The Revolution will (not) be decentralised: Blockchains

Rachel O'Dwyer
23rd March 2015

The data centre rules.

Decentralised topologies and non-discriminatory protocols have been all but replaced by a recentralisation of infrastructure, as powerful corporations now gatekeep our networks. Everything might be accessible, but this access is mediated by a centralised entity. Whoever controls the data centre exercises political and economic control over communications. It's difficult to see how we can counteract these recentralising tendencies in order to build a common core infrastructure. There are significant barriers in place. This includes the age-old problem of scaling distributed forms of organisation beyond the local. But it also includes barriers in terms of access and control of network resources. There are political and economic constraints governing the ownership and distribution of computational power, servers, bandwidth and energy. While we can access any range of software applications for free, the core network is always substantiated in property and provisioned on a scale that blocks access to all but the most powerful actors.

These centralising tendencies have also reared their head in cryptocurrencies. If Bitcoin was hailed as financially disruptive in much the way that VoIP and mesh networks were thought to be disruptive to cellular, powerful mining pools now control much of the infrastructure and rent-seeking individuals control a lion's share of Bitcoin's value. But we don't need to throw the baby out with the bathwater. While Bitcoin in and of itself may be problematic as an alterative currency, the underlying architecture has potentials not only for the future of money, but also for the future of networked cooperation.

Equality as a standard

Blockchain-based technologies may still have a role to play. They look set to have significant implications for money, for property and for cooperative organisation going forward. For example, there's been some discussion about how the blockchain could support new forms of peer-production, and fully decentralised infrastructures for applications as varied as finance, mesh networks, cloud databases and share economies. The broader implication is that the blockchain could support the activities and resources necessary to the commons, as suggested in this recent article by David Bollier. At the same time, there are a number of other important considerations going forward. These include how key criteria like trust, property and governmentality are architected within a blockchain and what centralising tendencies or emerging possibilities for control might accompany this protocol. A lot of what follows is

pretty speculative, but worth discussing in the context of peer-production.

But first of all, what is the blockchain? The blockchain is the distributed ledger that keeps track of all transactions made using the Bitcoin cryptocurrency. Arguably this is Bitcoin's key innovation, allowing users to transact without the intervention of a trusted third party such as a Central Bank or Federal Reserve. In what is sometimes called the second wave of blockchain innovation, people are now looking at the underlying database as an infrastructure for more than monetary transactions. Just as Bitcoin makes certain financial intermediaries unnecessary, new innovations on the blockchain remove the need for gatekeepers from other processes. The key takeaway is that the blockchain could support not only cryptocurrencies but also other financial instruments like equity, securities and derivatives; smart contracts and smart property; new voting systems; identity and reputation systems; distributed databases; and even the management of assets and resources like energy and water. Because of the way it distributes consensus, it routes around many of the challenges that typically arise with distributed forms of organisation– issues such as how to cooperate, scale and collectively invest in shared resources and infrastructures. There are a number of start-ups and groups currently innovating in this space such as Ethereum, Ripple and Mastercoin.

The Ethereum project really illustrates this possibility to abstract the blockchain from a specifically monetary context to one in which we're thinking about decentralised economies and services more generally. In short, it extends the decentralised capabilities of Bitcoin beyond financial transactions. Bitcoin involves two parameters: a trustless database (more on this later) and a transactions system capable of sending value from place to place. In order to do this, Bitcoin implements a simple scripting language. But this scripting language is limited in terms of what it can do.[1] Bitcoin's scripting language lacks certain fine-grained controls and nuances that might be necessary to provision other services. To do more complicated things, the expectation was that you needed to create an entire meta-protocol layer or even a new blockchain. Ethereum developers recognised that these functions could be implemented and scaled if there was a stronger foundational layer with a powerful scripting language for these protocols to be built on. Ethereum builds a generalised framework that extends the capabilities of the blockchain to allow developers to write new consensus applications. This is a blockchain with a built in Turing-complete programming language, allowing anyone to create applications and rules to support them. In this way, we move beyond monetary transactions towards any number of foreseeable applications.[2]

How the blockchain might support a commons

Some of these applications are still speculative; some of them are already implemented. Potential applications of Ethereum include peer-to-peer forms of cloud computing or Dropbox; incentivised Wi-Fi mesh networking or big data and machine learning; games and gambling; reputation systems; and of course financial applications. Already existing applications include Airlock.me a keyless access protocol; La'Zooz, an alternative ride-sharing application; the Eris stack, a distributed application server; Bitvote a distributed voting system; and Traity and Cryptoswartz, both online reputation systems.

Distributed Organisations & the Trust Web: One significant claim is that blockchain-based technologies such as Ethereum can support and scale distributed forms of cooperation on a global scale. This has been referred to under a few different names: the recent Coin Center report refers to Distributed Collaborative Organisations, while Ethereum's founding developer Vitalik Buterin speaks elsewhere about Decentralised Autonomous Organisations. As David Bollier recently pointed out, this model resonates with organisations that are interested in fostering commons-based peer-production. Where questions about how to reach consensus, negotiate trust and especially scale interactions beyond the local are pervasive in the commons, the blockchain looks set to be a game changer.

In this context, the blockchain is presented as an algorithmic tool to foster trust in the absence of things like social capital, physical colocation or trusted third-party management. These are actually referred to as 'consensus' algorithms, and they are the staple of projects such as Ethereum and Ripple. As David Cohen has described it "Trust, rules, identity, reputation and payment choices are embedded at the peer level. Participants arrive already trusted and decentrally acknowledged". Cohen and Mougayar have dubbed this innovation the "trust web" to describe the new suite of applications that weave network value and consensus into the protocol itself, forgoing the social institutions and relations that were previously mandatory.

Node Incentivisation: Another innovation is that Ethereum incentivises participation, encouraging actors to contribute without introducing centralisation. Ethereum also puts features in place to discourage centralisation in the future. In order to use an Ethereum application, users make micropayments to the developers in ether, Ethereum's coin, or 'cryptofuel' as they term it. This might be making a micropayment in turn for storage space on a server or for acting as a relay in a mesh networking protocol. For example, in a hypothetical Ethereum mesh network, anybody could act as a node, charging small amounts for relaying people's messages (in the region of a few microcents per kb) and alternatively paying to have their own messages relayed. We can take this further and reward people for other kinds of contributions, such as writing source code or producing creative content on a

website. Monetary transactions aside, this encourages people to contribute to the commons and puts systems in place to try and protect its resources from commercial expropriation.

Decentralised Infrastructures: A third significant innovation is a change to infrastructure. Ethereum describes itself as "an infrastructure for next generation social and economic systems". Blockchain innovations that manage networks, servers or natural resources really do radicalise infrastructure. We're no longer speaking about monolithic resources with prohibitive barriers to entry, the quintessential server farm housed in some distant industrial estate. Instead, we can imagine infrastructure as something immaterial and dispersed, or managed through flexible and transient forms of ownership. Where powerful servers, channels and processing capacities seem like the primary chokepoint of open networks, the blockchain is a powerful antidote. As Buterin argues in a recent interview:

We would build a decentralised Internet network where all of us would access documents and content without going through a server. It means that you will need zero infrastructure to develop and distribute applications.
The payoff seems to be that new blockchain-based technologies have the potential to support new forms of commons-based peer production, supplying necessary tools for cooperation and decision making, supporting complementary currencies and even provisioning infrastructures.

Trust in the code

At this early stage of development, it's also crucial to think about how criteria like governance, property relations and modes of production are engineered into the blockchain, and what centralising tendencies or emerging possibilities for control might accompany this protocol. The issue most frequently cited has to do with the difficulty of regulating rogue companies in a distributed system. Primavera de Filippi, a researcher at the forefront of legal challenges in distributed organisation, points to the difficulty regulating companies and identifying who or what is in charge when things go wrong. The blockchain is still anybody's baby and not the exclusive bequest of groups working towards a decentralised Internet or a 'Post-Snowden' Internet economy. Companies from share economy start-ups to major players in IT are looking to the blockchain for their next meal ticket. IBM, for example, is currently in talks about a blockchain-tied cash system with a number of central banks.

Other issues concern the design of trustless architectures and smart property.

Trustless Architectures: First of all, what kind of subjectivity does the blockchain support? In the development of consensus algorithms and monetary incentives, there's an assumption that we can delegate much of the messiness

of human relations to algorithmic governance, anticipate the motivations of individual actors and foreclose destructive behaviours. This comes back to this question of trust, something I've already written about in relation to Bitcoin. The claim being made is not that we can engineer trust in friends, institutions or governments, but that we might dispense with them altogether in favour of what Bill Maurer, Taylor C. Nelms and Lana Swartz refer to as 'trust in the code.' As outlined in the Bitcoin whitepaper, proof-of-work is not a new form of trust, but the abdication of trust altogether as social confidence in favour of an algorithmic regulation. In other words, it doesn't matter whether I believe in my fellow peers just so long as I believe in the technical efficiency of the blockchain protocol.

What kinds of subjectivity do we want to algorithmically inscribe into our systems? Blockchain start-ups begin from the assumption that there is no trust and no community, only individual economic agents acting in self-interest. Fair enough, you might think, it's precisely the fact that projects like Ethereum engineer confidence and provide economic incentives for contribution that may distinguish it from other services like Freenet. But it also proceeds from a perspective that *already presumes* a neoliberal subject and an economic mode of governance in the face of social and/or political problems. 'How do we manage and incentivise individual competitive economic agents?' In doing so, it not only *codes* for that subject, we might argue that it also *reproduces* that subject.[3]

Smart Property: Innovations in property and infrastructure also seem to go both ways. While greater flexibility around ownership of core infrastructure is arguably a good thing, the introduction of artificial scarcity and the new controls implied by smart property also have worrying implications for Internet copyright and Digital Rights Management. Property doesn't disappear, but instead it is enforced and exercised in different ways. If rights were previously exercised through norms, laws, markets and architectures, today they are algorithmically inscribed in the object.

Going forward, it's clear that there are a number of considerations to take into account, foremost not only how we provision the necessarily technical tools or resources for building a commons, but how we work to cultivate the necessarily kinds of social relations and subjectivity that might accompany this shift. There is real potential in the blockchain if we appreciate it not as some ultimate techno-fix but as a platform that, when combined with social and political institutions, has real possibilities for the future of organisation.

[1] It can't support more complicated forms of joint accounts or savings for example.
[2] For more on this see the Ethereum Whitepaper.
[3] This is similar to criticisms that are sometimes made of Elinor Ostrum's approach to governing the commons.