scripted

Volume 13, Issue 3, December 2016

DECENTRALISATION, DISTRUST & FEAR OF THE BODY – THE WORRYING RISE OF CRYPTO-LAW

Alan Cunningham[*]

Abstract

The increasing collective use of distributed application software platforms, programming languages and crypto-currencies around the blockchain concept for general transactions may have radical implications for the way in which society conceptualises and applies trust and trust-based social systems such as law. By exploring one iteration of such generalised blockchain systems – Ethereum – and the historical lineage of such systems, it will be argued that indeed their ideological basis is largely one of distrust, decentralisation and, ultimately, via increasing disassociation of identity, a fear of the body itself. This ideological basis can be reframed as a crypto-legal approach to the problems of human interaction, one whereby the purely technological solutions outlined above are considered adequate for reconciling many of the problems of our collective existence. The article concludes, however, by re-iterating a perspective of law more so as an entirely embodied and trust dependent notion. These aspects go some way to explaining the necessarily centralised role it takes on within societies. They also explain why the crypto-legal approaches advanced by systems like Ethereum – or even the co-opting of blockchain technology by law firms themselves – will only ever be at best efficiency exercises concerned with the processing of data relating to legal affairs, and not the more radical, ambiguous and difficult process of actual legal thought or, indeed, engagement with trust.

DOI: 10.2966/scrip.130316.235

[*] Lecturer, University of Manchester School of Law, United Kingdom. E-mail: alan.cunningham@manchester.ac.uk.

1. Introduction

The emergence and subsequent success of Bitcoin in 2009 was primarily driven by an underlying and, at the time, somewhat unheralded technology, the now infamous blockchain. Put simply, the blockchain ensured that Bitcoin could fulfil its promise of decentralisation from mainstream institutions and still function. Bitcoin, however, was concerned specifically with one function only, the decentralisation and anonymisation of *payment transactions.* Since its emergence, the blockchain concept has been co-opted, in conjunction with other technologies and principles, to apply to potentially all manner of transactions.

This move towards generalising the application of the blockchain concept has important implications for the notion of trust and trust-based social systems such as law. This is due to the fact that the entire basis for the development of the blockchain system within Bitcoin was to ensure that the so-called "weakness" of the trust-based model (whereby individuals and institutions are trusted, but trust can never truly be guaranteed,) could, in theory, be bypassed.

In this article, I will examine some of the implications – but more so the somewhat problematic ideological basis – of this move towards generalised blockchain applications. By exploring one specific iteration of generalised blockchain, a platform called Ethereum, I hope to illustrate the potential danger in how society conceptualises law, particularly in regard to the important role played in law by trust, centralisation and, for the most part, an identifiable bodily involvement.

2. Ethereum

Ethereum is "a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference."[1] Fuelled by a crypto-currency called Ether, which can be purchased, gifted or obtained through the voluntary validation of transactions on the network, individuals pay for programs running on Ethereum.[2] Programs running on the Ethereum platform may in turn generate their own internal crypto-currencies using the platform, but what is more interesting about Ethereum and the programs running upon it are the uses to which they can be put.

Examples of current projects include: decentralised applications such as Airlock, a "next generation keyless access protocol for smart property"[3]; Boardroom, a "block chain governance suite" that amongst proposed uses includes arbitration and equity allocation to board members[4]; and slock.it[5], wherein "slocks", or smart, safe, secure locks, control real world physical objects (the owner of a slock sets a deposit, if

[1] "Ethereum: Homestead Release Blockchain App Platform" (2016) available at https://www.ethereum.org (accessed 10 Nov 16).

[2] As of the date of writing (30 October 2016), 1 Ether was worth, respectively, Euro 9.33, £8.41, $10.25 and 0.0145 Bitcoin.

[3] "airlock" available at http://www.oranjeblock.com/airlock/ (accessed 10 Nov 16).

[4] "Boardroom: Blockchain Governance DApp" (2015) available at http://boardroom.to (accessed 10 Nov 16).

[5] "Slock.it" (2015) available at https://slock.it (accessed 10 Nov 16).

necessary, and a price for using the item; users find slocks using mobile apps and make a payment on the Ethereum blockchain). Of particular interest to lawyers, law firms, and perhaps technology companies or technologists who may view the law as just another service in need of a disruption they can provide, is how Ethereum proposes the handling of such generalisable transactions.

It is suggested that that the use of a blockchain, in conjunction with a crypto-currency, Turing completeness, and a decentralised, largely anonymous structure, will guarantee the enforceability element of such transactions, without any need for trusted third parties or, indeed, trust in the law as a reliable social praxis. This paper is not primarily concerned with the role of the law in regulating the space that technologies such as Ethereum have opened or will open up. Rather it is concerned with the ideological perspective that appears to be driving such developments and how that perspective conflicts with another, perhaps more valuable perspective, about what the law can be.

What is unique about the projects listed above, and specifically with Ethereum, is therefore not necessarily the substance of what they want to do i.e. what substantive matters any particular Ethereum-based contract is concerned with, such as insurance or leasing of property. It is instead the manner of execution. Given how transaction success is guaranteed within such systems, one can see that a particular perspective on "what law is" is maintained. It is seen as largely untrustworthy, too centralised within large institutions and, ultimately, fearful of the role the body plays in interacting and adjudicating with others.[6] All transactions running on Ethereum will, it is argued, be cryptographically secure, decentralised (not dependent on trusted third party intermediaries for any aspect of the transaction, apart from the code, of course, a point which I will address later) and anonymous[7].

Given the potential range of uses of Ethereum (including not just the applications mentioned above but also the creation of, for example, democratic autonomous organisations (DAOs)[8], or the development of trustless crowd sales[9]), these relatively new ways of transacting will have important and potentially radical implications.

[6] By body I mean the primarily physical nature of the body inhabited by the individual, the body, therefore, as a largely untrustworthy human element in transactional affairs (the impossibility of absolute trust being due to the physicality of the body, the physical constraints any body imposes on our more easily realized ideals). I write this not to denigrate the notion of the body; quite the opposite. As will be discussed later in this article, it is precisely this element of our bodily existence that law relates – and should relate – to. Given the crypto-anarchistic basis of decentralized systems such as Ethereum – the aspiration towards abstraction of agency from any slightly more compromised physicality – this definition, and my emphasis on fear of bodies as an ideological position underlying decentralized systems, is both apt and necessary.

[7] Although via basic network analysis techniques, Ethereum cannot be considered completely anonymous – as it would have some believe. However, Ethereum certainly reinforces pseudonymity through the dissociation from body and identity that it involves.

[8] Instead of, as with traditional organisations, having to "hire managers, find a trustworthy CFO to handle the accounts, run board meetings and do a bunch of paperwork", Ethereum suggests that you instead "simply leave all that to an Ethereum contract. It will collect proposals from your backers and submit them through a completely transparent voting process." As they add, "One of the many advantages of having a robot run your organisation is that it is immune to any outside influence as it's guaranteed to execute only what it was programmed to."

An important preliminary aside regarding these DAOs – or, rather, one DAO in particular (important as reference will be made to this DAO throughout). In June 2016, and in a major blow to the claims of Ethereum as being highly secure and immune to outside influence, a hack was undertaken on a DAO that had been created as a vehicle for supporting Ethereum related projects. This DAO is generally referred to as "The DAO" (or the DAO Hub), given its success in relation to other deployed DAOs. The DAO, through the purchase of DAO tokens (which provide voting rights to owners) had accumulated roughly $130million worth of Ether by the time of the hack. The purpose of the DAO fund was to fund sharing economy projects.

In June 2016, however, and taking advantage of a vulnerability in how members exited from the DAO, a hacker removed Ether units worth, at the time of the hack, some $76 million (not unexpectedly, the dollar value of Ether units plummeted in the wake of the hack). Generally considered to be an issue with the DAO and not with Ethereum itself, the Ethereum community considered a number of solutions to the theft (solutions were still possible as there is a 27 day waiting period factored into exits). These solutions were to do nothing; a soft fork; or a hard fork. Soft forking would have added a patch to the Ethereum code to freeze the stolen Ether so that it could not be used. Hard forking would roll back the transactions in the blockchain and effectively reverse the hack. Ethereum community members voted for the hard fork and it was undertaken in July 2016.

This reaction to the hack – a decision being made by human beings based on circumstance and consensus, and not simply by code itself – illustrates the discrepancy between the aspirations of systems such as Ethereum and the reality of and need for contextual decision making in hard cases. The hard fork solution was a judgment call. Contextual elements had to be considered in deciding how to judge.

The implications of this hack will be the subject of more in-depth discussion throughout this article. Prior to that, however, and in order to understand and appreciate what systems such as Ethereum[10] are doing and why they may have radical implications for trust, institutions and the law (indeed for the very idea of the state itself) one needs to look first at its antecedents.

In particular, one needs to look at Bitcoin, itself a decentralised system (albeit a decentralised *peer-to-peer payment* system). More specifically one needs to look at the *cryptographic* and *anarchistic* underpinnings of this antecedent. They highlight the role distrust (or rather a pining for trust that can be 100% guaranteed) and fear of the human element, emerging from the physical body, play in the architecture of blockchain-based systems.

[9] As provided on Ethereum.org, "Using Ethereum, you can create a contract that will hold a contributor's money until any given date or goal is reached. Depending on the outcome, the funds will either be released to the project owners or safely returned back to the contributors. All of this is possible without requiring a centralized arbitrator, clearing house or having to trust anyone." See note 1 above.

[10] Equivalent systems include: Counterparty (although Counterparty is more concerned with the decentralisation of finance); Monax (previously 'Eris' and more similar to Ethereum) and Ripple (slightly less decentralised, more in-sync with existing institutional frameworks). "CP" (2016) available at counterpartyfoundation.org (accessed 8 Nov 16); "Monax: The Ecosystem Application Platform" (2016) available at https://monax.io/?redirect_from_eris=true (accessed 8 Nov 16); "Ripple" (2016) available at https://ripple.com (accessed 8 Nov 16).

3. Cryptography and Currency

It was, arguably,[11] Wei Dai who first suggested that a form of money controlled by *cryptography* rather than by a centralised banking authority or commercial bank – banks being nothing more than centralised (to varying degrees) but more importantly *trusted* institutions – could and indeed should be developed.[12] Cryptography, especially in relation to the transfer of data over the Internet, can be understood as the development of techniques – encryption methods – that can secure communication in the presence of potential, unrequested observance of third parties (governments, commercial organisations, private individuals). Such encryption techniques can ensure that data is kept confidential and also that it is authentic. The most basic level of encryption used online involves the use of public keys and private keys.[13] The parties to an encrypted communication are concerned primarily with ensuring that information is as private as it can be but they are equally concerned that they can trust that the encrypted message is from whoever they expect it to be from.

In this sense, privacy and trust – not necessarily easy to align completely – must enter into a compromise with each other. Privacy and trust are difficult, though not impossible, to align, because true privacy to the point of anonymity makes authentication of identification difficult. Conversely openness and trust are easier to align – at least offline – because of the need for the presence of the actual person and not an anonymous identifier. Absolute privacy therefore takes one further away from bodily presence, beginning with the separation of real identity, the link to the body, from pseudonymous identity. This separation is obviously appealing from certain political perspectives but it comes at a cost; that cost is the existence of a general level of trust regarding society at large. Here, we can begin to see the implications of the removal of previously trusted third parties, including, notably, the institution and the idea of law. The greater the level of privacy that is possible, the higher the risk to trust as a general concept and social practice.

The specific suggestion from Wei Dei regarding the development of a crypto-currency was, as he termed it, "b-money" (a scheme for a group of "untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without any outside help"[14]). Crucially, there were strong *anarchistic* elements underpinning the b-money concept. In understanding this anarchistic root, one can better appreciate the link to decentralisation and anonymity within blockchain based systems.

[11] Nick Szabo, for example, is also considered one of the pioneers in this field, with his equivalent Bit Gold concept.

[12] However, see also: J Bonneau et al, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies"(2015) *IEEE Symposium on Security and Privacy* available at https://eprint.iacr.org/2015/261.pdf (accessed 8 Nov 16).

[13] In such an encryption method the public key (the clue is in the name) is disseminated widely and freely to the public at large. One can easily encrypt the message on the sending side using this public key, but only the recipient (in theory) has access to the private key, which is used to decrypt the message upon receipt.

[14] http://www.weidai.com/ (accessed 27 Nov 16).

4. Anarchy

Dai has written, discussing crypto-anarchy:

> Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because *its participants cannot be linked to their true names or physical locations (author's italics)*.[15]

Here we see the abstraction of identity – the removal of actions from the body acting – almost to the point of disappearance. For the crypto-anarchist, the state has (or at least should have) no reach over the body. But note how this abstraction is aligned with a still very active agency, through technology and more specifically, cryptography.

The emergence of encryption alongside increased digitisation and distributed communications, and even more with the increased commercialisation and regulation of the Internet, must be understood in the broader context of changing political attitudes concerning privacy, trust and the role of centralised, governmental institutions. In particular, it needs to be understood not only in relation to the anarchistic underpinnings of decentralised systems (which can explain the distrust of third parties), but also in relation to their *libertarian* underpinnings (which can explain the requirement of a maintenance of agency alongside a very real distrust).

The cypherpunk movement of the early 1990s is a pertinent example of how these themes of privacy, trust and technology – and a particularly libertarian political philosophy – all mingled together to produce some rather interesting practical results that have continued to influence the decentralised transaction platforms of today.

5. Cypherpunk

Cypherpunks – a neologism allegedly developed from the words *cipher* and *cyberpunk* (and not to be confused with the latter) – were described in "A Cypherpunk's Manifesto" as being "dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money."[16]

Eric Hughes, the author of "A Cypherpunk's Manifesto", explained that, in defence of the "open society" the cypherpunk wanted to reconcile freedom of speech with privacy. Reconciling these two rights was felt to be necessary because of the increasing power of electronic communication. Moreover, such a reconciliation was necessary because of the increasing capability of governments to use powerful electronic communication technology for what might be potentially invasive uses e.g. increased civilian surveillance. Indeed, countering this increasing power appears to be

[15] W Dai, "B-Money" (1998) available at http://www.weidai.com/bmoney.txt (accessed 8 Nov 16).

[16] E Hughes, "A Cypherpunk's Manifesto" (1993), available at http://www.activism.net/cypherpunk/manifesto.html (accessed 8 Nov 16).

the entire justification for the cypherpunk movement, if one views it as simply a very specific iteration of a libertarian organisation – one focused specifically on addressing freedoms in relation to electronic communication. Hughes has argued, “If I say something, I want it heard only by those for whom I intend it.”[17] This is defensible, of course, but as any good lawyer will tell you, is dependent on the venue where the statement is made and often on the role of the person saying it.

Hughes goes on to argue, “If the content of my speech is available to the world, I have no privacy.”[18] True again, in theory, but what one says is only really available to the whole world when one says it within the electronic medium. Privacy is easier to enforce in a small room in a house. Something posted online is much more difficult to keep private. In a sense, one can begin to see the non-compromising position that underpins much libertarian thinking. The individual is sovereign but society imposes somewhat annoying restrictions on the individual. These attitudes, I argue, feed into the architecture of contemporary decentralised platforms, but, problematically, cannot be indefinitely maintained in social systems. This is not to suggest, of course, that private individuals should not have a default expectation that private communications are private, even if made online. But it does speak to a potential unreasonableness inherent in libertarian conceptions of privacy. This unreasonableness may well be an ideological baseline for the systems and concepts that predate Ethereum and which, arguably, led to its emergence.

The difficulty for governments – and indeed commercial organisations – is that the data created through online transactions is too tempting to turn down. Indeed, companies provide individuals with free services in order to get their fill of it.[19] Hughes was well aware of this, writing that: “We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak.”[20] As a result, he argued:

> We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.[21]

All of this has to be read against the backdrop of broader political attitudes towards governments and commercial organisations operating in free-market societies, especially in the United States, with its long history of scepticism towards too much government.[22] Hughes, a mathematician, was not the only founding member of the

[17] *Ibid.*

[18] *Ibid.*

[19] For example, note, *inter alia*, the entire free software as a service (SaaS) phenomenon.

[20] E Hughes, see note 16 above.

[21] *Ibid.*

[22] Ronald Reagan seemed to represent this feeling best when he memorably commented in his 1981 inaugural address as President of the United States, “Government is not the solution to our problem; government is the problem”. Indeed, the very existence of the US can be seen as a perhaps admirable

Cypherpunks. The other two were Timothy C May, an electronic engineer, and John Gilmore, a self-proclaimed civil libertarian, and all members were US citizens.

Stephen Levy, writing in *Wired* magazine of an early Cypherpunk meeting at the offices of private company Cygnus Support, highlighted how: "everything has an underlying, if not explicitly articulated, political theme: the vital importance of getting this stuff out to the world for the public weal."[23] Technology was thus co-opted into realising this political objective with a great degree of faith – trust, in other words – placed in the ability of technology to assist in political aims. In the words of Hughes, evidencing a great degree of computationalism (to be discussed in more detail below): "That's the kind of society I want to build. I want a guarantee – with physics and mathematics, not with laws – that we can give ourselves real privacy of personal communication."[24]

Here we see the roots of what could be termed a very real *crypto-law*: fearful of the possibility of error, determined to obtain 100% accuracy in all matters, and, perhaps most crucially of all, somewhat sceptical of the necessary bodily element – the requirement for the bodily element – in all human affairs and especially in our conceptualisations of justice.

6. The Problem of Exchange, or: Existence is an Exercise in Compromise, even for Libertarians

Privacy and decentralisation from the state and third parties are central tenets behind encryption use. Therefore there is an implicit support of libertarianism and tendency towards absolute agency, perhaps, in some iterations, towards complete anarchism (maybe even anarcho-capitalism, given the maintenance of currency concerns): the complete elimination of the state as a legitimate political system and organisation; the complete agency of the individual to act at his or her liberty. This mixed bag of political underpinnings of the early cypherpunk movement travelled through to developments such as crypto-currencies, although one might well wonder how anarchistic movements would favour the establishment of a *currency*. It is arguable, however, that a crypto-currency – as opposed to a normal currency – actually encourages separation from the state. More specifically, such crypto-currencies encourage separation from a state *that is feared* and perhaps eventually makes that state, as Dai puts it, "permanently forbidden and permanently unnecessary."[25]

The problem, of course, is that even for libertarians or anarchists, exchange is still necessary, and there is no guarantee that those with whom one is exchanging will share one's political belief or beliefs about how to live. Some might become completely self-sufficient, of course, but there will always be a limit to self-

reaction against too much government. Ronald Reagan "Inaugural Address" (1981) available at http://www.presidency.ucsb.edu/ws/?pid=43130 (accessed 8 Nov 16). More recently, US President-elect Donald Trump can be seen as representing another, perhaps much more dangerous, iteration of this inherently sceptical approach towards the value of centralised government and intensive government involvement in certain matters.

[23] S Levy, "Crypto Rebels" (1994) available at http://archive.wired.com/wired/archive/1.02/crypto.rebels_pr.html (accessed 8 Nov 16).

[24] E Hughes, see note 16 above.

[25] W Dai, see note 15 above.

sufficiency, especially in matters where specific skills or technologies are required. Exchange with those who perhaps still operate within the feared state, using its laws, currencies and potentially untrustworthy intermediaries, will therefore occasionally be required. Unless, of course, one can develop one's own medium of exchange. Doing so brings one closer to the libertarian dream of almost complete sovereignty.[26]

Dai acknowledged all of this and believed it to be the key element in developing such a crypto-anarchistic community, pointing out that:

> Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government-sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by *untraceable entities (author's italics)*.[27]

This protocol was b-money and lack of traceability – effective encryption – was a core feature. The purpose of it was not to simply remove the role of government and third parties but to increase the sovereignty and agency of the individual alongside that. Dai in fact suggested two protocols, both of which assumed "the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e. public keys) and every message is signed by its sender and encrypted to its receiver."[28]

In the first protocol, every participant would maintain a separate database of how much money belonged to each pseudonym. "Money" would be created by the publication of a solution of a previously unsolved computational problem. The only conditions proposed by Dai regarding this process were that "it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual."[29] Dai's early work on b-money was notably referenced in the paper published by Satoshi Nakamoto[30] where he introduced the Bitcoin concept – a lineage that takes us even closer to the current decentralised systems.

[26] Although, as my Manchester colleague Vincenzo Bavoso has pointed out in feedback on an earlier draft of this paper, this still does not answer the question: what is the value of money, and how is it developed? Bavoso considered that crypto-currencies could be seen as being completely baseless in value precisely *because of* the absence of the state. In this sense, any universal value only comes from an *imprimatur* from the majority and/or authoritative position. Thus, rather perversely, the creation and use of successful crypto-currencies in fact requires the establishment of some kind of authoritative/majority position, such as occurred, e.g. in resolving the DAO hack.

[27] W Dai, see note 15 above.

[28] *Ibid.*

[29] *Ibid.*

[30] S Nakamoto, "Bitcoin: A Peer to Peer Electronic Cash System" (2008) available at http://nakamotoinstitute.org/bitcoin/ (accessed 8 Nov 16).

7. Bitcoin

Nakamoto introduced his paper on Bitcoin by arguing that while online commercial transactions rely almost exclusively on existing financial institutions to serve as a trusted third party to facilitate electronic payments, such systems suffer "from the inherent weaknesses of the trust based model."[31] One might wonder whether Nakamoto thought the trust based system had an inherent weakness or whether he simply could not accept anything less than a 100% percent guarantee of trust being enforced. It is at this stage of the philosophical lineage of the decentralised systems like Ethereum that a new element is added to the mix, alongside anarchism and libertarianism; something we can now term "computationalism". I argue that computationalism is a complete faith in the ability of mathematics and technology to eradicate problems emerging from human behaviour.

In theory, Nakamoto is right; it is arguable that trust is completely defined by an acceptance of the possibility of betrayal. In other words, trust incorporates an understanding that no one person can be trusted completely. Without this element of risk, there is no trust. Arguably, however, what is more important than being assured that one can trust someone 100% is instead a guarantee that one can trust them to be competent in the trust relationship *in some way*. Therefore, I argue that from the very beginning, Nakamoto fundamentally misunderstood the notion of trust, expecting it to be perfect, neglecting inevitable problems associated with the element of trust in transactions. This misunderstanding feeds into the architecture of all decentralised systems that emerge from the block-chain technology (as was illustrated with the DAO hack). In fact, I argue that this mistaken understanding of trust drives most, if not all, of the associated decentralised systems, albeit somewhat implicitly. Expectations regarding trust, and understandings of the nature of trust are, in this sense, far too high.

Nakamoto argued that what was needed to facilitate the trust required (100%) was "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."[32] In other words, to create a fully trustworthy transaction, trust as a social construct must be replaced with a different type of trust: a trust only in mathematics.

8. Double Spending and Trust

Nakamoto argues that Bitcoin was also a response to a specific problem, the so-called "double-spending" problem. Double spending is complex, but it is an important concept to understand. As a problem to which the blockchain responds, it further illustrates the necessary side-lining of trusted third parties within blockchain based systems. Double spending occurs in digital cash systems and results from the fact that unlike transactions with physical token money, such as a coin or a note, it is difficult to prevent people from spending digital cash twice. Electronic files can be easily replicated. One possible solution to this problem is, as Nakamoto argued:

> to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction,

[31] *Ibid.*

[32] S Nakamoto, see note 30 above.

> the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.[33]

In other words, as with most socially complex systems, someone *other* than oneself has to be trusted. At a certain point, if one is interacting with others, someone or, indeed, something, has to be trusted.[34]

Of course, given the crypto-anarcho-capitalistic tendencies underlying the Bitcoin project, this solution of a single, centralised, trusted third party such as a mint was considered unsatisfactory. Due to the computationalism inherent in the thinking of the participants, technology was believed to offer a more secure solution.

Nakamoto suggested in his paper that the system itself needs a way "for the payee to know that the previous owners did not sign any earlier transactions"; or, in other words, "the earliest transaction is the one that counts". And, as he also stated, "the only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first."[35] The mint based model, relying as it does on the very existence of the mint as a third party (and also on its administration and running by actual, potentially untrustworthy, people) is not satisfactory in counteracting the weaknesses of the trust based model.

Crucially, therefore, Nakamoto argued that to solve the double buying problem without recourse to a trusted third party, all transactions must be publicly announced and a system required for participants to agree to a single history of the order in which they were agreed. This public nature to the transactions is admirable, but should not distract from the concurrent retreat into an excessive, and potentially problematic, individual sovereignty. Publication only serves as a retreat from trust as a social, necessarily flawed construct.

The Bitcoin solution was a combination of (a) timestamp server and (b) application of the Proof-of-Work concept. Proof-of-Work – a concept first coined by Jakobsson and Juels[36] – is a notion whereby, in contrast to a number of cryptographic protocols

[33] *Ibid*. I am reminded here of a comment by Bertrand Russell, that "Man is not a solitary animal, and so long as social life survives, self-realisation cannot be the supreme principle of ethics" (B Russell, *A Short History of Western Philosophy* (London: Routledge, 2016)). One could compare this with another comment, by Nietzsche: "Every superior human being will instinctively aspire after a secret citadel where he is set free from the crowd, the many, the majority" (F Nietzsche, *Beyond Good & Evil* (London: Penguin, 2003)) – which perhaps represents the more libertarian side of the human interaction coin.

[34] Of course, the separation of powers theory, which was instrumental in US government evolution (and itself a reaction to what was felt to be a much too centralised and powerful government) could also offer an alternative solution. Perhaps in the future landscape of decentralised systems this might be a possibility. But why would the decentralised platforms allow for this – and why, perhaps, should they?

[35] S Nakamoto, see note 30 above.

[36] M Jakobsson and A Juels, "Proofs of Work and Bread Pudding Protocols", in B Preneel, (ed.) *Communications and Multimedia Security* (Kluwer Academic Publishers, 1999), 258–272.

where "a prover seeks to convince a verifier that she possesses knowledge of a secret or that a certain mathematical formula holds true", a prover instead "demonstrates to a verifier that she has performed a certain amount of computational work in a specified amount of time."[37] The timestamp server works by "taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper of Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get the hash."[38] The combination of the two facilitates electronic transactions without relying on trust. Trust is thus replaced with proof of work and a timestamp.

The innovative element of Bitcoin is the fact that there is no "trust" involved in the sense that there is no known backer, no recognised issuer such as a national central bank and of course, therefore, there is no established value embodied in the third party. As noted in The Economist:

> This set-up is the first workable solution to one of the more nagging problems of the digital realm: how to transfer something of value from one person to another without middlemen having to make sure that the item is not copied or, in the case of money, spent more than once? And Bitcoin does the trick while being open (unlike conventional payment mechanisms, which aim for security by shielding themselves from outsiders). This means that third parties can make use of Bitcoin's features without having to ask anyone for permission—as is the case with the Internet.[39]

What are of some value, of course, are these very facts. The non-existence of such institutions is the thing of value. It is itself illustrative of a severe (but arguably deserved) lack of trust in established and centralised banking institutions in developed economies and an interest in developing alternatives, but also of the fact that the trust has simply been displaced. For those involved trust does exist, just simply in themselves alone; in their individuality, once allied with the requisite technology.

Admittedly, Bitcoin is only a solution to a number of trust and encryption problems in pursuit of a digital cash system that could eliminate the need for a trusted third party or centralised institutions. It contains political underpinnings but is focused purely on digital cash. Ethereum and systems like it address a much wider field of activity.

9. Ethereum

Proponents of Ethereum, and of decentralised systems like it, are positing that certain concepts contained within the Bitcoin model can be adapted *for potentially any transactional use*; or at least any transaction requiring some form of consensus, which is much the same thing. As stated in the current Ethereum white paper:

> Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency,

[37] *Ibid.*

[38] M Jakobsson and A Juels, see note 36 above.

[39] "Bitcoin's Future: Hidden Flipside" (2014) available at http://www.economist.com/news/finance-and-economics/21599054-how-crypto-currency-could-become-internet-money-hidden-flipside (accessed 8 Nov 16).

> being the first example of a digital asset which simultaneously has no backing or "intrinsic value" and no centralized issuer or controller. However, another, arguably more important, part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus.[40]

The white paper refers to commonly cited applications of this innovative blockchain technology such as "using on-blockchain digital assets to represent custom currencies and financial instruments"; "the ownership of an underlying physical device"; "non-fungible assets such as domain names"; as well as "more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules…or even blockchain-based "decentralized autonomous organizations."[41]

Key in all of this, of course, is the blockchain concept, first established to deal with weaknesses in the so-called "trust based model" concerning the minting of money.

9.1 Applying the Proof of Work Blockchain Concept to All Things

The Economist has another way of describing the blockchain concept; it is instead "the great chain of being sure about things".[42] Or, as it was also put, it is "a way of making and preserving truths", offering "a way for people who do not know or trust each other to create a record of who owns what that will compel the assent of everyone involved."[43]

The blockchain is simply the chain of the proof of work plus the timestamp server. Once the proof of work exists, along with a time stamp, a block is created, itself containing a hash code of the previous blocks header data. As pointed out, "this hashing is a one way street" and "it is this concatenation that makes the blocks into a chain".[44] Within Bitcoin, creating blocks creates new bitcoin. Most data in the blockchain are concerned with bitcoin, but they do not have to be. In this respect, it has been suggested, "Mr. Nakamoto has built what geeks call an "open platform"—a distributed system the workings of which are open to examination and elaboration."[45]

Ethereum builds upon the blockchain innovations developed in the Bitcoin concept and, indirectly, the conceptual avoidance of reliance on a trusted third party. For Nakamoto, the problem was in trusting a third party with money going in and out of the mint. With Ethereum, the problem of trust is compounded by application to a much wider group of transactions, and in a way can be viewed not as a problem with

[40] "White Paper: A Next Generation Smart Contract and Decentralised Application Platform" (2016) available at https://github.com/ethereum/wiki/wiki/White-Paper (accessed 8 Nov 16).

[41] *Ibid.*

[42] "Blockchains: The Great Chain Of Being Sure About Things" (2015) available at http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable (accessed 8 Nov 16).

[43] *Ibid.*

[44] *Ibid.*

[45] *Ibid.*

trust but as a concern about having more agency in all things. The problem thus turns into one of trusting information use *generally;* having agency over potentially anything, with the blockchain. This problem is otherwise known as the "Byzantine General Problem" (or BGP), a problem in computer science where by trust in general is hard to establish. Simply put:

> Imagine a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement.[46]

In general terms, the "B.G.P. poses the question of how to establish trust between otherwise unrelated parties over an untrusted network like the Internet."[47] This is a slightly more advanced notion of the trust issue related to a specific central authority, such as a mint; here the problem is how to trust parties in general, for any informational purpose. Applying the blockchain concept to the problem – since "any type of asset can be can be transferred into the blockchain"[48] – simply required a conceptual leap, which Ethereum and some others have taken. Their leap, however, is potentially the most radical of those of the blockchain innovators.

This is because some blockchain based innovations are concerned merely with the transfer of assets, riding on the back of blockchain bitcoins with additional "data dyes" to represent, for example, shares or bonds.[49] Others simply use the blockchain as a registry of ownership.[50] Systems like Ethereum, however, want to use the blockchain for "smart contracts", wherein programmed rules running on the Ethereum blockchain have a very active agency, either simply as contracts, as autonomous organisations, or even, most radically, as the abstract regulation of third party objects. Thus, as has been suggested:

> a car-key embedded in the Ethereum blockchain could be sold or rented out in all manner of rule-based ways, enabling new peer-to-peer schemes for renting or sharing cars. Further out, some talk of using the technology to make by-then-self-driving cars self-owning, to boot. Such vehicles could stash away some of the digital money they make from renting out their keys to pay for fuel, repairs and parking spaces, all according to preprogrammed rules.[51]

[46] L Lamport, R Shostak and M Pease, "The Byzantine Generals Problem" (1982) 4 *ACM Transactions on Programming Languages and Systems*, 382-401 http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf (accessed 8 Nov 16).

[47] M Andreessen, "Why Bitcoin Matters" (2014) available at http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (accessed 8 Nov 16).

[48] "White Paper", see note 40 above.

[49] "Colu" available at https://www.colu.co (accessed 8 Nov 16).

[50] "Everledger" (2015) available at http://www.everledger.io (18 Nov 16).

[51] "Blockchains", see note 42 above.

How disputes are to be resolved in such scenarios is, of course, another matter entirely. The difficulty that occurred with the DAO hack over the summer of 2016 illustrated that human based adjudication is still required.

The consequence of this innovative leap is that, as with all previous efforts to decentralise, irrespective of intention, the value of previously centralised and trusted institutions is considerably lessened. One must then consider: are these systems being developed because trust more generally in centralised institutions and concepts is weakening, or is trust weakening because of the development of these systems that no longer depend on centralised institutions or concepts? Regardless, one can clearly see the attraction of systems such as Ethereum. Trustless transactions – not just of a monetary nature – are possible, so why pay for the middleman to ensure trust? Why worry about the notion of trust as a social concept at all?

Arguably, and as previously discussed, trust is not necessarily removed within this system; it is merely displaced to technology and writers of code. Can they be trusted any more than centralised institutions and established doctrine? Will they themselves not also become entrenched and centralised over time? The Economist refers to critics of systems like Ethereum, who see it simply as:

> the latest techy attempt to spread a "Californian ideology" which promises salvation through technology-induced decentralisation while ignoring and obfuscating the realities of power—and happily concentrating vast wealth in the hands of an elite.[52]

They add, "the idea of making trust a matter of coding, rather than of democratic politics, legitimacy and accountability, is not necessarily an appealing or empowering one."[53] In addition, with regard to certain transactions, such as hedging contracts, even Ethereum states that:

> Note that this approach is not fully decentralized, because a trusted source is still needed to provide the price ticker, although arguably even still this is a massive improvement in terms of reducing infrastructure requirements (unlike being an issuer, issuing a price feed requires no licenses and can likely be categorized as free speech) and reducing the potential for fraud.[54]

As Ethereum admits there may well be intermediaries, because (a) people like doing things and adding value to the things that they do and (b) some people are prepared to pay for that added value, as it (the payment, allied with the incentive of receiving payment for something done) can sometimes minimise the risk that Ethereum itself – and systems like it – seem so afraid of.

[52] *Ibid*.

[53] *Ibid*.

[54] "White Paper", see note 40 above.

10. Ethereum in Practice

Ethereum can thus be best understood as a model of doing things that combines a number of already existing technologies and concepts. What is potentially innovative about the Ethereum platform is that it believes it can be generalisable, the "technology on which all transaction–based state machine concepts may be built."[55]

It is clear that there are many different perspectives driving the Ethereum project forward.[56] One key goal, however, has been the facilitation of "transactions between consenting individuals who would otherwise have no means to trust one another".[57] This focus on trust, or lack of it, seems key, especially as it is embedded in the central architecture of the system. Indeed, it is the very justification for it if we accept blockchain as foundational. It has been stated that the lack of trust "may be due to geographical separation, interfacing difficulty, or perhaps the incompatibility, incompetence, unwillingness, expense or uncertainty, inconvenience or corruption of existing legal systems."[58] Irrespective of the reasons, bypassing the need for a more compromised, human trust is key.

It is therefore tempting to view Ethereum and systems like it as strongly rooted in the anarcho-crypto libertarian philosophy previously discussed, but it is also important to recognise how such decentralised systems are somewhat disconnected from these roots. The proponents of these systems and their concerns are less overtly political, for example (representative of the culture of the time, perhaps) and may be driven simply by a desire for more individual sovereignty in matters of agency. Removing the trust aspect simply improves agency. Therefore, trust as a fluid and flawed concept must go. In this way, those involved in Ethereum may not even be aware of the philosophical roots of the architecture involved. However, use of the system cannot avoid perpetuating the ideological basis of excessive individual sovereignty, abstraction of the body and a deep distrust towards centralised third party institutions, individuals and concepts. The conceptual element may appear contrived but note that the Ethereum project has always been upfront about impacting human interaction and concepts are key to this:

> […] around the 1990's it became clear that algorithmic enforcement of agreements could become a significant force in human cooperation. Though no specific system was proposed to implement such a system, it was proposed that the future of law would be heavily affected by such systems. In this light, Ethereum may be seen as a general implementation of such a crypto-law system.[59]

[55] G Wood, "Ethereum: A Secure Dencentralised Generalised Transaction Ledger" at 1 available at http://gavwood.com/Paper.pdf (accessed 8 Nov 16).

[56] Informal private discussions with individuals involved with Ethereum made it clear that for some, the major perspective was the decentralised aspect of the system, while for others it was the openness, or the cryptographic element or the attraction of the 'start-up' mode of being.

[57] G Wood, see note 55 above, at 1.

[58] *Ibid*.

[59] *Ibid*, 2.

Practically, Ethereum builds on the innovations of previous systems to offer a "blockchain with" – and this is another key innovation – "a Turing–complete language and an effectively unlimited inter-transaction storage capability."[60] The Turing completeness scripting language that Ethereum applies (solidity, a so-called "contract-orientated programming language") has the consequence of implementing a new entity on the back of the blockchain network.[61] That new entity is the smart or programmable contract. Such contracts become:

> […] like "autonomous agents" that live inside of the Ethereum execution environment, always executing a specific piece of code when "poked" by a message or transaction, and having direct control over their own ether balance and their own key/value store to keep track of persistent variables.[62]

Notably, Bitcoin was not Turing complete. It did not need to be as it only had one real purpose. Thus, instructions simply need to be communicated to such smart contacts[63]. Assuming that all actions are fuelled appropriately with the relevant currencies[64], they will be (in theory) enforced autonomously, encrypted, decentralised and will not require the involvement of a trusted third party to be fairly enforced. Importantly, it is admitted by the Ethereum project that "dealings in this proposed system would have several attributes not often found in the real world. The incorruptibility of judgment, often difficult to find, comes naturally from a disinterested algorithmic interpreter."[65] Transparency, another key goal of the project, "never happens perfectly in human based systems since natural language is necessarily vague, information is often lacking and plain old prejudices are difficult to shake." And yet interest and lack of absolute precision seem integral to the question and process of judgment as a human concept, emergent from the body.

As co-founder of Ethereum Gavin Wood stated, one of the overall objects of the project is:

> […] to provide a system such that users can be guaranteed that no matter with which other individuals, systems or organisations they interact, they can do so with absolute

[60] *Ibid*, 1.

[61] Turing completeness refers to the ability of a computer to compute every Turing computable function i.e. solve any computation problem (with no guarantees as to time involved of course – or how much memory would be needed).

[62] "White Paper", see note 40 above.

[63] Any transaction effected by Ethereum will be a single cryptographically-signed instruction sent by an actor external to Ethereum. As is stated in the Ethereum White Paper, "the external actor can be a person (via a mobile device or desktop computer) or could be from a piece of automated software running on a server."

[64] As noted previously, Ethereum utilises its intrinsic currency "Ether" as an agreed method for transmitting value in order to incentivise computation – computation itself fuelling the blockchain.

[65] Here we see mirrored some of the formalistic arrogance of computer scientists in the eighties when proposing true legal AI. A critique of that perspective in: P, Leith, *Formalism in A.I. and Computer Science* (Upper Saddle River: Ellis Horwood, 1990).

> confidence in the possible outcomes and how those outcomes might come about. [66]

The aspiration of absolute agency in all matters, in other words – which somehow seems more worrying that one may have ever thought.

11. Conclusion: The Dream of Sovereignty

Ethereum, and systems like it, offer the possibility of an alternative realm for the settling of many types of personal affairs, in what they suggest is a relatively apolitical platform. The private nature of these decentralised, encrypted systems is also attractive to a generation fuelled by events such as Snowden *et al* and thus to those who value privacy, at least online, to a greater degree than ever before. It is this apparent ability to have complete control over one's affairs and the dispensability of trusted third parties, that appears to be most attractive to this generation. Complete autonomy and sovereignty over one's affairs and how they are administered is now a common aspiration.

Why is such control so important, however? This question perhaps takes on a greater significance when it is asked in light of the broader context of the public versus private debate i.e. how best to organise human affairs. Decentralised, encrypted systems seem to fight corruption and government interference with a greater retreat into more privately, individually controlled and ordered worlds. In this there appears to be a great fear of public systems or private/quasi-private systems operating in a public orientated world. One could almost say that such systems represent fear of anything other than a type of utopia, which is an admirable goal. But existing is an exercise in compromising autonomy. Otherwise, as Russell points out, the reality of a common ethical space becomes dangerously compromised.[67] This desire for complete autonomy and sovereignty over one's affairs risks the eradication of the notion of the public interest. However, can we not instead have an approach that aspires to the creation of zones of "mutually agreed vulnerability", as suggested by legal theorist Roberto Unger in his seminal work *The Critical Legal Studies Movement*?[68]

Arguing for development within the context of established doctrine (but also for a reweighting of the principle/counter-principle balance), Unger discusses the often unreal and "stark contrast between contract and community" as presented and accepted in legal discourse and conceptualisations of law.[69] He writes: "The starting points of this contrast are a conception of community, as an idyllic haven of harmony, and contract, as a realm of unadulterated self-interest and pure calculation."[70] The result of such a recurring conceptual contrast, however, is acceptance and fostering of a "confusion of mutual loyalty with acquiescence in a regime of personalistic power while depriving the elements of trust and interdependence in business life of appropriate legal help."[71]

[66] G Wood, see note 55 above, at 1.

[67] B Russell, see note 33 above.

[68] R Unger, "The Critical Legal Studies Movement" (1982-1983) 96 *Harvard Law Review* 561.

[69] *Ibid*, 644.

[70] *Ibid*.

[71] R Unger, see note 68 above, at 644.

Unger considers it possible to correct these effects, beginning with "effacing the sharpness of the opposition between contract and community".[72] This process, he further argues, should end by suggesting:

> a view of contract that can more readily accommodate both a broad range of different sorts of rights or obligations and a conception of community as a zone of heightened mutual vulnerability, that gives a more satisfactory account of what attracts us to the communal ideal in the first place.[73]

Arguably, one can conceptualise recent events within the Ethereum community as a return to less sharp contrasts between contract and community. Previously, the contract, as code, was felt simply be an instrument of pure calculation and self-interest; and further, where previously the community was simply a haven of supposed harmony. As a result of the June 2016 DAO hack, this sharpness was necessarily effaced so that a zone of heightened mutual vulnerability came into existence.

As a result of the hack, the reputation of the Ethereum project was at risk, as well as the personal reputations of people involved with project; purchasers of Ether were also concerned. The community *qua* individual bodies thus understood its communal purpose by making a decision to resolve this incredibly vulnerable situation.

These decentralised systems therefore seem less like radical movements and more like zones (only) attempting 100% guaranteed safety, which does not bode well for social interaction or social life in general.[74] Even if the intentions are admirable, the very architectural roots of the blockchain on which Ethereum is built are ideological and have as their purpose the eradication of the value of a more compromised type of trust. By admiring and using such systems, we appear to be retreating via technology away from our bodies, away from vulnerability, away from common society and towards defensive citadels of anonymity and sovereignty. Building on the Ungerian argument, admiration for and use of such systems would appear to also be advancing the notion of contract and community as only strongly contrasting principles.

In theory, if not necessarily always in practice, the law (as understood as a critical social practice) is a good system for preventing such problematic developments. In this sense the law is of course another version of the utopia that is being sought, being composed itself of equally abstract notions of reality, goals, aspirations, and deviation from human behaviour to something slightly more reified than that. The law can be viewed here as another type of programming language, providing another perspective on the infamous "code is law" comment of Lawrence Lessig.[75] Code may be becoming (and may already be) law, but law was and is already a type of code.

But the law is not simply – perhaps disappointingly so – a Rawlsian notion of justice, even if it is a type of code. Rawls asks us to imagine ourselves without a particular

[72] *Ibid.*

[73] *Ibid.*

[74] Symbolic of this danger is the enthusiasm seen in the financial and legal worlds for blockchain-based systems..

[75] L Lessig, *Code and other Laws of Cyberspace* (Basic Books, 1999).

body, just yet, so that the rules of existence could be fairly decided.[76] An abjection of the idea of our own body, a casting off of it to decide what is just. Rawls conceptualised an "original position of equality", a "hypothetical situation characterized so as to lead to a certain conception of justice."[77] The key feature of this original position being that "no one knows his place in society, his class or social status, nor does anyone know his fortune in the distribution of natural assets and abilities, his intelligence, strength and the like."[78] Thus the principles of justice are to be chosen behind the infamous veil of ignorance.

There is something similar in the notion of autonomous contracts existing in the blockchain to the Rawlsian approach to conceptualising justice; smart contracts as dispassionate executors of intentions and contractual clarity, completely encrypted. But, in matters of justice, it is not the body that we are in, or the imagining of others' bodies we might be in/have been in instead, that is the problem with law or justice. Law as it occurs is imperfect and one that deals with our bodies *as they are* and, more importantly how they are around other bodies that are as they are. It is therefore living in the body that we in fact have, the body given, and *amongst other bodies*, that is the problem in matters of justice. Laws are then interpreted, as a type of guiding code, but still interpreted and enforced by human beings, this way or that, to enforce a sacred zone over the body existing, once we are embedded in it. Laws are used against the body to protect it or accuse it, as appropriate, because it, the body, has impinged itself upon another without welcome or is being impinged upon. How does law combat this need for a sacred zone, after the fact of our corporeality? If it is not doing this, can it really be said to be law at all?

Decentralised systems such as Ethereum suggest a mode based on the Rawlsian ideal, an abjection of the body. But the central problem still emerges: what principles are to be relied upon when difficulties emerge in the ethics and/or aesthetics of our existence as it is? Some suggest code can dispassionately avoid such problems, and perhaps it can. But what does that bode for our expectations concerning justice in matters where code cannot operate well? Trust is the fuel and result of human interaction especially in legal affairs and human systems. With Ethereum it is the system that is the trusted object and only because of that are the actors emerging from the veil of the system, trusted in their own way.

The situation with the DAO hack illustrates all this difficulty perfectly. One can theorise how smart contracts will give effect to the intentions of people without the need for identification and or presence of their body (the Rawlsian notion of justice in transactional matters, for example). But justice is in fact always heavily compromised by the actions and or omissions of the bodies we are in. Thus, the motivations of the hacker who decided to hack the DAO. And thus, the operation of justice subsequent to that hack: a flawed solution, not ideal, but agreed by the human participants in light of the circumstances. This is a form of real legal activity.

Law is thus perhaps more preferable as a system for continual development within (regardless of its centralising force; regardless of the lack of complete trust possible) *because* of its dependence and reliance on the body as the main device for the

[76] J Rawls, *A Theory of Justice* (Oxford: OUP, 1999).

[77] *Ibid*, 11-22.

[78] *Ibid*.

exercise of such activity. This reflects the Ungerian approach of the deviationist doctrine. As an illustration of this, consider complex legal thinking perhaps as the only practice that one would not want exercised by a machine, even with all advances in technology. It is precisely the human element of law that one accused of a crime or injustice would be hoping to appeal to. It is also precisely this human element that was resorted to when technology failed the participants of the DAO.

But, the question remains: why so fearful? Is centralisation and the trusted party concept so bad? Slavoj Žižek argues that in emancipatory movements – which Ethereum seems somewhat connected to, at least in terms attempting to develop a stronger sense of individual emancipation – there is an importance in grounding one's individual emancipatory knowledge within a collective form. Making a historical parallel with the notion of the "Party", he writes that "protest movements prove inadequate the moment one has to act, to impose a new order – at this point something like a Party is needed." [79] He adds that, for the individual who believes he or she is right in opposition to the status quo, what is important is that he or she "should fight for [that] position within the collective form of the Party, not outside it."[80]

There are admirable elements to Ethereum but what is problematic is that it encourages a retreat into an environment where trust – conceptualised here as perhaps an Ungerian zone of mutual vulnerability – is not felt to be necessary. This can only act to de-collectivise human interaction to a degree so that whatever freedom or increased agency occurs is only individually and perhaps subjectively realised. Quite clearly there are issues with the way in which societal interaction often occurs. In countries, for example, where legal systems and other centralised services are not trusted, systems such as Ethereum could be useful in counteracting those weaknesses. It may well be that all such social systems cannot be trusted at all. But it would still be more important, perhaps in the long term, to develop trust or re-establish it as a social practice and not outsource it to esoteric and impersonal code. Once embedded there it will be hard, if not impossible, to recall it into the public space of society, amongst bodies and weak temperaments.

In addition, a retreat into autonomous, anti-bodied individual zones of sovereignty is not the only option as solution against difficulties of human interaction. A far more radical suggestion is following the Ungerian notion of the deviationist doctrine to the end and suggesting a change in the *dispositif* underlying how we regulate our affairs.[81] The *dispositif* currently seems to be of law as merely functional and instrumental and therefore to be destroyed and or feared. But that *dispositif* – how we allow ourselves to be governed – can be changed in line with what Unger and Žižek suggest so that less a crypto-law and more a truly human law, dealing with us in the bodies we are in, can emerge. As Žižek writes:

> the task of emancipatory politics lies…not in elaborating a proliferation of strategies for how to resist the predominant

[79] S Žižek, *Less Than Nothing: Hegel And The Shadow Of Dialectical Materialism* (New York: Verso, 2013), at 1000.

[80] *Ibid*.

[81] *Dispositif* is used here with the meaning ascribed to it by Giorgio Agamben:"that in and through which a pure activity of governing without any foundation in being realises itself." G Agamben, *Qu'est-ce qu'un dispositif?* (Paris: Payot & Rivages, 2007) at 26-27.

> dispositif from marginal subjective positions but in thinking about the modalities of a possible radical rupture in the predominant dispositif itself.[82]

What would this new *dispositif* be? In the context of systems such as Ethereum it might be that flawed trust could be a useful and even necessary concept.

Perhaps a more radical thought might be that the *dispositif* here is our outdated notion of trust and interaction. Perhaps the decentralised future imagined by systems such as Ethereum will indeed open up a world where we can be free from boring work and where code works for us. All this technological development also fits in with work such as that outlined in *Inventing The Future*, where technology is given a dominant role in eradicating the need for work.[83] Consider Žižek's conceptualisation of the most perfect romantic encounter, wherein technology, the toys of sex, do all the work leaving the couple to simply enjoy properly intimate moments.[84] Perhaps we *should* be encouraged to autonomise Ethereum smart contracts and remove ourselves as much as possible from the gritty work of negotiating with others on transactional matters.

Unfortunately, decentralised system such as Ethereum are not as sovereign and abstract as their proponents imagine. While the almost impregnable status of the blockchain is well known (in theory it would require control of more than half the computers in the chain to compromise it), tactics have been identified that might "allow a sneaky and well financed miner to compromise the block chain without direct control of 51% of it."[85] In addition:

> getting control of an appreciable fraction of the network's resources looks less unlikely than it used to. Once the purview of hobbyists, bitcoin mining is now dominated by large "pools", in which small miners share their efforts and rewards, and the operators of big data centres, many based in areas of China, such as Inner Mongolia, where electricity is cheap.[86]

Human desires, the result of the bodies we are in, and the other bodies that surround us, are not so easily eradicated. The recent DAO hack illustrated this. A form of law, where intentions or promises can never really be guaranteed in any event, is still required to usefully address *ex post* what our bodies want to do. This is a form of law as action emerging from the body, and not one that attempts to retreat from it, and from the consequence of the bodies of others.

[82] S Žižek, see note 79 above, at 994.

[83] N Srnicek and A Williams, *Inventing The Future: Post Capitalism & A World Without Work* (London: Verso, 2015). See also: DJ Pangburn, "The Humans Who Dream Of Companies That Won't Need Us" available at http://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them (accessed 8 Nov 16).

[84] S Žižek, "Slavoj Žižek on Synthetic Sex and 'Being Yourself'" (2015) available at http://bigthink.com/videos/online-dating-and-synthetic-sex (accessed 8 Nov 16).

[85] "Blockchains", see note 42 above.

[86] *Ibid*.

The development of projects such as Ethereum – and even the use of blockchain technology in a more traditional fashion, such as part of the legal services offered by law firms – seems therefore more in line with a globalised race towards abstracted efficiency, where the market determines all. Human involvement, conversely, adds an element of choice to such matters, the choice to develop and add to or express various ideologies in how we interact. Technology, while useful, aims for abstraction and efficiency only, and seems to be a slightly less flexible – and much more (or at least equally) dangerous – reality.