders at virtually no costs and without external control. As such, it can serve as a new backbone technology for depository institutions, increasing the speed and efficiency of inter-bank transfers and making it easier for banks to convert funds from one currency to another.

On the technical level, Bitcoin is a so-called trustless payment system, enabling people or institutions that do not know each other (and therefore do not trust each other) to exchange value directly, without the need for any trusted authority or centralized clearing house. It is trustless not because there is no trust in the transactions, but because things simply cannot go wrong in the first place. Bitcoin has its own rules and regulation programmed directly into its fabric: trust is delegated to the network itself, where all transactions are public and verifiable by everyone. The sustainers of the network —the so-called miners or validators— act as an insurance for the actual execution of these transactions.

This is important for two main reasons:

1. It allows for a more distributed network of exchange, where people can exchange value directly with one another, instantaneously, and without relying on any potentially corrupted, unreliable, or monopolistic (rent-taking) financial intermediary.
2. It provides a mechanism for banking the unbanked —enabling those who are currently cut off from the financial system, often because they have no trust to offer, to enter the global economy. This is particularly relevant for the most vulnerable persons who have not been able to access financial services, such as immigrants and migrants, as well as the swaths of populations that live under corrupt, authoritarian or unstable governments and political systems.

The same technology can also be used to vastly improve the remittance market, while enabling a greater degree of financial inclusion. Currently, the remittance fees charged by multinational corporations, which maintain a monopoly on international value transfer networks, amount to a large portion of the global financial aid sent to developing countries. The World Bank estimates that even a reduction of a few percentage points in the costs of remittance would save billions of dollars to the overall remittance costs.

Of course, given the lack of a central regulatory authority, Bitcoin also comes along with a number of challenges. Given the ease of access to this decentralized peer-to-peer payment system, Bitcoin provides new opportunities for criminal activities, including tax-evasion and money-laundering (as shown by the case of SilkRoad, where Bitcoin was used as a near-anonymous payment system for the sale of illegal drugs).

The response, in the US at least, has been to regulate decentralized virtual currencies, by regulating the commercial operators (such Bitcoin exchanges and wallet providers) as if they were regular financial operators or money transmitters —and thus require them to comply with Anti Money Laundering (AML), Know Your Customers (KYC) and money transmission laws.

Note that these same regulations, when applied into the blockchain space, may undermine standard expectations of financial privacy. There is therefore, a growing need to reconsider the impact of existing AML/KYC regulations (drafted in an era of closed “black boxes”) in light of this new technological framework that provides tools for for better governance and fraud prevention

—thereby reducing or even eliminating the need for such an extensive set of (onerous) regulations.

Most importantly, it is important to remember that the real innovation of Bitcoin is not the currency itself, rather than its underlying technology —the blockchain, a decentralized trust platform. Bitcoin is only one out of many possible applications of this new technology, which can be incorporated into many different types of applications that operate similarly to the Bitcoin blockchain in some respects, and differently in others.

Accordingly, before regulating Bitcoin as a virtual currency, it is necessary to understand the real opportunities that its underlying technologies provides, without getting sidetracked by the crypto-currency hype.

In particular, the blockchain gives rise to new possibilities that were previously impossible – or impractical – and are therefore not fully accounted for in the current regulatory regime.

Looking at financial applications, blockchain technologies can be used to execute more secure and trustless transactions: for example, creating free and secure escrow system with built-in multi-signature features.

Blockchain technologies can also provide a more efficient and secure securities market, by enabling both automatic settlement and clearance by peers, without a centralized clearinghouse. The U.S. Securities and Exchange Commission has understood this and now allows for securities to be issued directly onto the blockchain.

The derivatives market can also be made more efficient and transparent, by encoding the terms of a derivative instrument directly into the blockchain, automating both transactions and payment. A direct monetary connection can be established linking the actual value of collaterals with the derivative, which makes liquidity-freezes like those of 2008 impossible.

Beyond financial applications, the blockchain can also be used as a decentralized and tamper-proof registry of titles, such as a land registry (as the current experiment in Honduras might show) or as a way to record any contractual or licensing agreements, such as intellectual property.

In the context of Internet of Things and smart cities initiatives, it is estimated that there will be over 50 billion interconnected devices in 2020, each needing to communicate and transact with one another. Because no central public or private authority could possibly act as the central clearing for all of these transactions, the blockchain provides an efficient and secure solution to govern and execute trillions of transactions in a trustless manner.

Finally, the most recent versions of the blockchain make it possible to execute complex code, in a decentralized and deterministic manner, without relying on any central server.

This allows for the creation of decentralized applications (such as decentralized market places, or decentralized prediction markets), which are neither owned nor controlled by anyone, but simply subsist on the blockchain, and are executed each time someone interacts with them.

The benefit is that no one can alter the operations of that code —which is actually incorruptible. Besides, as blockchains enable new forms of value creation and distribution within a particular network, they opens up new possibilities for new establishing of decentralized organisation and the generation of social and economic coordination, with greater transparency, lower cost and more equality of access.

However, the problem is that there is no one to be held responsible for the operations of that blockchain code, for better or worse. These applications do not reside in any actual jurisdiction and could therefore be constructed to be agnostic to any jurisdiction's rules.

As with the Internet, it will be nearly impossible to stop all unlawful activities that will be made possible by blockchain technologies. Yet, while governments might not be able to halt the use of these technologies, they could at least limit the adoption, and regulate the development of these technologies.

So how should this regulation look like?