future internet

MDPI

Article

Socialism and the Blockchain

Steve Huckle * and Martin White

Creative Technology Group, Department of Informatics, University of Sussex, Chichester 1, 128, Falmer, Brighton BN1 9QT, UK; m.white@sussex.ac.uk

* Correspondence: s.huckle@sussex.ac.uk; Tel.: +44-0-1273-606755

Academic Editor: Carmen de Pablos Heredero

Received: 5 August 2016; Accepted: 10 October 2016; Published: 18 October 2016

Abstract: Bitcoin (BTC) is often cited as Libertarian. However, the technology underpinning Bitcoin, blockchain, has properties that make it ideally suited to Socialist paradigms. Current literature supports the Libertarian viewpoint by focusing on the ability of Bitcoin to bypass central authority and provide anonymity; rarely is there an examination of blockchain technology's capacity for decentralised transparency and auditability in support of a Socialist model. This paper conducts a review of the blockchain, Libertarianism, and Socialist philosophies. It then explores Socialist models of public ownership and looks at the unique cooperative properties of blockchain that make the technology ideal for supporting Socialist societies. In summary, this paper argues that blockchain technologies are not just a Libertarian tool, they also enhance Socialist forms of governance.

Keywords: Bitcoin; blockchain; cryptocurrency; fiat money; libertarianism; socialism; Marxism; anarchism

1. Introduction

Bitcoin (BTC) is referred to as cryptocurrency because it is a form of electronic cash that relies on cryptography. Since its inception in early 2009 [1], it has achieved a degree of prominence, not least in terms of market value; at the time of writing, its total market capitalisation was over US $6 billion [2]. Furthermore, governmental institutions are beginning to examine the blockchain technology underpinning BTC [3] because some of its properties, which we discuss below, may have implications that extend beyond economics and into social, political and humanitarian domains [4]. This paper investigates that potential and examines whether blockchain has ideological tendencies beyond the usual Libertarian narrative [5–8], an ideology that advocates individual freedom and minimal state intervention in people's lives [9]. In particular, the paper asks whether, in fact, the technology is directly applicable to Socialism, an economic theory and form of governance that advocates community ownership [10].

First of all, this paper gives an overview of BTC and blockchain technology. It then introduces Libertarian ideology before investigating how that applies to the blockchain. We then discuss Socialist philosophy, and similarly apply its ideas to blockchain technology. This allows us to examine whether the core concepts behind BTC and blockchain are ideally suited to support the social and political philosophies discussed.

This article uses the term *State* to refer to an organised political entity that forms a single system of government. Furthermore, in the UK, parliament is the legislative, elected body of Government, and: "Parliamentary sovereignty is a principle of the UK constitution. It makes Parliament the supreme legal authority in the UK, which can create or end any law" [11]. Therefore, in this paper, the terms *Sovereign*, *State* and *Government* are synonyms that we use interchangeably.

2. Bitcoin

Satoshi Nakamoto first proposed BTC, an implementation of electronic cash that did not need authorising by banks, in a 2008 whitepaper [12]. The system Nakamoto described was a peer-to-peer

(P2P) network whose overriding purpose was to propagate transactions requiring validation to all of the participants in the ecosystem [13]. Thus, a fundamental component of BTC is a transaction, which contains some inputs that map to one or more outputs and behaves similarly to individual lines in a double-entry bookkeeping ledger [13]. Essentially, transactions are BTC owners informing the network that they have transferred ownership of some of their coins to other users [13]. Those new owners can, in turn, create another transaction that authorises ongoing transfer. Thus, a chain of ownership, known as a blockchain, is formed [13].

Antonopoulos explains BTC transactions by using the example of Alice buying a cup of coffee from Bob's coffee shop [13]. Alice spends BTC with Bob by using a BTC wallet on her smartphone (there are a number of wallets to choose from [14]). She does so by scanning a two-dimensional barcode, known as a QR code, of the payment request generated from Bob's BTC enabled point-of-sale (POS) system (again, many POS solutions exist [15]). This contains Bob's destination address, how much Alice should pay and the written description of the trade. Figure 1, below, shows the transactions involved.

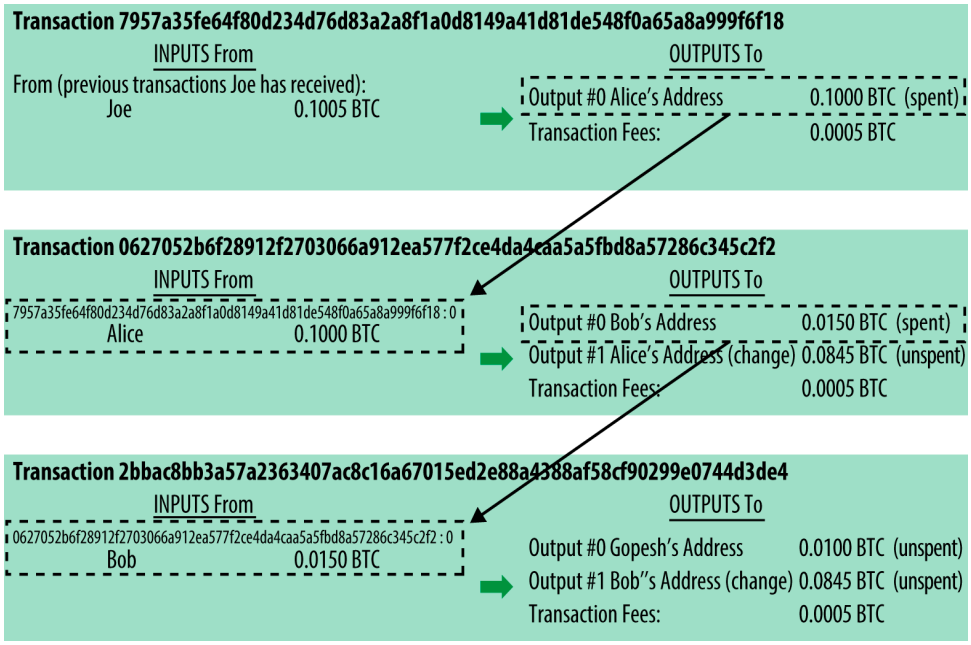

Figure 1. Bitcoin (BTC) transaction [13].

BTC transactions are authorised using public key cryptography [16], whereby *user x* is granted a public and private key. This ensures that only *user x* can perform transactions belonging to *user x*; the public key establishes *user x's* identity and *user x* uses their private key to prove that particular transactions belong to them. In Figure 1, Alice pays Bob for his cup of coffee by creating new outputs from the inputs of a previous transaction with Joe, who used Alice's public key as the destination address for the BTC involved. When Alice uses some of those funds to pay Bob for his coffee, she supplies her private key to unlock them. This ensures that those transactions are read-only to every other user on the BTC network because it is practically impossible for anyone to modify them without knowing Alice's private key. Once the network is satisfied Alice has a sufficient number of BTC to cover the necessary outputs for the transaction with Bob, the required BTC are transferred using Bob's public key. This encumbers this output with the requirement that, to spend the amount transferred, Bob must produce his private key. In other words, it represents a secure transfer of value between Alice and Bob [13]. Security of this transfer is enforced by the timestamping and hashing functions of the validators on the BTC network (which we will discuss later), who form a chain of final transactions [16]. This ensures that even Alice, with her private key, can not modify confirmed transactions, since it is technically infeasible; she would have to change all the blocks in the chain to change a single

block. As Harvey points out, in 2014, a computing array with the power of 1,753,694 Peta floating point operations per second (FLOPS) would have been needed to make a fake block on the BTC blockchain [17]. At the time, the world's fastest supercomputer, the Chinese Tianhe-2, could manage 33.9 PetaFLOPS. This means over 50,000 Tianhe-2 supercomputers would be required to attempt to create the fake block.

The first reference implementation of BTC was published online in early 2009 [18] and the first transaction of BTC, in block 170, took place on 12 January 2009. This first transaction was between Nakamoto and a developer specialising in cryptography, called Hal Finney, who lauded BTC and remarked that the underlying technology, the blockchain, included "some interesting features" [19]. Blockchain technology is described in more detail next.

2.1. Blockchain Technology

The blockchain is an essential component of Bitcoin (BTC) because it is an immutable ledger of every BTC transaction that has ever taken place. As BTC is an open source GitHub project [20], any developer can fork the code and create their implementation of a cryptocurrency. Indeed, since its launch, BTC has spawned a group of alternative blockchain technologies, known as *altcoins* [21], examples of which are Ethereum [22], Ripple [23], Litecoin [24] and Stellar [25]. Although such altcoins may use different means of consensus or different optimisations, they all use the same general approach based on a decentralised P2P network, which, assuming there's a functioning Internet, means they have no single point of failure. The authors of a report for the UK Government describe the technology as: "essentially an asset database that can be shared across a network of multiple sites, geographies or institutions" [3]. However, the blockchain has capabilities far beyond any ordinary asset database because it also includes algorithms that provide a secure mechanism for electronic collaboration that does not rely upon a central authority for the assets to be trusted. This includes the concept of smart contracts, which is the ability of blockchains to execute autonomous scripts that can represent verifiable application logic and help automate a system's rule set [26]. Furthermore, blockchain technology is a distributed network of transactions including tracked changes and where the control of write permissions is via public-private key cryptography. Thus, the blockchain is a trusted, shared public ledger that is open to inspection by everyone, but which cannot be controlled by any single entity [27]. As we show below, because no central control implies individual freedom, those are the aspects of blockchain that are commonly held as Libertarian. However, we will also argue that blockchain technology has mechanisms ideally suited to Socialist philosophy.

2.2. Bitcoin Mining

Fundamental to BTC validation is the idea that network validators must exhibit proof, known as a proof of work (PoW) that they have solved a difficult cryptographic problem [28]. Nakamoto, in his original paper on BTC, defines the steps necessary to creating a BTC based blockchain network:

1 New transactions are broadcast to all nodes.
2 Each node collects new transactions into a block.
3 Each node works on finding a difficult proof-of-work for its block.
4 When a node finds a proof-of-work, it broadcasts the block to all nodes.
5 Nodes accept the block only if all transactions in it are valid and not already spent.
6 Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash [12].

Figure 2 below shows the BTC validation process, which is known as mining because a reward of "mined" BTC is given to the validator that created the accepted block. Miners that worked on the establishment of the block, but failed because other nodes solved the cryptographic puzzle faster than them, lose. As a result, bitcoin mining has been called "competitive bookkeeping" [29]. Figure 2

shows the validation process running on application-specific integrated circuits (ASICs). ASIC-based computers dominate BTC mining because they are much faster and more energy efficient than machines that mine using field-programmable gate arrays (FPGAs), graphics processing units (GPUs) or central processing units (CPUs) [30].

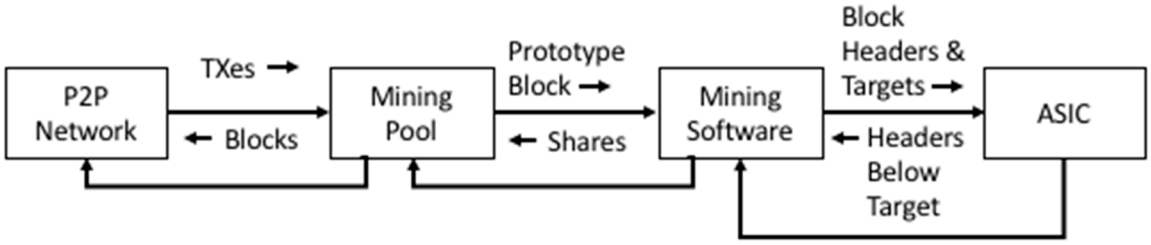

Figure 2. BTC validation process [31].

2.3. Bitcoin's Energy Use

PoW is a scheme based on a SHA-256 hashing algorithm, which produces a cryptographic hash with a value less than a target nonce. The average CPU effort needed to compute the PoW for a mined block is exponential to the number of zeroes required. The BTC network examines timestamps and calculates the time that has elapsed creating 2106 blocks; ideally, 1,209,600 s will have passed, which equates to the creation of a single block every ten minutes [13]. However, the production of blocks is via a random Poisson process whereby it might be that many blocks, or very few blocks, are found in a given hour [32]. BTC raises the hashing difficulty if it discovers that the creation of 2016 blocks took less time than 1,209,600 s. Conversely, the difficulty is dropped if creation took longer [33]. Invariably, as more processing power comes online to the BTC network, the difficulty goes upwards. For example, at the time of writing, the BTC difficulty is 163,491,654,909. The very first BTC had a difficulty of 1. This means that it is nearly 164 billion times harder to mine a BTC now than it was to mine the very first.

All of that computing power comes at an enormous energy cost. The authors of a BTC mining guide state that, based on price per hash and electrical efficiency, the ASIC miner *AntMiner S7* is the best BTC mining hardware available [30]. This mines at 4.73 Terra hashes per second (Th/s) and consumes 1293 Watts [34]. At the time of writing, the network hash rate of BTC was 1,411,498 Th/s [35]. Assuming that the *AntMiner S7* does indeed represent the best in class, we can use those figures to calculate the best case scenario for the total energy consumption of mining on the BTC network:

$$(1{,}411{,}498/4.73) \times 1293 \approx 385.84 \text{ MegaWatt hours (MWh).}$$

Therefore, at that rate of consumption, the daily energy use of BTC mining is given by:

$$385.84 \text{ MWh} \times 24 \approx 9.26 \text{ GWh.}$$

Hence, BTC mining's approximate annual electricity consumption is given by:

$$9.26 \times 365 \approx 3.38 \text{ TWh.}$$

To put that 3.38 TWh in context, according to the International Energy Agency, in 2014, the 2.72 million people of Jamaica consumed 3.03 TWh of electricity, or slightly less than the annual consumption of mining on the BTC network [36].

2.4. The Problems Addressed by Bitcoin and Blockchain Technology

In BTC's 2008 whitepaper, Nakamoto describes the issue of third-party financial institutions processing electronic cash; namely, that supposedly irreversible payments become reversible [12]. This leads to expensive dispute mediation, which makes small Internet-based payments for goods or services, known as micropayments [37], impractical because their cost outweighs any possible profit from such transactions. Moreover, fraud becomes endemic, which necessitates the need for trust between merchants and their customers; without it, the system fails. BTC overcomes that through the use of cryptographic proof, which allows parties to transact directly, thus removing the need for third parties to verify payments. Hence, the design of BTC obfuscates much of the necessity of trust inherent in *fiat money*, which is money established as legal tender through government regulation. This is another property of the technology that appeals to Libertarians, as we shall show.

Another problem is that physical banknotes are often forged, despite their including various unique characteristics supposed to authenticate their validity. BTC overcomes such issues because, as we have shown, it ensures authenticity through cryptography and blockchain validation [3].

Unlike physical cash, it is theoretically possible for digital financial transactions to be copied and spent in two different places almost simultaneously. This is known as the problem of *double spending* [38]; how can a recipient trust that someone else hasn't already spent the money intended for them? BTC solves that through its PoW based mining process, which combines cryptographic hashing and economic incentives [39].

BTC's distributed PoW also solves a conundrum in distributed computing, known as the Byzantine Generals Problem (BGP). How can Generals of the Byzantine army, camped with their troops around an enemy city, reach agreement on a common battle strategy [40]? While some of the Generals will be loyal to the Byzantine cause, unfortunately, others may be traitors who will try to undermine any plan. The problem is how to circumvent those malicious actors and ensure the army's success? A Byzantine-fault-tolerant (BFT) system must guarantee its validity even when it could include various malignant entities. Although there were theoretical solutions given in a 1982 paper by Leslie Lamport [40], Nakamoto's implementation of BTC was the first to provide de facto BFT consensus [18].

Finally, PoW gives BTC a natural way of overcoming 'Sybil Attacks', which is where an imposter creates multiple identities that they use to take control of a system [41]. This is because BTC establishes trusted identity through its requirement to perform some form of computational work [42].

All of these mechanisms ensure that BTC is 'trustless' because it entirely dispenses with many of the necessities for trust, which, again, are features that lend BTC to Libertarian ideology, which we will show next.

3. Libertarianism and Money

A Libertarian's primary political values are: the right to private property, freedom of speech, freedom of worship, legal equality and moral autonomy [43]. Indeed, the classical view of Libertarianism is one that advocates individual liberty in preference to collective judgement [44]. The result is a deep scepticism of the state and government power [43], and the belief that society should be freed from government backed banking systems. In particular, Libertarians would argue that banks should not have their risks underwritten by the State [45]. Indeed, a Libertarian believes that governments should not do anything beyond enacting legislation that protects individual rights.

Martin writes that because money relies upon a government promise that its value will be repaid with equivalent new notes [46], the relationship money creates between trust and its issuing authority is important. He believes that the Sovereign has distinct advantages as an issuer of money; namely, that (1) it conducts by far the biggest volume of economic transactions; (2) it has political authority; (3) it has legitimacy. In democratic nations, this authority has been conveyed upon the Sovereign by the very people who use the money issued. Hence, Martin describes the level of trust of the Sovereign's legitimacy as: "ideological and even spiritual" [46]. In modern economies, the Sovereign has deferred

the right to issue money to their central banks [47]; the Bank of England in the UK, the Federal Reserve in the U.S. and the European Central Bank (ECB) for the Eurozone. However, the U.S. Libertarian Party wants the government to halt the inflationary monetary policy. They also believe that fiat money should be scrapped [45]. Instead, they believe money should have a subjective value assigned to it by individuals, not governments, and that people should be free to use anything they like as a means of exchange. It appears that it is the U.S. form of Libertarianism that the Oxford English Dictionary refers to when defining it as: "an extreme laissez-faire political philosophy advocating only minimal state intervention in the lives of citizens" [9].

Libertarian views on individual freedom are deeply entrenched in U.S. society. Indeed, their national anthem proclaims the U.S. to be: "the land of the free" [48]. However, although hard-line Libertarian's believe that governmental control of money is incompatible with personal liberty: "politicians have often laboured under the delusion that money is something created and manipulable by themselves, when, in fact, it is the spontaneous institution of a free society and will continue to evolve in ways outside their grasp" [49], U.S. Libertarians, who tend to take a liberal view on personal freedom, have a more a conservative view on economic matters. This favours government led free-market Capitalism [50]. Indeed, Adam Smith, an 18th century Economist who maintains a considerable influence on Capitalist thinking, tended towards the Libertarian belief that social good is the result of the free reign of private self-interest: "it is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest" [51]. Boaz et al. summarise the U.S. Libertarian's political choices [50]:

> "Candidates who offer a program of big-government spending and aggressive social conservatism will tend to drive away libertarians. More specifically, candidates who favor lower taxes, spending restraint, free trade, Social Security private accounts, reproductive choice, and a welcoming attitude toward working women, immigrants, and gays are going to find favor with libertarian voters. Candidates who support protectionism, tax increases, ever-expanding entitlement programs, and intrusions into personal freedoms will lose the libertarian vote."

Hence, a U.S. Libertarian's political views may be tempered by a conservative-liberal divide, as shown in Figure 3.

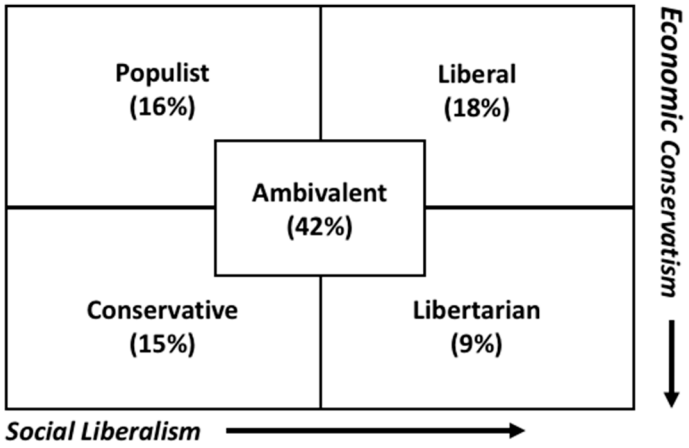

Figure 3. The conservative-liberal divide of U.S. Libertarianism [50].

Libertarianism, Bitcoin and Blockchain Technology

BTC has a great political potential for U.S. Libertarians, and BTC is considered a Libertarian ideological vehicle [6]. Indeed, Scott remarks that: "in particular, they (cryptocurrencies) have become associated with the hyper-individualism of conservative libertarianism" [8]. This is due to a number of

factors, namely: (1) cryptocurrencies reduce the monetary policy capabilities of the State because BTC's money supply is managed algorithmically by computer software [52], not by government-controlled central banks; (2) transactions are verified across a distributed P2P network, so there is no single authority in control; (3) it is the BTC miners, not Governments, who receive *seigniorage* [53], a term derived from Old French that literally means: "the right of the lord to mint money". It refers to the revenue earned by issuing the currency, which can occur in many ways, but, at its most basic, it's the profit earned because there's a difference between the value of money and what it costs to have it produced and distributed [54]; and (4) the cryptographic nature of BTC means that their ownership is difficult, if not impossible, to match to real people [6].

There is another important factor that attracts Libertarians to BTC; it can be traded or exchanged without requiring the trust of any financial institution [55]. As Gehring points out, in that regard, BTC differs significantly from fiat money, which carries a considerable counterparty risk because when someone deposits it into a bank, he or she are, effectively, trading fiat cash for a digital IOU which the bank promises to redeem on demand [56]. Martin describes such money is an "ephemeral and cosmetic" *unit of trust* that forms a particular type of transferable credit, whereby monetary exchange is the clearing of credit accounts, and notes and coins are tokens of an underlying credit relationship [46]. This is fine until the public's trust in those IOU's is undermined, such as it was in 2008, at the very bottom of a profound economic crisis, when, as Rifkin writes: "we began to realise that behind all the rules, regulations, and firewalls lay an empty chasm" [57]. This crisis was caused by, what Poszar et al. have deemed as the *Shadow Banking Sector* [58]. This was built on elaborate systems of financial supply chains that were worth, by the end of 2007, around US$25 trillion [46]. When the sector began to show signs of distress, it caused a contagion that, according to Laeven et al. [59], resulted in many countries experiencing a significant crisis in their traditional banking sectors that eventually required the governmental provision of direct credit support. In a paper titled *Banking on the State*, Allessandri et al. quantified the extent of the State's support: over US$14 trillion, or almost a quarter of the global economy [60]. As Martin writes: "this was the scale of the downside risks, taxpayers realised, that they had been bearing all along" [46]. Some, such as those in the Libertarian movement, find that risk unacceptable. Hence, their ideological support of BTC, which carries no such risk. Indeed, Yermack notes the interesting timing of BTC's release, coming as it did in the depths of that 2008 financial crisis [7].

4. Socialism and Money

Socialism is a term that encompasses many different political philosophies. Major branches are Marxism, Utopian Socialism and Anarchism. Although they differ in important regards, they all share egalitarian values, non-hierarchical societal structures [61] and various forms of social ownership whereby the means of production and distribution are owned by a community [10].

Marx thought that Socialism would be a natural outgrowth of the existing Capitalist system [62], which he considered to be based on conflict because there is an opposition between those who labour, who own nothing, and the class of Capitalists, who own the means of production [63]. Eventually, Marx believed the workers of the world would instigate revolution and free themselves [64]. Afterwards, a Socialist society would emerge, where the producers would control production, and goods and services would be created for their usefulness to society, not for their profit margin [65]. In Tressell's *The Ragged Trousered Philanthropists*, the character Barrington describes a Socialist State, where workers: "devote themselves to art or science, and some others will offer their services to the community as managers and superintendents, and the State will always be glad to employ all those who are willing to help in the Great Work of production and distribution" [66]. Marx described it as: "From each according to his ability, to each according to his needs" [67]. Key to Marxism is the co-ordination of the whole economy through central State planning [68]: "The national centralization of the means of production will become the natural base for a society which will consist of an association of free and equal producers acting consciously according to a general and rational plan" [62].

In works such as Capital [69], Marx wrote extensively on the complexities of value in monetary society. The basis of his theories centred on his labour theory of value [70] whereby value was closely related to the labour necessary to produce goods [69]. Marx held that Capitalists make a profit by extracting surplus value from their workforce because productive workers create more than they cost [71]. Marx felt that 'freedom' under Capitalism only meant: "free trade, free selling and buying" [72], which trap the working class because maximising profit means forcing them to work for subsistence wages [72]. Thus, he wanted to "deprive him of the power to subjugate the labour of others" [72] through the abolition of buying and selling, removing the need for money. Under a Marxist society, goods would not be produced for profit, but rather, for their use value and their propensity for satisfying human needs [73]. Marx believed that people would then learn to recognise the practical nature of their needs [74], and, as a result, real individuality would surface: "Then you can exchange love only for love, trust for trust, etc." [75].

Instead of money, Marx envisaged a system of labour certificates, whereby people get rewarded according to the number of hours they spend in production. Those certificates could then be used to buy all merchandise at cost price; goods whose value is determined in hours of labour [61]. Crucially, they could not be converted into capital and thus, they would not circulate. This was key to such certificates not being regarded as money since Marx believed that the *money–commodity–money* credit cycle was core to Capitalist society [69] because it provided liquidity [62]. Indeed, Chang writes that one of the foremost Economists of the 20th Century, John Maynard Keynes, thought liquidity as paramount to Capitalist economies because it made it possible, in an uncertain world, to increase capital very quickly [68]. Consider a business's position at the start of production. No goods exist, but there has to be an exchange of wages for labour. Since the company has not yet created any commodities, commodified money cannot exist. Hence, at the beginning of the production cycle, money takes the form of an "accepted promise of payment—in other words, credit" [74], which the business most likely received from a bank. The cycle of transfer is complete when the goods produced are exchanged for money, and the company reimburses the lenders for the loan they gave to pay those initial wages [63].

The Oxford English Dictionary describes Utopian Socialism as: "Socialism achieved by the moral persuasion of capitalists to surrender the means of production peacefully to the people" [76]. Utopian Socialism creates a form of Collectivism through the collective ownership of the means of production and distribution, where goods are distributed based on Marx's system of labour certificates. However, it is unlike Marxism because it believes in peaceful means of establishing ethically just cooperative communities which demonstrate the feasibility of such a society [77]: "Socialism is the expression of absolute truth, reason and justice, and has only to be discovered to conquer all the world by virtue of its own power" [78]. Although Utopian Socialism dispenses with the Marxist idea of a centrally planned state, Marx's idea that nobody should: "deprive no man of the power to appropriate the products of society" [72] is a core concept.

At its simplest, Anarchism's core belief is that human beings are reasonable and decent and, therefore, neither the individual or their communities need organising via hierarchical structures [79]. Like Utopian Socialists, Anarchists would reject any form of unjustified central planning. Moreover, it rejects the State and the State apparatus [61], viewing them as the means by which the non-egalitarian owning classes control society [80]. However, while an Anarchist rejects the mechanisms of the State, it is a mistake to think that Anarchists reject government and the rule of law entirely [61]. As Ludlow explains: "it is not the blanket rejection of authority or morality (to the contrary, autonomy places a great moral burden on each of us)" [81]. Rather, Anarchists redefine government as an institution of governance that makes rules and settles disputes [61]. Anarchism also believes in the outright abolition of money or anything that might be regarded as money, including Marx's system of labour certificates: "if we preserve the individual appropriation of the products of labour, we would be forced to preserve money, leaving more or less accumulation of wealth according to more or less merit rather than need of individuals" [82]. Instead, Anarchism believes in people performing the work for which they are

ideally suited, and that the surplus goods they create are not exchanged but consumed freely by those who need them [44].

Socialism, Bitcoin and Blockchain Technology

Scott describes blockchain as: "interesting because it has features that potentially allow for non-hierarchal self-organization and peer-to-peer collaboration within a communitarian network structure" [8]. The suggestion is that Nakamoto's design of BTC, which is based on a community of validators providing co-operative consensus [12], has qualities suited to Socialist ideology. Specifically, Scott asks whether blockchain systems can be used to provide governance for large-scale collaboration under Anarchist traditions, who rely on social and interdependent natures of the individual to create smaller-scale, egalitarian structures [8]. Indeed, some authors are exploring the Socialist ideology behind the technology and the idea of blockchains which enable collaboration through distributed autonomy. For example, Swan writes that blockchain has democratisation capabilities that include the concept of decentralised organisations [4]. Wright et al. write that the blockchain: "enables collective organisations and social institutions to become more fluid and promote greater participation, potentially transforming how corporate governance and democratic institutions operate" [83]. Valkenburgh et al. describe blockchain based smart contract-enabled distributed autonomous organisations that: "represent some sort of collective or non-profit interest" [84]. Indeed, Valkenburgh et al. share the Anarchist mistrust of large-scale hierarchical organisations, believing them to be imperfect and inefficient. Indeed, they write that, instead, blockchain's combination of digital currencies, smart contracts, and distributed data storage will usher in entirely new decentralised organisations that use source code to define secure, auditable governance [84]. Moreover, digital assets that are native to blockchain could be deployed for use within a Socialist society; however, it is deemed appropriate; they needn't be used for money. For instance, they might be employed as Marxist labour certificates. Fairfield writes that blockchain technology comes with tamper resistant algorithms for creating public, cryptographically secure ledgers of property interests [85], but the immutable audibility mechanisms of blockchain technology could extend beyond property ledgers and into auditing the production of goods. This would allow Anarchist societies to organise because the blockchain could be used as a means whereby Anarchists could audit the distribution of products or services to those who need them. For example, In the UK, the present government are charging people living in social housing for what they deem to be spare bedrooms [86]. The policy has proved controversial and has led to many claims that the tax is unfair; for example, one family successfully appealed against the tax because carers used their spare bedroom to help the family look after their son [87]. Now imagine an Anarchist community supported by blockchain smart contracts that encode what society deem fair and where that family above were allowed their spare room without needing recourse to the courts, on the basis that they required their extra room due their son's severe disability.

Buterin writes that blockchain technology can follow either public, consortium or private models [39]. BTC is a public blockchain, which the Bitfury Group and Garzik define as 'permissionless' because they have no read restrictions and since transaction processors, the miners in BTC, have an unknown identity and unrestricted write access [16]. Moreover, Buterin points out that anyone can have his or her valid transactions recorded on the public blockchain ledger, and anyone can take part in the consensus process for verifying transactions [39]. It is those qualities of good governance; transparency and auditability [88], which are inherent in public blockchain technology that make it an ideal tool for Anarchism or Utopian Socialism, because it enables: "a universal, permanent, continuous, consensus-driven, publicly auditable, redundant, record-keeping repository" [4]. By contrast, a private blockchain is 'permissioned' because it has a predefined list of entities, with known identities, which can process transactions [16]. However, a permissioned blockchain is not necessarily private; Buterin describes a wholly private blockchain as one where read permissions may be public, or partially restricted, but write permissions are centralised. Thus, a privatised blockchain resembles a centralised system with an infusion of cryptographic audit-ability [39]. It is important to note that a private

blockchain does not necessarily imply secrecy; it can still be publically accountable. To Buterin, a consortium blockchain is "partially decentralised", whereby a limited set of nodes participate in that consensus process [39]. The ledger may be readable to either all nodes, a specified list of participants or only partially readable to some. The model has the low-trust apparent with public blockchains and the highly-trusted characteristics of private blockchains [39]. Figure 4 below shows the degrees of centralisation between public, private and consortium blockchains. Both private and consortium models suggest the central planning ideology of Marxism.

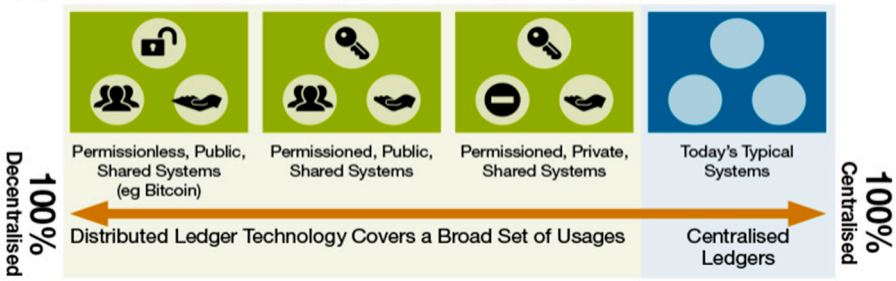

Figure 4. Degrees of centralisation [3].

5. Applications of Blockchain Technology to the Socialist Paradigm

Below, we give two applications of BTC to Socialism. The first relates to how BTC itself may be used in a Socialist society and the second refers to BTC development.

5.1. Bitcoin and Marx's Labour Theory of Value

The financial markets have deemed that, at the time of writing, 1 BTC is worth $661.73 [89]. However, because BTC is a native digital asset on the blockchain, we could choose to link it to any social construct of value. Here, we shall derive an interpretation of Marx's labour theory of value by using energy to quantify the amount of work, or labour, done [90]. We contend that is valid in industrial economies that are increasingly mechanised and therefore rely on energy for productivity and growth [57]. Furthermore, using energy as a measure of labour works well because, as we have shown, we can quantify the amount of energy required to create BTC as well as the amount of energy used by products over their lifetime, as we shall see below. Therefore, BTC is directly interchangeable for those same goods.

Assuming the total energy consumption of 385.84 MWh, which we derived earlier, and that a block is generated every 10 min, a single block uses the following amount of energy:

$$385.84 \text{ MWh}/(1 \text{ h}/10 \text{ min}) \approx 64.31 \text{ MWh}.$$

BTC miners currently receive a reward of 12.5 BTC for generating a block [91]. Therefore, the energy required to create a single BTC is as follows:

$$64.31 \text{ MWh}/12.5 \approx 5.14 \text{ MWh per BTC}.$$

We can use that value to calculate the value of a good. Imagine that the people of a Socialist society have deemed that, to mitigate the dramatic effects of climate change, they should disallow fossil-fuelled transportation. Electric vehicles have become standard, as has electricity generation using renewable energy. According to life-cycle analysis conducted by Aguirre et al. [92], an electric vehicle (EV) uses, over its lifetime (manufacturing, transportation, use, and disposal), 506,988 MJ, or 140.83 MWh [92]. Given that it requires 5.14 MWh to create a single BTC, the price of the *Nissan Leaf* EV is given by:

$$140.83 \text{ MWh}/5.14 \text{ MWh per BTC} \approx 27.4 \text{ BTC}.$$

Hence, by calculating the energy used in forging BTC and that used during a product's lifecycle, we can create a Marxist labour theory of value for the Nissan Leaf of 27.4 BTC.

5.2. Bitcoin Community Development

Nakamoto's community-driven consensus model also applies to BTC's development. BTC Core is the open source GitHub project [20] from where the BTC code is released for the day-to-day operation of the system. Developers contribute documentation, test code, improve the user interfaces, or bug fix. Although BTC has no formal structure, the community has instigated a standard system for submitting ideas, called a BTC improvement proposal (BIP). This constitutes a design document used for introducing features or information to BTC. Figure 5 below shows the BIP workflow.

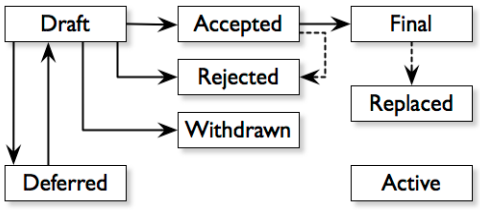

Figure 5. BTC improvement proposal workflow (bip-0001) [93].

Furthermore, the codebase is maintained using peer reviewed GitHub "pull requests" of patch proposals. Contributions use the Open Source meritocratic model, where code from longer term contributors is trusted more by the community. The development cycle is thus:

1 Fork the GitHub repository and clone it locally.
2 Check out the master branch.
3 Create a topic branch.
4 Write patches.
5 Stage and commit patches.
6 Push the new branch back up to the GitHub fork.
7 Send a Pull Request.

BTC development, using GitHub's meritocracy model, has many similarities to Kropotkin's description of Anarchism, where order emerges through: "an infinite variety of capacities, temperaments and individual energies" [61]. Furthermore, BTC's BIP Workflow might also be construed as the rules and mechanisms needed for settling disputes under an Anarchist's requirement for governance.

6. Conclusions

The intention of this paper is not to promote one form of political philosophy over another. Rather, it has been to discuss the deployment of blockchain in support of different social theories. However, Blockchain technology is often described as a Libertarian ideal [6,7], but authors such as Scott offer a description of the technology that is very different to the standard description provided by Libertarianism [8]. They point to blockchain's co-operative consensus-driven model of collaboration and describe distributed autonomous organisations that suggest Socialist tendencies. Ludlow says this of cryptographic technologies, such as blockchain: "certain anarchist ideals may be possible, if not inevitable" [81]. Indeed, this paper suggests that, while BTC has properties that support Libertarian ideals, there is much about blockchain technology and its development that is directly applicable to various forms of Socialism.

Author Contributions: Steve Huckle is responsible for the conception and design of the work presented. He collected all of the included data and conducted the analysis and interpretation of that research. Steve Huckle also drafted the original article and completed subsequent revisions. Martin White provided critical revisions and approved the final article for publishing.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bitcoin Wiki. Category:History. Available online: https://en.bitcoin.it/wiki/Category:History (accessed on 16 July 2015).
2. Coinmarketcap.com. Crypto-Currency Market Capitalizations. Available online: http://coinmarketcap.com/ (accessed on 16 February 2016).
3. UK Government Chief Scientific Adviser. *Distributed Ledger Technology: Beyond Block Chain*; UK Government Office for Science: London, UK, 2015.
4. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
5. The Libertarian Party. Make a Bitcoin Contribution. Libertarian Party. Available online: https://www.lp.org/make-a-bitcoin-contribution (accessed on 4 August 2016).
6. Karlstrom, H. Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion Scand. J. Soc. Theory* **2014**, *15*, 23–36. [CrossRef]
7. Yermack, D. *Is Bitcoin a Real Currency? An Economic Appraisal*; National Bureau of Economic Research: Cambridge, MA, USA, 2013.
8. Brett Scott. *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?*; United Nations Research Institute for Social Development: Geneva, Switzerland, 2016.
9. Oxford Dictionary. Libertarianism. Available online: http://www.oxforddictionaries.com/definition/english/libertarianism (accessed on 7 July 2016).
10. Oxford Dictionary. Socialism. Available online: http://www.oxforddictionaries.com/definition/english/socialism (accessed on 7 July 2016).
11. UK Parliament. Parliamentary Sovereignty. UK Parliament. Available online: https://www.parliament.uk/about/how/role/sovereignty/ (accessed on 4 August 2016).
12. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 10 February 2016).
13. Antonopoulos, A.M. *Mastering Bitcoin*, 1st ed.; O'Reilly: Sebastopol, CA, USA, 2015.
14. Bitcoin. Choose Your Wallet—Bitcoin. Available online: https://bitcoin.org/en/choose-your-wallet (accessed on 7 September 2016).
15. Bitcoin Wiki. How to Accept Bitcoin, for Small Businesses—Bitcoin Wiki. Available online: https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses (accessed on 7 September 2016).
16. BitFury Group; Garzik, J. Public versus Private Blockchains Part 1: Permissioned Blockchains White Paper. Available online: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1--1.pdf (accessed on 2 March 2016).
17. Harvey, C.R. Bitcoin Myths and Facts. Available online: http://bit.ly/2cHRu90 (accessed on 24 February 2016).
18. Nakamoto, S. Bitcoin v0.1 Released. Available online: http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html (accessed on 12 February 2016).
19. Hal, F. Re: Bitcoin v0.1 Released. Available online: http://www.mail-archive.com/cryptography@metzdowd.com/msg10184.html (accessed on 12 February 2016).
20. Bitcoin. Bitcoin Developer Guide. Available online: https://bitcoin.org/en/developer-guide#block-chain (accessed on 29 February 2016).
21. Guadamuz, A.; Marsden, C. Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday* **2015**, *20*. [CrossRef]
22. Ethereum. Ethereum Project. Available online: https://www.ethereum.org/ (accessed on 23 July 2016).
23. Ripple. Welcome to Ripple. *Ripple*. 2016. Available online: https://ripple.com/ (accessed on 4 August 2016).
24. Litecoin. Litecoin—Open Source P2P Digital Currency. Available online: https://litecoin.org/ (accessed on 29 February 2016).
25. Stellar. *Stellar*. 2016. Available online: https://www.stellar.org (accessed on 29 February 2016).

26. Eris Industries. Explainer | Smart Contracts. *Eris Ind. Doc.* 2016. Available online: https://docs.erisindustries.com/explainers/smart_contracts/ (accessed on 29 February 2016).
27. The Economist. *The Trust Machine*; The Economist: St. Louis, MO, USA, 2015.
28. Bitcoin Wiki. Proof of Burn—Bitcoin Wiki. Available online: https://en.bitcoin.it/wiki/Proof_of_burn (accessed on 26 February 2016).
29. Harvey, C.R. *Cryptofinance*. 2016. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438299 (accessed on 27 April 2016).
30. bitcoinmining.com. Best Bitcoin Mining Hardware ASICs Comparison. Available online: https://www.bitcoinmining.com/bitcoin-mining-hardware/ (accessed on 26 September 2016).
31. Ethereum. Ethereum White Paper. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 20 March 2016).
32. Andresen, G. Seventy-Five, Twenty-Eight. *Gavin Andresen on Svbtle*. 2015. Available online: http://gavinandresen.ninja/seventyfive-twentyeight (accessed on 27 April 2015).
33. Bitcoin. Bitcoin Core. Available online: https://bitcoin.org/en/bitcoin-core/ (accessed on 29 February 2016).
34. Amazon.com. Amazon.com: Antminer S7~4.73TH/S with 2 Fans @ .25W/GH 28nm ASIC Bitcoin Miner: Computers & Accessories. Available online: https://www.amazon.com/Antminer-~4--73TH-Fans-Bitcoin-Miner/dp/B014OGCP6W (accessed on 29 September 2016).
35. Blockchain.info. Bitcoin Hash Rate. Available online: https://blockchain.info/charts/hash-rate (accessed on 22 July 2016).
36. International Energy Agency. Key World Energy Statistics. Available online: http://www.iea.org/publications/freepublications/publication/KeyWorld2016.pdf (accessed on 29 September 2016).
37. W3C. Common Markup for Micropayment Per-Fee-Links: A W3C Public Working Draft. Available online: https://www.w3.org/TR/Micropayment-Markup/ (accessed on 4 August 2016).
38. Bitcoin Wiki. Double-Spending—Bitcoin Wiki. Available online: https://en.bitcoin.it/wiki/Double-spending (accessed on 4 August 2016).
39. Buterin, V. On Public and Private Blockchains. Available online: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed on 15 February 2016).
40. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Programm. Lang. Syst.* **1982**, *4*, 382–401. [CrossRef]
41. Douceur, J.R. *The Sybil Attack*; Microsoft Research: Redmond, WA, USA, 2002.
42. Andrychowicz, M.; Dziembowski, S. *Distributed Cryptography Based on the Proofs of Work*; University of Warsaw: Warsaw, Poland, 2014.
43. David Boaz. Libertarianism | politics | Britannica.com. Available online: http://www.britannica.com/topic/libertarianism-politics (accessed on 26 June 2016).
44. Woodcock, G. *Anarchism: A History of Libertarian Ideas and Movements*; Broadview: Peterborough, ON, Canada; Orchard Park, NY, USA, 2004.
45. Libertarian Party. *Libertarian Party Platform*; Libertarian Party: London, UK; Available online: https://www.lp.org/platform (accessed on 11 July 2016).
46. Martin, F. *Money: The Unauthorised Biography*; Vintage: New York, NY, USA, 2014.
47. Huber, J. What Is Sovereign Money? *Sover. Money*. 2016. Available online: http://www.sovereignmoney.eu/what-is-sovereign-money/ (accessed on 23 July 2016).
48. Key, F.S. Star Spangled Banner Lyrics. Available online: http://www.usa-flag-site.org/song-lyrics/star-spangled-banner/ (accessed on 30 June 2016).
49. Elliott, N.; Libertarian Alliance. *The Uses and Abuses of Money*; Libertarian Alliance: London, UK, 1992.
50. Boaz, D.; Kirby, D. *The Libertarian Vote*; Cato Institute: Washington, DC, USA; Available online: http://www.cato.org/publications/policy-analysis/libertarian-vote (accessed on 30 June 2016).
51. Smith, A. *The Wealth of Nations: An Inquiry into the Nature and Causes of the Wealth of Nations*; Wordsworth: Hertfordshire, UK, 2012.
52. Bitcoin Wiki. Controlled Supply—Bitcoin Wiki. Available online: https://en.bitcoin.it/wiki/Controlled_supply (accessed on 27 April 2016).
53. Miller, C. What the arrival of Bitcoin means for society, politics and you. *WIRED UK*. 2013. Available online: http://www.wired.co.uk/article/bitcoin-demos (accessed on 20 July 2016).

54. Bank of Canada. Seigniorage. Available online: http://www.bankofcanada.ca/wp-content/uploads/2010/11/seigniorage.pdf (accessed on 4 August 2016).
55. Martinez, J. XRP: Math-Based Currency. Available online: https://ripple.com/knowledge_center/math-based-currency-2/ (accessed on 23 July 2016).
56. Gehring, B. How Ripple Works. Available online: https://ripple.com/knowledge_center/how-ripple-works/ (accessed on 23 July 2016).
57. Rifkin, J. *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*; Palgrave Macmillan: New York, NY, USA, 2014.
58. Pozsar, Z.; Singh, M. *The Nonbank-Bank Nexus and the Shadow Banking System*; IMF Working Papers; International Monetary Fund: Washington, DC, USA, 2011; pp. 1–18.
59. Laeven, L.; Valencia, F. *Systemic Banking Crises Database: An Update*; International Monetary Fund: Washington, DC, USA, 2012.
60. Alessandri, P.; Haldane, A.G. *Banking on the State*; Bank of England: London, UK, 2009.
61. Pëtr Kropotkin. Anarchism: Its Philosophy and Ideal. The Anarchist Library. Available online: http://theanarchistlibrary.org/library/petr-kropotkin-anarchism-its-philosophy-and-ideal (accessed on 30 June 2016).
62. Arnold, N.S. Marx, Central Planning, and Utopian Socialism. *Soc. Philos. Policy* **1989**, *6*, 160–199. [CrossRef]
63. Graziani, A.; Vale, M. Let's Rehabilitate the Theory of Value. *Int. J. Political Econ.* **1997**, *27*, 21–25. [CrossRef]
64. Bakunin, M. On the International Workingmen's Association and Karl Marx. Available online: https://www.marxists.org/reference/archive/bakunin/works/1872/karl-marx.htm (accessed on 7 July 2016).
65. Ollman, B.; Schweickart, D. (Eds.) *Market Socialism: The Debate among Socialists*; Routledge: New York, NY, USA, 1998.
66. Tressell, R. *The Ragged Trousered Philanthropists*; Wordsworth Editions: Ware, UK, 2012.
67. Marx, K. Critique of the Gotha Programme. Available online: https://www.marxists.org/archive/marx/works/1875/gotha/index.htm (accessed on 7 July 2016).
68. Chang, H.-J. *Economics: The User's Guide: A Pelican Introduction*; Pelican Books: London, UK, 2014.
69. Marx, K. *Capital: A Critique of Political Economy*; Progress Publishers: Moscow, Russia, 1887; Volume 1.
70. Ernest Mandel. Karl Marx—6. Marx's Theory of Money. Available online: http://www.ernestmandel.org/en/works/txt/1990/karlmarx/6.htm (accessed on 7 July 2016).
71. Frederick Engels. Capital and Surplus Value. Available online: https://www.marxists.org/archive/marx/works/1877/anti-duhring/ch19.htm (accessed on 7 July 2016).
72. Marx, K.; Engels, F. *Manifesto of the Communist Party*; Progress Publishers: Moscow, Russia, 1848.
73. The Socialist Party of Great Britain. Why We Don't Need Money. The Socialist Party of Great Britain. Available online: http://www.worldsocialism.org/spgb/education/depth-articles/socialism/why-we-dont-need-money (accessed on 7 July 2016).
74. Graziani, A.; Vale, M. The Marxist Theory of Money. *Int. J. Political Econ.* **1997**, *27*, 26–50. [CrossRef]
75. Karl Marx. The Power of Money. Available online: https://www.marxists.org/archive/marx/works/1844/manuscripts/power.htm (accessed on 14 July 2016).
76. Oxford Dictionary. Utopian Socialism. Available online: http://www.oxforddictionaries.com/definition/english/utopian-socialism (accessed on 7 July 2016).
77. Draper, H. *Karl Marx's Theory of Revolution. 4: Critique of Other Socialisms*; Monthly Review Press: New York, NY, USA, 1990.
78. Frederick Engels. Socialism: Utopian and Scientific (Chapter 1). Available online: https://www.marxists.org/archive/marx/works/1880/soc-utop/ch01.htm (accessed on 14 July 2016).
79. David Graeber. *Are You an Anarchist? The Answer May Surprise You!* Available online: https://theanarchistlibrary.org/library/david-graeber-are-you-an-anarchist-the-answer-may-surprise-you (accessed on 22 July 2016).
80. Infoshop. An Anarchist FAQ—I.1 Isn't Libertarian Socialism an Oxymoron? Available online: http://www.infoshop.org/AnarchistFAQSectionI1 (accessed on 29 June 2016).
81. Ludlow, P. (Ed.) *Crypto Anarchy, Cyberstates, and Pirate Utopias*; MIT Press: Cambridge, MA, USA, 2001.
82. Graham, R. (Ed.) *Anarchism: A Documentary History of Libertarian Ideas*; Black Rose Books: Montreal, QC, Canada; New York, NY, USA, 2005.

83. Wright, A.; de Filippi, P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Available online: http://bit.ly/2cDOiqT (accessed on 3 August 2016).
84. Van Valkenburgh, P.; Dietz, J.; de Filippi, P.; Shadab, H.; Xethalis, G.; Bollier, D. Distributed Collaborative Organisations. Available online: http://bollier.org/sites/default/files/misc-file-upload/files/DistributedNetworksandtheLaw%20report,%20Swarm-Coin%20Center-Berkman.pdf (accessed on 3 August 2016).
85. Fairfield, J.A.T. BitProperty. *South. Calif. Law Rev.* **2015**, *88*, 805.
86. Shelter. Bedroom Tax: Are You Affected? *Shelter Engl.* 2016. Available online: http://england.shelter.org.uk/get_advice/housing_benefit_and_local_housing_allowance/changes_to_housing_benefit/bedroom_tax (accessed 3 August 2016).
87. BBC News. Family of disabled grandson: 'Bedroom tax unfair'. *BBC News*. 2016. Available online: http://www.bbc.co.uk/news/uk-wales-south-west-wales-35419211 (accessed on 16 January 2016).
88. Good Governance. What Is Good Governance—Good Governance Guide. Available online: http://www.goodgovernance.org.au/about-good-governance/what-is-good-governance/ (accessed on 23 July 2016).
89. Coindesk. Bitcoin Price Index—Real-time Bitcoin Price Charts. *CoinDesk*. 2016. Available online: http://www.coindesk.com/price/ (accessed on 14 July 2016).
90. Western Oregon University. Energy Basics. Available online: https://www.wou.edu/las/physci/GS361/EnergyBasics/EnergyBasics.htm (accessed on 29 September 2016).
91. BBC News. Bitcoin Rewards Halve for Virtual Cash Money Miners. *BBC News*. 2016. Available online: http://www.bbc.co.uk/news/technology-36763524 (accessed on 22 July 2016).
92. Aguirre, K.; Eisenhardt, L.; Lim, C.; Nelson, B.; Norring, A.; Slowik, P.; Tu, N. Lifecycle analysis comparison of a battery electric vehicle and a conventional gasoline vehicle. In *Full Lifetime Cost Analysis of Battery, Plug-in Hybrid and FCEVs in China in the Near Future, Frontiers in Energy*; Cai, Z., Ou, X., Zhang, Q., Zhang, X., Eds.; California Air Resources Board: Sacramento, CA, USA, 2012; Volume 6, pp. 107–111.
93. Bitcoin Wiki. Bitcoin Improvement Proposals—Bitcoin Wiki. Available online: https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals (accessed on 19 February 2016).