POLICY PAPER 02 / 2015

BRETT SCOTT

VISIONS OF A TECHNO-LEVIATHAN

THE POLITICS OF THE BITCOIN BLOCKCHAIN

In Kim Stanley Robinson's epic 1993 sci-fi novel *Red Mars,* a pioneering group of scientists establish a colony on Mars. Some imagine it as a chance for a new life, run on entirely different principles from the chaotic Earth. Over time, though, this illusion is shattered as multinational corporations operating under the banner of governments move in, viewing Mars as nothing but an extension to business-as-usual.

It is a story that undoubtedly resonates with some members of the Bitcoin community. They see the vision of a free-floating, digital economy based around a cryptocurrency – a decentralised currency that uses encrypted transactions, and a public ledger of all such transactions (Bitcoin's blockchain) that is divorced from the politics of colossal banks and aggressive governments – as under threat. Take, for example, the purists at Dark Wallet,[1] who accuse the Bitcoin Foundation[2] of selling out to the regulators and the likes of the Winklevoss twins.[3]

Bitcoin sometimes appears akin to an illegal immigrant trying to decide whether to seek out a rebellious existence in the black-market economy, or whether to don the slick clothes of the Silicon Valley establishment. The latter position – involving publicly accepting regulation and tax whilst privately lobbying against it – is obviously more acceptable and familiar to the authorities.

Of course, any new scene is prone to developing internal echo chambers that amplify both commonalities and differences. While questions regarding Bitcoin's regulatory status lead hyped-up cryptocurrency evangelists to engage in intense sectarian debates, to many onlookers Bitcoin is just a passing curiosity, a damp squib that will eventually suffer an ignoble death by media boredom. This belief is mistaken. Bitcoin's core innovation is not going away, and it is deeper than currency.

What Bitcoin has introduced to the world is a method to create *decentralised peer-validated time-stamped ledgers.* That is a fancy way of saying it is a method of bypassing the use of centralised officials to record information. Such officials are pervasive in society, from a bank that records electronic transactions between me and my landlord, to patent officers who record the date of new innovations, to parliamentary registers noting the passing of new legislative acts.

The most visible use of this technical accomplishment is in the realm of currency, though, so it is worth briefly explaining the basics of Bitcoin[4] in order to understand the political visions being unleashed as a result of it.

THE TECHNICAL VISION 1.0

Banks are information intermediaries. Gone are the days of the merchant dumping a hoard of physical gold into the vaults for safekeeping. Nowadays, if you have '£350 in the bank', it merely means the bank has recorded that for you in their data centre, on a database that has your account number and a corresponding entry saying '350' next to it. If you want to pay someone electronically, you essentially send a message to your bank, identifying yourself via a pin or card number, asking them to change that entry in their database and to inform the recipient's bank to do the same with the recipient's account.

Thus, commercial banks collectively act as a cartel controlling the recording of transaction data, and it is via this process that they keep score of 'how much money' we have. To create a secure electronic currency system that does not rely on these banks thus requires three interacting elements. First, the private databases that are controlled by them need to be replaced. Second, a way needs to be found for people to change the information on that database ('move money around'). Third, people need to be convinced that the units being moved around are worth something.

To solve the first element, Bitcoin provides a public database, or ledger, that is referred to reverently as the *blockchain.* There is a way for people to submit information for recording in the ledger, but once it gets recorded, it cannot be edited in hindsight. If you've heard about Bitcoin 'mining' (using 'hashing algorithms'), that is what that is all about. A scattered collective of mercenary clerks essentially hire their computers out to collectively maintain the ledger, baking (or weaving)[5] transaction records into it.

Second, Bitcoin has a process for individuals to identify themselves in order to submit transactions to those clerks to

ROSA LUXEMBURG STIFTUNG

be recorded on that ledger. That is where public-key cryptography comes in. I have a public Bitcoin address (somewhat akin to my account number at a bank) and I then control that public address with a private key (a bit like the way I use my private pin number with my bank account). This is what provides anonymity.

The result of these two elements, when put together, is the ability for individuals to anonymously record transactions between their Bitcoin accounts on a database that is held and secured by a decentralised network of techno-clerks ('miners'). As for the third element – convincing people that the units being transacted are worth something – that is a more subtle question entirely[6] and I will not address it here.

THE POLITICAL VISION 1.0

Note the immediate political implications. Within the Bitcoin system, a set of powerful central intermediaries (the cartel of commercial banks, connected together via the central bank, underwritten by government), is replaced with a more diffuse *network intermediary,* apparently controlled by no-one.

This generally appeals to people who wish to devolve power away from banks by introducing more diversity into the monetary system. Those with a left-wing, anarchist bent, who perceive the state and banking sector as representing elite interests, may recognise the potential within Bitcoin for collective direct democratic governance of currency. However, it also really appeals to conservative libertarians who perceive Bitcoin as a commodity-like currency,[7] free from the evils of a central bank and regulation.

The political reaction from policy-makers and establishment types takes three immediate forms. First, there are concerns about Bitcoin being used for money laundering and crime ('Bitcoin is the dark side'). Second, there are concerns about consumer protection ('Bitcoin is full of cowboy operators'). Third, there are concerns about tax ('Bitcoin enables people to evade tax').

The general bias of regulators towards the status quo leads them to become fixated on the negative aspects of Bitcoin whilst remaining blind to the negative features of the current system; this sets the stage for a political battle. Bitcoin enthusiasts, passionate about protecting the niche they have carved out, become prone to imagining conspiratorial scenes of threatened banks fretfully lobbying the government to ban Bitcoin, or of paranoid politicians panicking about the integrity of a national currency.

THE TECHNICAL VISION 2.0

Beyond the media hype associated with these Bitcoin dramas, a deeper movement is developing. It focuses not only on Bitcoin's potential to disrupt commercial banks, but also on the more general potential for *decentralised blockchains* to disrupt other types of centralised information intermediaries.

Copyright authorities, for example, record people's claims to having produced a unique work at a unique date and authoritatively stamp it for them. This form of centralised 'time stamping' is more generally known as 'notarisation'. One non-monetary function for a Bitcoin-style blockchain could thus be replacing the privately controlled ledger of the notary with a public ledger on which people can record their claims. This is precisely what Proof of Existence[8] and Originstamp[9] are working on.

What about domain name system (DNS) registries that record web addresses? When you type in a URL such as www.e-ir.info, your browser first steers you to a DNS registry such as Afilias[10] that maintains a private database of URLs alongside information on which IP address to direct you to. However, a blockchain could also be used to create a decentralised registry of domain name ownership, which is what Namecoin[11] is doing. Theoretically, this process could be used to record share ownership, land ownership, or ownership in general (see, for example, Mastercoin's projects).[12]

The biggest information intermediaries, though, are often hidden in plain sight. What is Facebook? Is it not just a company that you send information to which is then stored in their database and subsequently displayed to you and your friends? You log in with your password (proving your identity), and then you can alter the database by sending further messages ('delete that photo'). The same can be said of Twitter, Dropbox and countless other web services.

Unlike the original internet, which was largely used for the transmission of static content, we experience sites like Facebook as interactive playgrounds where we can use programs installed on far-away computers. In the process of such interactivity, we give groups such as Facebook *huge* amounts of information. Indeed, they set themselves up as *information honeytraps* in order to create a profit-making platform where advertisers can sell users things based on this information. This simultaneously creates a large information repository for authorities such as the NSA to browse. This interaction of corporate power and state power is inextricably tied to the profitable nature of centrally held data.

But what if you could create interactive web services that did not revolve around single information intermediaries like Facebook? That is precisely what groups such as Ethereum[13] are working towards. Whereas Bitcoin is a method of recording simple transactional information on a decentralised ledger, Ethereum wants to create a 'decentralised computational engine': a system for running programs, or executing contracts, on a blockchain held in play via a distributed network of computers rather than Mark Zuckerberg's data centres.

It all starts to sounds quite sci-fi, but organisations such as Ethereum are leading the charge on building 'decentralised autonomous organisations'[14] – hardcoded entities that people can interact with, but that nobody in particular controls. I send information to this entity, triggering the code and setting in motion further actions. As Bitshares[15] describes it, such an organisation "has a business plan encoded in open source software that executes automatically in an entirely transparent and trustworthy manner."

THE POLITICAL VISION 2.0

By removing a central point of control, decentralised systems based on code – whether they exist to move Bitcoin tokens around, store files, or build contracts – resemble self-contained robots. Mark Zuckerberg of Facebook or Jamie Dimon of JP Morgan Chase are the human faces behind the digital interface of the services they run. They can overtly manipulate, or bow in to pressure to censor. A decentralised currency or a decentralised version of Twitter[16] seems immune to such manipulation.

It is this that gives rise to a narrative of empowerment and, indeed, at first sight this offers an exhilarating vision of self-contained outposts of freedom within a world otherwise

dominated by large corruptible institutions. At many cryptocurrency meet-ups, there is an excitable mix of techno-babble infused with social claims. The blockchain can record contracts between free individuals, and if enforcement mechanisms can be coded in to create self-enforcing 'smart contracts', we have a system for building encoded law that bypasses nation-states.

Bitcoin and other blockchain technologies are empowering precisely because they are underdogs. They introduce diversity into the existing system and thereby expand our range of tools. In the minds of hardcore proponents, however, blockchain technologies are more than this. They represent a *replacement system,* and one that is superior to existing institutions in every possible way. Yet when amplified to this extreme, the apparently utopian project can begin to take on a dystopian, conservative hue.

BINARY POLITICS

When asked about why Bitcoin is superior to other currencies, proponents often point to its *'trustless'* nature.[17] No trust needs be placed in fallible 'governments and corporations'. Rather, a self-sustaining system can be created by individuals following a set of rules that are set apart from human frailties or intervention. Such a system is assumed to be fairer because it enables people to win out against those powers who can abuse rules.

The vision is not one of bands of people getting together into mutualistic self-help *groups.* Rather, it is one of *individuals* acting as autonomous agents, operating via hardcoded rules with other autonomous agents, thereby avoiding those who seek to harm their interests.

Note the underlying dim view of human nature. Whereas anarchist philosophers often imagine alternative governance systems based on mutualistic community foundations, the 'empowerment' in trustless relations does not stem from building community ties. Rather, it is imagined as based on the retreat from trust and the refuge found in defensive individualism mediated via mathematical contractual law.

It carries a certain disdain for human imperfection, particularly the imperfection of those in power, but by implication the imperfection of everyone in society. We need to be protected from ourselves by vesting power in lines of code that execute automatically. If only we could lift currency away from manipulation by the Federal Reserve. If only we could lift Wikipedia away from the corruptible Wikimedia Foundation.

Activists traditionally revel in hot-blooded asymmetric battles of interest (such as that between StrikeDebt![18] and the banks), implicitly holding an underlying faith in the redeemability of human-run institutions. The Bitcoin community, on the other hand, often seems attracted to a detached anti-politics, one in which action is reduced to the binary options of *Buy In* or *Buy Out* of the coded alternative. It echoes consumer notions of the world, where one 'expresses' oneself not via debate or negotiation, but by choosing one product over another: We're leaving Earth for Mars. Join if you want.

It all forms an odd, tense amalgam between visions of exuberant, risk-taking freedom and visions of risk-averse anti-social paranoia. This ambiguity is not unique to cryptocurrency (an excellent parody of the trustless society has recently been published on Youtube),[19] but in the case of Bitcoin, it is perhaps best exemplified by the narrative offered by Cody Wilson in Dark Wallet's crowdfunding video: "Bitcoin is what they fear it is, a way to leave […] to make a choice. There's a system approaching perfection, just in time for our disappearance, so, let there be dark".[20]

THE MYTH OF POLITICAL 'EXIT'

But where exactly is this perfect system Wilson is disappearing to? Back in the days of roving bands of nomadic people, the option of a political 'exit' was a reality. If a ruler was oppressive, you could actually pack up and take to the desert in a caravan. The bizarre thing about the concept of 'exit to the internet' is that the internet is a technology premised on massive state and corporate investment in physical infrastructure, fibre optic cables laid under the seabed, the mass production of computers by low-wage workers in the East, and mass affluence in Western nations. If you are in the position to dream of technological escape, you are probably not in a position to be exiting mainstream society: you are mainstream society.

Do not get me wrong. Wilson is a subtle and interesting thinker,[21] and it would be unfair to suggest that he really believes it is possible to escape the power dynamics of the messy real world by finding salvation in a kind of internet Matrix. What he is really trying to do is to invoke one side of the crypto-anarchist mantra of *'privacy for the weak, but transparency for the powerful'.*

That is a healthy, radical impulse, but the conservative element kicks in when the assumption is made that somehow privacy alone is what enables social empowerment. That is when it turns into an individualistic 'leave me alone' impulse fixated on negative freedom. Despite the rugged frontier appeal of the concept, the presumption that empowerment simply means being left alone to pursue your individual interests is essentially an ideology of the already-empowered, not the vulnerable.

This is the same tension found in the closely related cypherpunk movement.[22] It is often pitched as a radical empowerment movement, but as Richard Boase notes, it is "a world full of acronyms and codes, impenetrable to all but the most cynical, distrustful, and political of minds."[23] Indeed, crypto-geekery offers nothing like an escape from power dynamics. One merely escapes to a different set of rules, not one controlled by 'politicians', but one in the hands of programmers and those in control of computing power.

It is only when we think in these terms that we start to see Bitcoin not as a realm 'lacking the rules imposed by the state', but as a realm imposing its own rules. It offers a *form* of protection, but guarantees nothing like 'empowerment' or 'escape'.

TECHNO-LEVIATHAN

Technology often seems silent and inert; a world of 'apolitical' objects. We are thus prone to being blind to the power dynamics built into our use of it. For example, is email not just a useful tool? Actually, it is highly questionable whether one can 'choose' whether to use email. Sure, I can choose between Gmail and Hotmail, but email's widespread uptake creates network effects that mean opting out becomes less of an option over time. This is from where the concept of becoming 'enslaved to technology' emerges. If you do not buy into it, you *will* be marginalised, and that *is* political.

While individual instances of blockchain technology can clearly be useful, as a *class* of technologies designed to mediate human affairs, they contain a latent potential for

encouraging technocracy. When disassociated from the programmers who designed them, trustless blockchains floating above human affairs contain the spectre of *rule by algorithms.* It is a vision (probably accidently) captured by Ethereum's Joseph Lubin when he says, "There will be ways to manipulate people to make bad decisions, but there won't be ways to manipulate the system itself".[24]

Interestingly, it is a similar abstraction to that made by Hobbes. In his *Leviathan,* self-regarding people realise that it is in their interests to exchange part of their freedom for security of self and property, and thereby enter into a contract with a *sovereign,* a deified personage that sets out societal rules of engagement. The definition of this sovereign has been softened over time – along with the fiction that you actually contract to it – but it underpins modern expectations that the government should guarantee property rights.

Conservative libertarians hold tight to the belief that if only hard property rights and clear contracting rules were to be put in place, optimal systems would spontaneously emerge. They are not actually that far from Hobbes in this regard, but their irritation with Hobbes' vision is that it relies on politicians who, being actual people, do not act in the manner in which a detached contractual sovereign should, but rather attempt to meddle, make things better, or steal. Do decentralised blockchains offer the ultimate prospect of protected property rights with clear rules, but without political interference?

This is essentially the vision of the internet *techno-leviathan,* a deified crypto-sovereign whose rules we can contract to. These rules are a series of algorithms: they represent step-by-step procedures for calculations that can only be overridden with great difficulty. Perhaps, at the outset, this represents, à la Rousseau, the *general will* of those who take part in the contractual network, but the key point is that if you become locked into a contract on that system, there is *no breaking out of it.*

This, of course, appeals to those who believe that powerful institutions operate primarily by *breaching* property rights and contracts. Who *really* believes that though? For much of modern history, the key issue with powerful institutions has not been their willingness to break contracts. It has been their willingness to *use* seemingly unbreakable contracts to exert power. Contracts, in essence, resemble algorithms, coded expressions of what outcomes should happen under different circumstances. On average, they are written by technocrats and, on average, they reflect the interests of elite classes.

That is why liberation movements have always sought to break contracts set in place by old regimes, whether they are peasant movements refusing to honour debt contracts, property owners, the DRC challenging legacy mining concessions held by multinational companies, or SMEs contesting the terms of swap contracts[25] written by lawyers for Barclays. Political liberation is as much about contesting contracts as it is about enforcing them.

BUILDING THE TECHNO-POLITICAL VISION 3.0

The point I am trying to make is that you do not escape the world of big corporates and big government by wishing for a trustless set of technologies that collectively resemble a technocratic crypto-sovereign. Rather, you use technology as a tool within on-going political battles, and you maintain an on-going critical outlook towards it. The concept of the decentralised blockchain is powerful. The cold, distrustful edge of cypherpunk, though, is only empowering when it is firmly in the service of creative warm-blooded human communities situated in the physical world of dirt and grime.

Perhaps this means de-emphasising the focus on how blockchains can be used to store digital assets or property,[26] and focusing on those without assets. For example, think of the potential of *blockchain voting systems* with which groups like Restart Democracy[27] are experimenting. Centralised vote-counting authorities are notorious sources of political anxiety in fragile countries. What if the ledger recording the votes cast was held by a decentralised network of citizens, with voters having a means to anonymously transmit votes to be stored on a publicly viewable database?

I would argue against both a future society free from people we have to trust, and one in which the most we can hope for is privacy. Rather, technology should be used to dilute the power of those systems that cause us to doubt relationships built on trust. Screw escaping to Mars.

Brett Scott is the author of *The Heretic's Guide to Global Finance: Hacking the Future of Money* (Pluto Press: 2013). He has written for publications including *The Guardian, New Scientist* and *Wired Magazine,* and he blogs on alternative finance at www.suitpossum.blogspot.com. He tweets at @Suitpossum.

1 https://www.indiegogo.com/projects/bitcoin-dark-wallet/ **2** https://bitcoinfoundation.org/ **3** http://www.cnbc.com/id/101372209/ **4** http://suitpossum.blogspot.co.uk/2013/04/how-to-explain-bitcoin-to-your.html/ **5** http://bitcoinmagazine.com/12311/weaving-better-metaphor-bitcoin-instead-mining/ **6** http://aeon.co/magazine/living-together/so-you-want-to-invent-your-own-currency/ **7** In conservative libertarian circles, Austrian economic ideas of 'sound money' often hold sway. Gold, silver and other commodities with limited supply are presented as 'real' money and contrasted with 'fraudulent' government fiat money and commercial bank money created under the fractional reserve banking system. In such circles, Bitcoin is often perceived as a form of digital gold. **8** http://www.proofofexistence.com/ **9** http://www.originstamp.org/ **10** http://www.info.info/about/ **11** http://www.coindesk.com/what-are-namecoins-and-bit-domains/ **12** http://www.mastercoin.org/ **13** https://www.ethereum.org/ **14** http://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/ **15** http://bitshares.org/ **16** http://twister.net.co/ **17** http://www.thebitcoinsociety.org/content/bitcoin-beauty-trustless-transactions/ **18** http://strikedebt.org/ **19** https://www.youtube.com/watch?v=z5Otla-5157c/ **20** https://www.indiegogo.com/projects/bitcoin-dark-wallet/ **21** https://www.youtube.com/watch?v=wlJThk-eTAM/ **22** An anti-surveillance movement that advocates the use of cryptography to protect against the prying eyes of the authorities. **23** http://www.cybersalon.org/cypherpunk/ **24** http://www.theepochtimes.com/n3/665367-bitcoin-2-0/ **25** http://www.risk.net/risk-magazine/feature/2196423/uk-banks-face-up-to-sme-swap-misselling-claims/ **26** http://www.theepochtimes.com/n3/665367-bitcoin-2-0/ **27** http://restartdemocracy.org/

IMPRINT

POLICY PAPER is published by the Rosa-Luxemburg-Stiftung
Responsible: Henning Heine
Franz-Mehring-Platz 1 · 10243 Berlin, Germany · www.rosalux.de
ISSN 1867-3163 (Print), ISSN 1867-3171 (Internet)
Editorial deadline: February 2015
Proofreading: Simon Phillips, Berlin
Setting/Production: MediaService GmbH Druck und Kommunikation
Printed on Circleoffset Premium White, 100 % recycled paper