Bitcoin beyond ambivalence

DOI:
10.1177/0725513616689390

Document Version
Accepted author manuscript

Link to publication record in Manchester Research Explorer

Citation for published version (APA):

Published in:
Thesis Eleven

Citing this paper
Please note that where the full-text provided on Manchester Research Explorer is the Author Accepted Manuscript or Proof version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version.

General rights
Copyright and moral rights for the publications made accessible in the Research Explorer are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Takedown policy
If you believe that this document breaches copyright please refer to the University of Manchester's Takedown Procedures [http://man.ac.uk/04Y6Bo] or contact uml.scholarlycommunications@manchester.ac.uk providing relevant details, so we can investigate your claim.
Abstract

In the aftermath of the 2008 financial crisis, Bitcoin emerged as an alternative monetary system that could circumvent political and financial authorities. A practice in libertarian prefigurative politics, Bitcoin demonstrates the capacity for online subgroups to creatively appropriate internet-based technologies to enact alternative futures. Andrew Feenberg’s critical theory of technology clarifies this capacity and outlines the significance of agency in technical action. As technology mediates many social relations, it has a significant role in the reproduction of social power. Technological agency is therefore a crucial site of resistance in which users can form alternative, democratic rationalisations of technology. Yet are such instances of agency intrinsically democratic? In analysing this aspect of Feenberg’s theory, this article argues that Bitcoin represents a ‘popular rationalisation’ of technology – a creative appropriation of technology that empowers some groups while lacking the ethical justification necessary to be considered democratic.

Key words: Critical theory, technological agency, Bitcoin, blockchain technology.

Introduction

On January 14th 2016 Mike Hearn, an influential software engineer who had spent over five years as a Bitcoin developer, announced he was ending his involvement with the technology. Bitcoin, he said, was an experiment which had failed: “It has failed because the community has failed. What was meant to be a new, decentralised form of money that lacked ‘systemically important institutions’ and ‘too big to fail’ has become something even worse: a system controlled by just a handful of people. Worse still, the network is on the brink of technical collapse” (Hearn 2016). Bitcoin’s success as an alternative monetary system, Hearn explained, had been thwarted by social forces. What had originated as a libertarian instance of prefigurative politics had been challenged by the actions of various social groups, many motivated by alternative visions for the technology that contested those in its initial design. Andrew Feenberg’s critical theory of technology offers an incisive means for interpreting these processes. In this paper, I present the value of Feenberg’s theory for understanding the ways in which particular subgroups are able to appropriate various technical innovations to advance their interests. Ultimately, I argue that the meaning of Bitcoin remains contested, yet while it remains in a stage of interpretive flexibility, articulations of the technology are often neither democratic nor progressive, and while they may empower some groups, they lack the ethical justification necessary to be considered democratic. This brings into question aspects of Feenberg’s theoretical vocabulary, to which I propose the concept of popular rationalisation.

Feenberg’s critical theory is presented in three major works, A Critical Theory of Technology (1991), Alternative Modernity (1995), and Questioning Technology (1999). His analysis of contemporary power structures is one of technocracy, at the heart of which lies the capacity of industry and institutions to reproduce the conditions of their supremacy, unchallenged by the interests of subordinate actors. Technocracy thus underpins social inequalities for Feenberg, and in this analysis of power structures technological agency, the capacity to influence technical design, becomes a principal mode of resistance. Technology must be democratised. But what exactly is meant here by democratic? Are instances of technological agency intrinsically democratic? The first section of this article presents these aspects of Feenberg’s work in more depth. After outlining Feenberg’s insightful account of modern technocracy, this section examines Feenberg’s proposed models for its resistance.
The second section of the article outlines the technical architecture of Bitcoin, drawing on Feenberg’s theory to examine the role of social imperatives in design. Bitcoin illustrates how a subgroup of internet users, brought together through their shared values and relations to technology, were able to reimagine and repurpose particular innovations to advance their aims of creating a new and alternative monetary system. The terminology used in design, as well as the practices outlined for its users, reveal design choices intended to extend a particular set of interests and definitions. While this empowers those that share such interests, it fails to challenge the normative elements of ‘hegemonic technological rationality’: the production of techniques that mediate social relations with no obligation to seek ethical justification or regard the moral or political consequences upon subordinate groups. I therefore argue that Bitcoin demonstrates an instance of creative appropriation that does not challenge technological hegemony.

In the third section of this article, the contested meaning of Bitcoin is presented among different users and social groups. Drawing on primary research into Bitcoin users, this section details the difficulties and changes experienced by those endeavouring to advance Bitcoin as an alternative monetary system. I argue that, while interest from financial firms and institutions appears to be redefining Bitcoin as ‘blockchain technology’ and adapting it to new purposes, the technology is not yet a technique for reproducing the supremacy of these organisations. Nor however, was it ever a counter-hegemonic practice. Instead, Bitcoin represents a complex case of popular rationalisation, in which various groups have appropriated the technology for particular purposes, yet these are often neither democratic nor progressive. In light of these findings, I conclude by proposing a change in Feenberg’s theoretical vocabulary to include more focus on the political ambivalence of appropriation; and to consider a concept of popular rationalisation, to account for such instances of creative appropriation that are not of themselves democratic.

---

I – Technological Agency

Why has democracy not been extended to technically mediated domains of social life despite a century of struggles? Is it not because technology is incompatible with democracy or because it has been used to suppress it? The weight of the argument supports the second conclusion. Technology can deliver more than one type of technological civilization. We have not yet exhausted its democratic potential – Andrew Feenberg (2010: 29)

Feenberg’s critical theory of technology can broadly be outlined in two key aims: to demystify the processes of technological development; and to determine models for democratising technology. As technology increasingly mediates social relations, Feenberg argues, it is crucial to understand its role in the reproduction of social power and how it may be opened to more democratic controls and participation. At the heart of Feenberg’s theory is thus a conception of technological agency. Revealing the political processes at play in technology design is the first step in challenging its hegemonic consequences. Feenberg’s critique here opens up visions of an alternative rationality or modernity, in which technological agency is a normative democratic value. In the following, I examine this critique, and Feenberg’s models for democratising technology. Ultimately, I argue that Feenberg’s demystification of technology design remains incisive and crucial in understanding the role of social imperatives in the design of new technologies such as Bitcoin. My criticism is instead directed at his models for democratising technology. Are instances of technological agency intrinsically democratic,
and counter-hegemonic? Do such instances always challenge to hegemonic power? And are the effects of such instances always to democratise technology? In examining Feenberg’s concepts of democratic rationalisation, with particular focus on ‘creative appropriations’, I question Feenberg’s theoretical vocabulary, and propose that while instances of technological agency may represent popular rationalisations, they are not necessarily democratic.

In *Questioning Technology* (1999), Feenberg outlines the social forces active in any given design process. There always exist alternative possibilities in technology design, and the choice between these alternatives “depends neither on the technical nor economic efficiency, but on the ‘fit’ between devices and the interests and beliefs of the various social groups that influence the design process” (1999: 79). Furthermore, there is a political dimension to this process. As the greater part of technological development involves only those that can mobilise considerable resources, this entails the exclusion of many, often those that experience most the effects of new technologies. Examples may range from the design of office workspaces to the development of industrial power plants, in which workers and residents respectively have little influence over the design process. This is rationalised by a dominant understanding of technology as politically neutral, that its progress simply reflects scientific laws of efficiency. This serves to conceal the political processes at play in design and ensures technology is always managed from above. In this way, the rationality governing technology design and development is hegemonic. It is normative that the vast majority of users are excluded from influencing the design of technologies, and this serves to reproduce power as it maintains the privileged position of those that can direct technological development. This normative understanding of technology as politically neutral forms the basis of a rationality which ensures technology exists outside the realms of social critique, even as it mediates social relations through devices that reflect and reproduce social power. Thus,

> Technological rationality is not merely a belief, an ideology, but is effectively incorporated into the structure of machines. Machine design mirrors back the social factors operative in the prevailing rationality (Feenberg, 1992: 310)

Technological rationality is thus an effective hegemony as it reproduces social imperatives with no recourse to democratic processes. Feenberg therefore speaks of *hegemonic technological rationality*, as social forces and technical requirements are condensed within a system of domination. The social imperatives informing technology design are concealed and inequalities are reproduced.

Feenberg describes the processes that have occurred historically under the expansion of capitalism in which capitalist imperatives for increasing control, power, and efficiency have been condensed with technical logic in what he terms the capitalist technical code. The ability of capitalism as a social system to produce strategies of power with no obligation to regard certain consequences, or ‘externalities’, is founded on this rationality. Capitalism is thus freed from such limitations, its dominant operatives, such as managers and technicians, have enhanced *operational autonomy* – the ability to make strategic choices concerning various areas of social life.

> The preservation and enlargement of operational autonomy lies at the heart of the capitalist technical code. Any society in which technical development is governed by this code will exhibit the chief traits of capitalism regardless of its property system or political arrangements (1995: 93)

Technocracy thus underpins social inequalities for Feenberg, and in this analysis technological agency becomes a principal mode of resistance. Forms of democratic intervention in technology design are
necessary for challenging the perpetuation of elite power structures. But what constitutes democratic intervention?

Feenberg offers three particular models for democratising technology. The key outcome is to “open technical issues to general democratic debate and lay out the parameters for official ‘technology assessment’” (1999: 121). Briefly, they consist of (1) controversies, in which attention is drawn to incidents such as environmental or public safety threats, sparking debate and in some cases collective action; (2) public participation in design, in which dialogue is established between developers of technology and communities; and (3) ‘creative appropriations’ in which users are able to ‘reinvent’ technology through appropriating it to new purposes and investing it with new meanings. While other scholars in the field focus on action related to the former two forms of democratisation as means for redirecting technological development (see for example, Hess, 2007), Feenberg has increasingly placed much emphasis on creative appropriations. One of Feenberg’s chief empirical examples for democratising technology is described in such terms, the reimagining of the French Minitel system by groups of users (1995: 161). Moreover,

Feenberg calls the type of democratic rationalisation most relevant to the Internet “creative appropriation,” the process in which users innovate new functionalities for already existing technologies (Bakardjieva & Feenberg, 2002: 187).

The internet allows certain groups to add new socio-technical “layers” to computer networks, forming communities around shared relations to technology that enable them to perceive and actualise alternative meanings and purposes. Feenberg argues this is a democratic process as it opens spaces for collective reflection on technology design, and opportunities to appropriate technology in ways that align with the values and interests of those groups. Yet how exactly, do creative appropriations democratise technology? Can isolated incidents of groups pursuing their particular interests culminate in a more democratic internet? Feenberg’s argument here is built on a conception of tactics and strategies borrowed from Michel de Certeau, and appears to suggest that tactics are intrinsically counter-hegemonic, and thus contain democratic potential.

Feenberg outlines ‘tactics’ as constituting a principle means of subverting technological hegemony in Questioning Technology. With the use of any technology, there exists a ‘margin of manoeuvre’ in which users can push the perceived limits of its functionality and insert new meanings. These are tactics: “Tactics thus differ from outright opposition in that they subvert the dominant codes from within by introducing various unexpected delays, combinations, and ironies into the application of strategies” (1999: 113). Tactics are rooted in a Foucauldian conception of power, and more specifically, in Michel de Certeau’s response to this conception.

In The Practice of Everyday Life (1984) Certeau discusses the ramifications of Foucault’s theory of disciplinary power on human agency. If, as Foucault posits, power in modern societies has shifted away from institutions and is increasingly situated in minuscule techniques – techniques that culminate in widespread practices of domination regulating behaviour, organising space, and producing knowledge – how is it that an entire society can resist being reduced to it? In what ways do human agents resist these techniques? This is the focus of Certeau’s investigation, to “bring to light the clandestine forms taken by the dispersed, tactical, and makeshift creativity of groups and individuals already caught in the nets of ‘discipline’” (1984: xiv). It is within this conceptual framework Feenberg posits the idea of tactical challenges to technological hegemony, an idea that implies users of technology may be able to subtly appropriate the technologies around them, redefining their meanings and functionalities.
Certeau argues the miniscule techniques of Foucault’s theory culminate in practices of domination as they originate from a privileged position in the social system. This position both justifies and informs them through dominant rationalities. Certeau cites the examples of techniques emerging from an enterprise or scientific institution that act, from this privileged base, upon externalities defining them as, for example, ‘competitors’, ‘targets’, or ‘objects of research’. These practices become widespread and begin to ‘inform a system’ (1984, 48): producing knowledge, developing a discourse, becoming dominant and normative. Certeau identifies this process as strategy. Strategy underlies modern political, economic and scientific rationalities. However, Certeau maintains that society always consists of practices that do not inform a system, do not produce knowledge, and yet account for much of social life. These practices, Certeau states, are tactics, scattered techniques and practices ‘dominated but not erased’ by strategy. Strategy defines human action, delimiting its movements in much the same way as the rules of a game or the structure of a language. Tactics are the ways seemingly powerless individuals or groups seek to manipulate these definitions from within; seizing an opportunity to bend the rules of the game, inserting their own meanings and accents into language.

Feenberg sees in these concepts a model for technological agency. Hegemonic technological rationality justifies and informs the spread of techniques that maximise the operational autonomy of capitalist enterprise. This is analogous to De Certeau’s strategy. Technology is presented to everyday users as the complete device, with a designated function, structured around certain activities and within the process of its design capitalist imperatives have played a prominent role. However, these activities and functions are nevertheless carried out by users who have the capacity to appropriate these technologies in various ways; ways of operating technology not intended in its design. This tactical capacity is the ‘margin of manoeuvre’ held by everyday users of technology and it holds political potential. Tactical practices can sometimes ‘inform the system’, revealing alternative potentialities for technology:

Action on the margin may be reincorporated into strategies, sometimes in ways that restructure domination at a higher level, sometimes in ways that weaken its control. Foucault’s “subjugated knowledges” are elaborated in the “space” of tactical involvement, the margin of manoeuvre opened by strategies (Feenberg, 2002: 84-5)

Communities forming around shared relations to internet technologies, therefore, may be able to open up a new ‘truth’ through their tactical practices of creative appropriation, revealing alternative rationalisations that may cumulatively redefine the internet in much the same way users of the Minitel system appropriated it to suit their interests of “amusement, companionship, and sex” (1999: 126).

Feenberg asserts that the internet remains in a stage of ‘interpretive flexibility’ as it has yet to establish a concrete definition and purpose and this makes it particularly open to creative appropriations. Although he warns of encroaching business strategies for defining the internet around market rationality, exemplified in the net neutrality issue, he nonetheless asserts that the internet is still dominated by the free communication of users capable of reinventing it with new meanings and definitions (2012: 11). Achieving technological agency is thus possible for marginal actors through their innovative and creative appropriations of internet technologies. Where these appropriations orientate around the interests of a social group, this can trigger a democratisation of technology, ‘informing the system’.

The rest of this article will focus on a critique of this model for democratising the internet. Drawing on my research into Bitcoin, I argue that while Feenberg is correct in identifying the processes in which marginal actors may bring new meanings and functionalities to technologies, actions on the margin are often not counter-hegemonic. The emergence of Bitcoin illustrates the value of creative
appropriation as a conceptual tool for understanding the capacity of subgroups to innovate new functionalities for internet technologies. This is the subject of the following section, in which an examination of the technical architecture of Bitcoin reveals design choices that reflect the values of a subgroup engaging in prefigurative politics, performing an alternative future of free market relations through innovative practice. The role of social imperatives in design is clear here, and the practices emerging around Bitcoin indicate a reproduction of these values in new contexts. The ramifications of these practices for technological rationality however, remain unclear. An analysis of these practices continues in the third section, in which various usages of Bitcoin are presented. Together, these analyses highlight the need to detach the category of appropriation from the dialectical model of domination, resistance, and transcendence that frames Feenberg’s technical politics.

II – Technical Architecture

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party – Satoshi Nakamoto (2008)

The design for Bitcoin, first put forward in a white paper posted to the Cryptography mailing list at metzdowd.com in 2008¹, brings together technical elements from earlier projects discussed on the site, with other innovations for publishing digital documents and encrypting communication. The technical architecture of Bitcoin reveals a collaborative effort on the part of internet users brought together through their shared values and relations to technology. These values shaped the ways in which the technology, in each of its components, was interpreted by early users. The terminology used in design, as well as the practices outlined for its users, are decisive design choices that continue to maintain a definition of this ambivalent technology as a new monetary system. This section draws on Feenberg’s theory to examine the ways in which a subgroup of internet users creatively appropriated encryption techniques as a means to engage in prefigurative libertarian politics. Ultimately, I argue that Bitcoin demonstrates an instance of creative appropriation that sits uneasily with Feenberg’s concept of democratic rationalisation.

The Cryptography mailing list was a forum for discussion on the “technical aspects of cryptosystems, social repercussions of cryptosystems, and the politics of cryptography”¹°. Cryptosystems are a means of securing information across a computer network through the use of algorithms that convert plaintext (data that needs protecting) to ciphertext (encrypted data) and back again. Crucially, the ability to encrypt and decrypt lies only with those that possess the cryptographic key that can trigger this conversion process¹¹. Through the individual possession of cryptographic keys, cryptosystems were perceived by subscribers to Cryptography as a means of shifting power away from large centralised organisations entrusted with protecting data, to the individual.

The archives of Cryptography reveal connections to other mailing lists associated with Cypherpunk activists – a subculture committed to creating cryptosystems that challenge those run by powerful organisations, organisations they see as threatening the privacy and security of individuals. Of these alternative networks, an electronic payments system that encrypted user information and did not require banks was a central aim. As Eric Hughes stated in the Cypherpunk Manifesto (1993), “Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with

¹ For detail on the cryptography of Bitcoin, and its position within a history of encryption technologies, see Du Pont, Q. (2014)
cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.” A system of electronic money that was encrypted and decentralised would remove the need to trust in powerful organisations to record and store the financial information of private individuals.

The key innovation put forward in the Bitcoin white paper was the design of a network that could provide proof of publication without third party verification. This posed a solution to a key issue for Cypherpunks, as it theoretically allowed for a system in which users themselves would record and verify transactions. This issue was often referred to as the ‘double spend problem’, as systems without a central authority recording transactions suffered from an inability to prevent users publishing multiple transactions simultaneously – effectively spending the same tokens multiple times. A similar achievement of the Bitcoin design was to affirm an interpretation of digital signatures as ‘coins’. In doing so, it was possible to project a libertarian monetary theory chiefly oriented around precious metals onto a system of digital signatures. The significance of this latter achievement is rarely discussed, yet it stands out as a pivotal moment in which social values were condensed with technical logic. After outlining the functionality of Bitcoin, I focus on this aspect of social imperatives guiding design.

The design for Bitcoin orientates around two functionalities: a public ledger system, in which the responsibility to record and verify information published to the network is shared among users; and an incentive structure, which encourages nodes in the network to participate in its maintenance. The former functionality has come to be known as the ‘blockchain’, although this term was not used in the original design. The latter function was from the outset named ‘mining’, intentionally drawing upon a lexicon for uncovering precious metals.

The public ledger functionality brought together elements of previous innovations in decentralised networks built on cryptography, chiefly Adam Back’s ‘HashCash’, and Stuart Haber and W. Scott Stornetta’s ‘time-stamp server’. Haber and Stornetta’s time-stamp server was originally designed as a means of protecting intellectual property rights in “a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media” (1991: 0). They proposed a network in which a decentralised server could record information securely and verifiably, through the use of a cryptographic hash function. Hashes are a form of encryption commonly used in data storage, as large amounts of information (strings of data) can be reduced to much smaller fixed values. They also act as a security mechanism: while it is relatively simple for a computer to recognise that a hash accurately contains the data it is supposed to, the function is practically impossible to invert.

In the original white paper for Bitcoin, Satoshi Nakamoto states “the solution we propose begins with a timestamp server” (2008: 2). Nakamoto’s insight was to employ Haber and Stornetta’s innovation as currency. A cryptographic hash function, instead of timestamping digital documents, would timestamp digital account balances. This would ensure all digital signatures – or recorded transactions – would be near-impossible to duplicate or manipulate. It would do this by ensuring that each new digital signature submitted to the server included all the information of previous transactions: “each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it” (ibid: 2)

---

2 The role of Bitcoin in the Cypherpunk movement is discussed in Assange, J. (2012)

3 At the time of writing the true identity of Nakamoto is still unconfirmed, although current evidence now strongly suggests Australian cryptographer Craig Wright. Andrew O’Hagan presents this evidence in a publication for the London Review of Books, accessible here: [http://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair](http://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair) (accessed 21/06/16).
This provided a public ledger system to solve the ‘double-spending problem.’ The responsibility for recording and verifying transactions would be shared among nodes in the network, and cryptography would protect against fraudulent actions. However, this process was decentralised but not automated. To function, it required constant maintenance by nodes in the network. Nakamoto proposed to solve this via an incentive structure.

Nakamoto’s incentive structure built on Adam Back’s (2002) Hashcash model. Back had proposed a system in which sending data across a network was a costly process. For data to be confirmed on the network and sent, a cryptographic test had to be solved. A set of conditions were set in the Hashcash algorithm, and for data to be accepted, a hash must be generated by a user’s computer that met these conditions.

Generating a hash involved ‘brute computational force’. A computer would generate thousands of hashes until one matched the conditions set in the algorithm. Difficulty was therefore set in the core algorithm by making the conditions harder or easier to meet, calculated by the probable time it would take a computer to generate enough hashes. Back’s original proposal was to use this system to combat email spam. The hash function would require an amount of processing time small enough to go by unnoticed by a node sending one email, yet large enough to obstruct a node attempting to send multiple emails at once.

The use of Back’s proof-of-work model allowed Nakamoto to set particular conditions in the cryptographic hash function underpinning the ledger. Nodes in the network would hash together and timestamp blocks of transaction information. If their hash met the conditions set in the algorithm, it would be accepted. Once achieved, a successful hash would be broadcast to the network and nodes could check that the hash did indeed meet the conditions. Compressed into this successful hash would be transaction information, a hash of the previous block, a timestamp signalling when the conditions were successfully met, and all of the generated hashes representing the ‘proof-of-work’ carried out. Nodes in the network confirm their acceptance of the block by incorporating this successful hash into their ongoing process. It would make up the first part of their pursuit to confirm the next block.

To incentivise users to participate in this process, each successful hash would be rewarded with ‘new coins’. As the confirmation of blocks is the only time a balance can be updated without a transaction between two users, this acts as a minting mechanism. The incentive structure thus acted as the network’s monetary policy:

The first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant amount of new coins is analogous to gold miners expending
resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. (Nakamoto, 2008: 4)

The user is thus rewarded for maintaining the currency network in new units of the currency. This acts as a dual incentive for users to both serve the network and advance its value as currency more broadly. To the key technical innovation of Nakamoto’s paper, the ledger, is added an incentive structure for all users to contribute to its development as a network of value.

In this aspect of design, the technical object becomes distinctly active. The ‘blockchain’ ledger design offers a model for decentralised proof of publication, yet its use retains a significant level of ambivalence. The blockchain allows for digital signatures to timestamp information in such a way that it is both visible and unalterable. The character of this information however, though proposed as recorded transactions, is relatively open. The accumulation of digital signatures allows for all information types to be hashed together and timestamped into blocks. There is no necessity for the information to represent a new form of money (Evans, 2014: 4).

The addition of what Nakamoto terms mining as an incentive structure to encourage maintenance of the network by all nodes is designed to overcome this ambivalence and inscribe into the technology a specific set of practices and definitions. The network calls on users to become miners of bitcoin, committing their computers to an intensive process of hashing. Initially, it does so through an appeal to Cypherpunk values. For the network to achieve the size and functionality required for it to represent monetary value, it relies on the voluntary collaborations of those motivated to decentralise power. The mining structure however appeals beyond this to a further future of wider adoption and use, in which users commit their computational power for the primary purpose of making a profit. Furthermore, the mining incentive structure is designed to increase with difficulty as the number of users in the network increases, while at the same time, the number of bitcoins released as rewards for successful hashing is predetermined to decrease as time goes on, ultimately to a finite supply. This deflationary model promises increasing value for early adopters.

The increasing difficulty for computers to meet the conditions set in the algorithm requires increasing computational power, inducing a competition among ‘miners’ to constantly seek means for faster data processing. The decreasing number of bitcoins released as rewards increases this competition through ensuring a high degree of Bitcoin scarcity, as demand rapidly outpaces supply.
Figure 2.2: Users of the Bitcoin network, ‘miners’, are encouraged to program their computers to generate hashes. The computer that generates a hash matching conditions set in the algorithm receives a reward in Bitcoins.

These design choices thus compel users to accept the interpretation of the network as a system for exchanging the digital equivalent of a precious metal. Indeed, this definition of Bitcoin is made explicit in the design through the analogies to gold. The unit of currency is thus a ‘coin’ to represent the familiar process of moving an object signifying value from one owner to another. While this assists Nakamoto in explaining how a chain of digital signatures can function as money, it also maintains focus on the construction of bitcoin as electronic ‘cash’, as opposed to credit money. Electronic coins are thus referred to as things in the possession of ‘owners’, rather than a balance attributed to a client, and this can be quite misleading.

Coins in the bitcoin network exist only as digital signatures registered on a public ledger. When a transaction occurs, the addresses (personal accounts) of the two users involved are updated on the public ledger through the broadcasting of new digital signatures that represent changes on the ledger. The terminology of coins being transferred from one owner to the next is a convenient metaphor but it is also a misnomer⁴. Its primary purpose is to affirm the interpretation of Bitcoin as a physical currency, and in so doing, imprint the libertarian values of its developers into the technology. These values are centred on the claim that hard currency, such as gold, represents the best form of money.

Precious metals are understood in Mengerian monetary theory to have emerged historically as the most suitable commodities to represent a means of exchange. Due to their physical properties, individuals engaging in trade increasingly valued precious metals and this gave rise to their emergence as money. The process was thus “no accident, nor the consequence of state compulsion... it was the just apprehending of their [actors in the market] individual self-interest which brought it to pass, that all the more economically advanced nations accepted the precious metals as money” (Menger, 2009: 48-9). While the gold standard fell out of favour in mainstream economics, as Nigel Dodd explains in The Social Life of Money (2014), Menger’s theory continued to resonate in circles committed to limiting the capacity of governments:

Menger’s theory is especially popular among libertarians, who believe that money is best organised by markets, not states. The argument that money began as an easily traded commodity offers persuasive support for the view that currencies should be linked to the value of a precious metal such as gold, which is naturally scarce (21)

As the designs for alternative crypto-currencies have come to prove, the design choice to give Bitcoin a predetermined finite supply, released only through ‘mining’, is not an inherent feature of the technical design (Franco, 2014). It follows a libertarian conviction in the superiority of precious metals, valued as currency for their properties, chiefly their scarcity, but also the inability of institutions to create them in response to market conditions. Bitcoin thus constitutes the ‘denationalisation of money’ once envisaged by Friedrich von Hayek as “the one way in which we may still hope to stop the continuous progress of all governments towards totalitarianism” (1976: 134). As a key component of the hashing process that underpins the network however, the mining function condenses this social imperative within the technical logic of design. The libertarian values informing the design are rationalised by the functionality of the technology, triggering a process of mutual justification. In a word, Bitcoin demonstrates to users that Mengerian monetary theory works.

⁴ Vigna and Casey (2015: 44) make this point, suggesting ‘bookkeeping’ as a more accurate term.
The design for Bitcoin affirms the value of Feenberg’s model for understanding the social imperatives underdetermining technology design. The choices made in Bitcoin’s design reflect the particular values and interests of those active in its design process, evidenced in the archives of the Cryptography mailing list. The appropriation of various technical innovations by these actors involved a reimagining of particular technical elements that fit their interests. These values and technical elements are condensed within design, delimiting and reproducing a particular set of meanings and practices for future users. As a creative appropriation, Bitcoin is therefore a successful demonstration of a subgroup introducing new and alternative values into technology design. As an alternative rationalisation of technology however, it does not challenge the capitalist technical code. The imprinting of Mengerian monetary theory into the core algorithm of Bitcoin seeks to circumvent democratic processes to advance libertarian economics. The normative elements of technological rationality: the production of techniques with no obligation to seek ethical justification or regard certain consequences, are left unchallenged. Feenberg’s theory helps to clarify this instance of creative appropriation, but in turn Bitcoin demonstrates that appropriation is not always counter-hegemonic.

**III - Popular Rationalisations**

When I first got into it I thought Bitcoin was the most amazing concept, and then I slowly realised actually it’s just the first - this is just the first thing... Basically it can be whatever you want it to be. It could be an investment, it could be an anarchical statement, it could be a protest, it can be an opt-out. It literally can be what you want it to be. – David Bailey, Bitcoin enthusiast

Democratic rationalisations of technology, Feenberg argues, can lead to a ‘deep democratisation’ of technology through the incorporation of popular agency into the standard procedures of technical design (1999: 147). As the design for Bitcoin demonstrates however, instances of popular agency need not be democratic. There was no necessity for the designers to justify the ethical significance of the technology, or how it impacts on the moral and political position of subordinate social groups. On the contrary, it deliberately evades conventional paths of democratic politics. The social values informing design entrenched Mengerian monetary theory in the core algorithm, ensuring a steadily decreasing and ultimately finite supply of Bitcoins. In this final section, I examine the practices and beliefs of Bitcoin users to suggest that while Bitcoin remains in a stage of interpretive flexibility, its appropriations are often neither democratic nor progressive. I argue that Bitcoin is not a democratic, but a popular rationalisation of technology. Consequently, its incorporation into procedures of technical design is unclear, and may well maximise the operational autonomy of capitalist enterprise.

While Bitcoin users are significantly fragmented (see Gao, Clark and Lindqvist, 2016), many I interviewed in the course of research are committed to developing Bitcoin as a new Mengerian monetary system. The majority of research participants explained the advantages of using Bitcoin with reference to gold, outlining the tenets of an alternative libertarian system impervious to the corruption of financial and political elites. Like gold, it was claimed, Bitcoin cannot be whipped into existence by governments. Also, like gold, Bitcoin cannot be redistributed by a central authority. These features resonated with many disillusioned with banks after a financial crisis that resulted in many Western countries committing to programmes of quantitative easing, effectively expanding the
money supply; and the mass redistribution of public money to rescue failing banks. Bitcoin was understood within this context to be a means of direct action, particularly to those with experience in new digital technologies. If the political establishment were colluding with a corrupt financial system, a new independent system answerable only to mathematical formulae presented an opportunity to redress this injustice from without.

The design of Bitcoin is crucial here. As Bitcoin is designed with a policy of finite supply, this restores the stability of a gold standard in a form fit for the digital age. For many users, Bitcoin thus stands as the next stage in an evolutionary history of money. As one Bitcoin meet-up organiser stated: “we had trust in people, then trust in metals, then trust in banks, which is the one that's clearly proven not to work, but now we’ve got trust in cryptography.” Cryptography has allowed for the creation of a new ‘hard currency’, a ‘digital gold’. The terminology used in design, along with the practices necessary to maintain Bitcoin, affirm this purpose for the users of the technology.

Users with the Mengerian understanding of Bitcoin acknowledge its position as a political project, often encouraging study and debate on Austrian economics and libertarian politics. As Bitcoin is perceived as a form of money, users often transfer their wages into Bitcoin, and use it frequently to purchase goods. Spikes in Bitcoin’s market value are sometimes spoken of excitedly, yet this is due to the interest it may generate in the wider public. These users do not hoard or invest in Bitcoin based on its market value, it is not a speculative pursuit. On the contrary, hoarding and trading induce volatility which is deleterious to the project of Bitcoin as a stable alternative monetary system.

While meet-up groups can often exhibit clashes in perceptions, many concern the degrees of necessary regulation or investment. Users openly speak of internet forums and meet-up groups as ‘echo chambers’, and strategies to counter this often revolve around reaching out to business communities. Introducing business owners to Bitcoin is also a crucial practice in ensuring its success as a form of money. Mengerians readily concede however that the short term benefits of doing so are relatively small. Aside from possible publicity, the uncertainty around Bitcoin, its price volatility, and the necessity to train staff in its usage make it unattractive to most business owners. Presenting the ideological case for Bitcoin thus becomes ever more important, leading some users to describe themselves and others as ‘evangelical’ about Bitcoin. It is this explicit relationship between ideology and technology development that has prompted some scholars, such as David Golumbia (2015), to claim that “Bitcoin is politics masquerading as technology, or technology soliciting and promoting a very specific politics” (119). Golumbia, unambiguously, describes the nature of this politics, a fusion of “right-wing, libertarian anti-government politics” with “conspiratorial anti-Central Bank rhetoric propagated by the extremist right in in the U.S.” (ibid.).

As indicated in the opening of this article, many users committed to developing Bitcoin as a Mengerian monetary system are increasingly encountering difficulties. Mike Hearn (2016) identified these problems as pertaining to a lack of coordination among developers, and a monopolisation of the hardware on which the network runs. Other scholars, such as Papadopoulos (in Cheun, 2015) affirm this, stating that “ironically, the solution to their problems could be regulation and integration into the official monetary system” (171). Drawing on Feenberg’s theory, it is possible to understand this as Bitcoin’s stage of ‘interpretive flexibility’. Various groups are contesting the Mengerian purpose of Bitcoin; their creative practices pushing the limits of its functionality. These adaptations however, present a more complex picture than that of counter-hegemonic appropriations.

After initial usages among developers on Cypherpunk mailing lists, Bitcoin went through a phase of criminal use for the trafficking of illicit goods online. The success of Bitcoin as a medium of exchange for these purposes led to the emergence of crypto-markets such as Silk Road (see Aldridge and Décary-
Hétu, 2014). Bitcoin’s use in this context shaded its emergence into mainstream media as part of the ‘dark net’ yet it also acted as a proof of concept. For the first time, large scale transactions were taking place at a high frequency. The network demonstrated robustness and security and began to attract speculators. Both of these instances presented a double edged sword for those endeavouring to develop Bitcoin as a Mengerian monetary system. While on the one hand, criminal usages were advancing the function of Bitcoin as a viable medium of exchange, it simultaneously led to a proliferation of practices at odds with the image of a superior monetary system. Similarly, the influx of speculators intrigued by the rapid rise in Bitcoin’s market value brought new interest, and new difficulties for those endeavouring to develop Bitcoin as a new monetary system.

As previously discussed, the interests of those seeking to buy low and sell high were at odds with those who understood Bitcoin as a monetary project. While price volatility attracts investment, it weakens the view that Bitcoin can function as a stable store of value or medium of exchange. These groups of speculators also triggered a wave of new technical practices. Various imitations of Bitcoin emerged, the vast majority of which made very slight modifications to its technical design. Nevertheless, they presented alternative crypto-currencies that speculators were keen to trade. Hundreds of ‘altcoins’ have been created over the last five years for this purpose. One particular site that charts their trading volume lists 386 altcoins. Most aim at competing with Bitcoin, receiving similar investment, and allowing users to trade between alternative crypto-currencies in response to the performance of their stock market value. Some are outright ‘pump and dump’ schemes, or ‘scamcoins’, developed solely to make quick money and then collapse. One meet-up organiser described how the volatility this has brought to crypto-currencies has become so prevalent, it is now difficult to imagine them succeeding as anything other than a digital market of commodity trading.

Increasingly, appropriations of Bitcoin are being sponsored by financial firms and institutions, and this is reflected in the changing nature of Bitcoin meet-ups. One Bitcoin entrepreneur and founding member of the UK Digital Currency Association, has run Bitcoin meet-up groups in London from 2014. In this time, he told me, the meet-up had changed considerably, with increasing interest from the City of London signalling a new direction in Bitcoin development:

[The meet-up group] has changed as the type of people that turn up have changed, as those who are interested in Bitcoin have changed. So I have done events, I have been invited to events with some of the main consultancies in London - the big four consultancies. There have been events with the Bank of England, there's one tomorrow, there's events at the core financial firms. And the same thing is reflected in the meet-ups, I've had people who run hedge funds, who are working in the City, they won't necessarily tell me where they are working but they're investigating it either personally or as a company. If it's the company they don't generally tell me where they work. But that whole wave, you've got the whole City, the whole financial sector has been starting to research it. So now, you've still got the early adopters who are still very libertarian. You've got that group, but they're kind of starting to be eclipsed, and I think moving forward, there is going to be a big shift.

The levels of research and investment into blockchain technology currently underway in London and elsewhere, coordinated by major financial firms and institutions, appear to be dominating the future development of the technology first articulated as Bitcoin. Blockchain technology is understood as a means of disintermediating financial services, streamlining the operations of financial organisations, and increasing the efficiency of various networked systems employed by banks.

---

5 http://www.cryptocoinrank.com/ (accessed 13/06/15)
In the initial years of Bitcoin’s development, social groups interpreted the technology as an alternative libertarian monetary system. This purpose was imprinted in its design. Many users have challenged the usages prescribed by this understanding of the technology and redefined it to align with their respective interests. Feenberg’s critical theory clarifies the processes in which the meaning of a technology is contested, and the social forces that determine successful paths of development. Indeed, the success of blockchain technology as a new ‘disruptive technology’ opening new markets and possibilities for the financial firms it was initially designed to circumvent perhaps provides an ironic example for Feenberg’s concept of strategic operational autonomy. Despite considerable investment and research however, this is not yet the case. Blockchain technology is not yet a technique that maximises the operational autonomy of capitalist enterprise. Nor was it ever a counter-hegemonic tactic. Instead, Bitcoin represents a complex case of popular rationalisation.

**Conclusion**

Bitcoin originated as a prefigurative practice of Cypherpunk libertarians. As it diffused through social networks, in some cases these libertarian values were reinforced or reproduced among groups of users that understood Bitcoin as an alternative monetary system. In other cases, the Mengerian definition of Bitcoin met resistance, as groups appropriated the technology to suit their particular interests. In these cases, the achievement of technological agency did not occasion progressive nor democratic technical politics. As argued in section one, Feenberg’s model for demystifying technological development is crucial in understanding the role of social imperatives in contemporary technical practices. Feenberg’s models for democratising technology also provide incisive concepts for understanding technological agency. To advance this understanding however, I propose a change in Feenberg’s theoretical vocabulary to include more focus on the political ambivalence of creative appropriation, which can often be more utopian than resistant in character; and to consider a concept of popular rationalisation, to account for instances of creative appropriation that are not of themselves democratic.

My critique builds on that of Gerald Doppelt (in Veak, 2006) who notes that without ethical standards, it is difficult to distinguish between instances of technological agency that are beneficial for democratising technology more generally, and those that serve only the interests of a particular group. “The fact that one subgroup of users of technology gains some power over it should not count as democratisation,” Doppelt argues, “especially if the changes come at the price of disempowering or excluding other broader groups of users with basic rights, opportunities, or interests at stake” (2006: 94) What is necessary, Doppelt argues, is for the subgroup to justify the ethical significance of the technical change they desire, how it impacts on the moral and political position of other social groups.

Feenberg responds to this criticism by reemphasising the importance of technocracy in reproducing social inequalities. Doppelt’s argument, Feenberg claims, remains representative of a tradition in political philosophy more broadly which, while bringing to light issues of material inequalities, has failed to account for the impact of technical arrangements on democratic rights in the same way. “It is in the context of technocracy” Feenberg states, “that agency appears as a central democratic value not just for excluded minorities, as Doppelt claims, but for everyone” (Veak, 2006: 182). It is technocracy, therefore, that underpins the necessity for agency. As discussed above, Feenberg asserts that any society governed by the capitalist technical code will continue to reproduce social inequalities via the operational autonomy retained by elites. In examining Feenberg’s identified models for democratising technology, this reply feels somewhat incomplete.
Controversies that generate public debate, or dialogue that fosters public participation in design, may be instances in which technology is brought into the public sphere. Design is opened to social criticism in ways that challenge the assumptions of technological rationality. Creative appropriations however, do not initiate the same processes of justification. Such instances demonstrate the capacity for subgroups to imprint new meanings and purposes into technologies without recourse to democratic discourse. While such groups may momentarily achieve technological agency, and their devices may be imprinted with new alternative values, it does not necessarily follow that the agency achieved will diffuse to other groups, nor that their values are democratic.

While I am in agreement with Feenberg that politics on the internet is “arising in the midst of a broader revival of agency in many different types of online communities” (2012: 9), Bitcoin raises questions over which types of agency will result in a democratic rationalisation of the internet. The second section of this paper was an attempt to show how values that are neither democratic nor progressive can gain considerable momentum when condensed with technical logic in design. This point was continued in the third section, in which I emphasised that Bitcoin represents a flourishing of libertarian values as much as it does that of technological agency. The questions raised by these findings are primarily the questions originally posed by Doppelt: “how do we determine which trade-offs, whose interests, what challenges contribute to a more, or less, democratic rationalization of technology?” (2006: 89). My argument that Bitcoin represents a ‘popular’ rationalisation of technology seeks to problematize Feenberg’s theoretical vocabulary for the purposes of addressing these questions.

Creative appropriations are a site of complex interactions with technology that have unclear ramifications for technological rationality. The internet has given rise to new forms of agency, allowing for popular rationalisations of various new technical arrangements. These rationalisations however require ethical justification. Popular rationalisations such as Bitcoin must be opened to social critique to determine how they impact on the moral and political position of other social groups before they can be considered democratic rationalisations. Technological rationality is an effective hegemony as it reproduces social imperatives with no recourse to democratic processes. In the efforts of libertarians engaging with Bitcoin however, we also see the active reproduction of social values in design with no recourse to democratic processes. Bitcoin thus illustrates an instance of technological agency that is neither progressive nor democratic; a creative appropriation and a popular rationalisation.

References


Available at: [http://www.weidai.com/bmoney.txt](http://www.weidai.com/bmoney.txt) (accessed 13/06/15)

Berkeley: University of California Press

Dodd, N. (2014) *The Social Life of Money*


Feenberg, A. (1991) *Critical Theory of Technology*
Oxford: University Press

Feenberg, A. (1992) *Subversive rationalization: Technology, power, and democracy*
Inquiry, 35:3-4, 301-322

London: University of California Press

Feenberg, A. (1999) *Questioning Technology*
London: Routledge

Feenberg, A. (2002) *Transforming Technology*
Oxford: University Press

Feenberg, A. (2010) *Between Reason and Experience*
London: MIT Press

Feenberg, A. (2012) *(Re)Inventing the Internet*
Rotterdam: Sense


Golumbia, D. (2015) *Bitcoin as Politics: Distributed Right-Wing Extremism*
Geert Lovink, Nathaniel Tkacz, and Patricia de Vries (eds), MoneyLab Reader: An Intervention in Digital Economy, Amsterdam: Institute of Network Cultures

Available at: [https://www.anf.es/pdf/Haber_Stornetta.pdf](https://www.anf.es/pdf/Haber_Stornetta.pdf) (accessed 10/06/15)

Hayek, F. (1976) *The Denationalisation of Money*
London: Goron

Hearn, M. (2016) *The Resolution of the Bitcoin Experiment*
Available at [https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.gg0agvo2q](https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.gg0agvo2q) (accessed 29/03/2016)

Hughes (1993) *A Cypherpunk’s Manifesto*
Available at: http://www.activism.net/cypherpunk/manifesto.html (accessed 29/03/16)

Available at: https://mises.org/library/origins-money-0 (accessed 29/03/16)

Available at: https://bitcoin.org/bitcoin.pdf (accessed 10/03/2016)


---

1 Full archive of the Cryptography mailing list is available at http://www.metzdowd.com/pipermail/cryptography/ (accessed 19/05/2016)
2 Quoted from the Cryptography mailing list http://www.metzdowd.com/mailman/listinfo/cryptography (accessed 19/05/2016)