Blockchain Technology as an Institution of Property

Ishmaev, G.

DOI
10.1111/meta.12277

Publication date
2017

Document Version
Final published version

Published in
Metaphilosophy

METAPHILOSOPHY

METAPHILOSOPHY
Vol. 48, No. 5, October 2017
0026-1068

BLOCKCHAIN TECHNOLOGY AS AN INSTITUTION OF PROPERTY

G. ISHMAEV

Abstract: This paper argues that the practical implementation of blockchain technology can be considered an institution of property similar to legal institutions. Invoking Penner's theory of property and Hegel's system of property rights, and using the example of bitcoin, it is possible to demonstrate that blockchain effectively implements all necessary and sufficient criteria for property without reliance on legal means. Blockchains eliminate the need for a third-party authority to enforce exclusion rights, and provide a system of universal access to knowledge and discoverability about the property rights of all participants and how the system functions. The implications of these findings are that traditional property relations in society could be replaced by or supplemented with blockchain models, and implemented in new domains.

Keywords: blockchain, bitcoin, property, rights, institutions.

1. Introduction

Blockchain technology conceived and implemented in the form of digital currencies such as bitcoin has from its very beginning been a puzzling development for regulatory bodies and legislators. Being essentially an alternative to fiat currencies, bitcoin gave rise to new markets and financial instruments functioning largely beyond the scope of legal frameworks. This became possible thanks to the decentralized nature of blockchain technology, enabling the creation of currencies independently of any central regulator (Vardi 2016). Initial reaction to the propagation of bitcoin from legal scholars and legislators was a question of if and how bitcoin should be regulated (Shcherbak 2014; De Filippi 2014; Tu and Meredith 2015). The push to address this issue was stimulated by the apprehensions (mostly justified) that bitcoin might contribute to the growth of contraband markets and tax-evasion schemes (Hendrickson, Hogan, and Luther 2014).

At the time of this writing (September 2017), efforts to implement these regulations have been largely unsuccessful, as so-called dark markets demonstrate a certain resilience (Kruithof et al. 2016; Dittus 2017), and consistent policy on the taxation of cryptocurrencies does

not seem feasible (Campbell 2016), which is even more likely to be the case in the future, due to the pseudonymous (bitcoin) or anonymous (monero, zcash) nature of these financial instruments. The only meaningful regulation now in practice concerns exchanges that offer cryptocurrency-fiat trade pairs, which fall within the scope of money-laundering laws and regulations. At the same time, alternative services facilitating bitcoin-to-fiat trades, such as "localbitcoins," largely operate beyond legal regulations (Melendez 2016).

The most interesting feature of bitcoin and other cryptocurrencies, however, is not just resilience to regulation enforcement but also successful functioning outside any meaningful legal frameworks, even in the light of numerous financial crashes, such as the bankruptcy of the Mt. Gox exchange, responsible for about 70 percent of bitcoin exchange transactions, amounting to losses of $470 million for its clients (McMillan 2014). Mt. Gox being the biggest case is not an isolated incident, as similar hacks have taken place, most recently of Bitfinex in August 2016, resulting in losses of roughly $70 million (Reuters 2016). Interestingly, Bitfinex compliance with legal regulations was named as the reason for this security breach; in order to comply with the U.S. Commodity Futures Trading Commission requirements of June 2016 (CFTC), Bitfinex kept customer funds in a form accessible online (a "hot wallet") rather than in more secure offline storage (a "cold wallet"). These examples make it possible to say that not only is the bitcoin economy functioning in the absence of meaningful regulations, sometimes it does so even in spite of regulations.

Cryptocurrencies are a flagship example of blockchain implementations but present only one possible application of this technology. Another application of blockchain is so-called smart contracts, which gained traction only recently (at least in terms of investment attraction). The idea behind smart contracts is the extension of bitcoin code beyond simple monetary transactions to more complex operations that can be carried out within a similar decentralized network (Buterin 2014). This, for instance, can mean that if two parties engage in a contractual agreement using a smart-contract application, performance of contractual terms is guaranteed not by the goodwill of parties or third-party arbitrage but rather by the encoded algorithm. The scope of smart-contract applications is wide-ranging, from simple contractual agreements to self-governing organizations. Self-governance here essentially means that such organizations can function without external regulation, purely on the basis of encoded algorithms executed on a decentralized network and fuelled by cryptocurrencies.

The promise of such powerful and complex systems has prompted the expression "code is the law," conveying the assumption that legal frameworks in many instances can be successfully replaced by computer code (Swan 2015, 16). The first large and ambitious enterprise of

this kind, the Decentralized Autonomous Organization (DAO), which aimed to create a self-governing organization on the basis of Ethereum smart contracts, created by the motto "code is the law," did not live up to expectations, in both financial and ideological senses. Conceived and advertised as an innovative self-governing investment fund, DAO attracted more than $150 million in crowdfunding, only to fall victim to hacking, leading to termination of the project (Greenspan 2016).

To amend the fallout from the hack and return stolen funds, the Ethereum foundation, the developer of the blockchain on which DAO was based, made a decision to change the protocol (implement a hard-fork), effectively annulling all transactions on the Ethereum blockchain past a certain date (Hertig 2016). This decision caused split opinions, with critics saying that such a decision violated the principles of self-governance. This somewhat ideological split lead to the creation of an alternative blockchain called Ethereum Classic, based on a protocol prior to the DAO hack.[1] And again, as in the case of the Mt. Gox hack, the failure of DAO hardly curbed or slowed down development of other smart-contract applications, such as Expanse, Counterparty, and Lisk, along with two Ethereum blockchains and possibly many others.

The idea that computer code implemented on the decentralized blockchain can replace legal institutions seems captivating not only to developers and investors but also to some academic researchers. Swan (2015) points out that many systems of governance, such as property registry, provision of identification documents, and even registration of marriages, can be replaced by the decentralized blockchain services. Fairfield (2014) suggests that blockchain technology has the potential to disrupt and reshape existing legal norms regarding digital property rights. He argues that the law of intellectual property does a poor job safeguarding intangible digital property rights, and suggests a replacement in the form of a new law of information property that can also provide governance for distributed ledgers. He thus does not suggest a replacement of legal structures but rather suggests a hybrid solution of "bitproperty."

Wright and De Filippi (2015) comprehensively review existing and prospective blockchain technology implementations and come up with a prognosis that legal frameworks in the future might be radically transformed by the rise of cryptocurrencies, smart contracts, and self-governed organizations. They suggest that a new type of techno-legal framework, "lex cryptographia," should be recognized and accommodated by existing legal institutions, in the form of a new body of law. Wright and De Filippi argue that implementation of complex systems

[1] Although from the technical point of view "creation" is an incorrect term, since Ethereum Classic is simply an existing blockchain, and "forked version" would strictly speaking be a new one.

of smart contracts and decentralized organizations may rewrite the basic tenets of property rights, constitutional rights, and even judicial enforcement of law.

Each of these claims deserves special consideration, but one of the most radical claims is that in the future property rights may vanish, becoming a subset of contract law. This can happen when physical devices, such as cars, locks, guns, and anything else with internet connectivity (smart devices), will be managed on the basis of blockchain technology, in the form of leasing, renting, and so on. Wright and De Filippi highlight this possibility along with other developments, but I shall argue that this claim is in fact the most crucial point of argumentation on the nature of contradictions between existing legal institutions and blockchain technology.

Arguments on the nature of property and property rights are central to many issues on the nature of individual rights and government power to interfere with individual freedom, highlighting the number of descriptive and normative questions. This centrality of the property issue can be traced back to Aristotle's *Politics* (1958), where he discusses the necessity and limits of property for a good life (1257b) and justice in the polis regarding distribution of property (1266b). Arguments on the nature of property were central for such thinkers as Locke (1993), who argued that the very idea of government is justified by the institution of property. One does not, however, have to subscribe to Aristotelian or Lockean views on the nature of society and the state in order to suggest that the question of the nature of property precedes other considerations of the wider impact of blockchain technology on the shape and role of normative social structures.

Looking at the historical timeline of blockchain technology development, it is possible to say that the core idea behind it was an attempt to develop cryptographic certificates in the form of an immutable public ledger (Haber and Stornetta 1990), which later was developed to function as a ledger of monetary transactions and the bitcoin protocol (Nakomoto 2008), effectively implementing the idea of basic monetary property. Granted, Szabo (1997) theorised the possibility of smart contracts and smart property earlier, but practical implementation of blockchain started as digital currency first, followed by smart contracts, which in turn made possible blockchain-enabled management of physical smart property (Naraynan et al. 2016).

Bitcoin is not only the first successful application but genealogically also the most basic successful implementation of blockchain technology focused on delivering functionality limited to monetary transactions. In technical terms, this means that the scripting language used in the bitcoin protocol is not Turing complete, basically having intentionally limited functionality, while the protocols used for smart contracts are

essentially extensions of currency protocols with added functionality (Buterin 2014). Thus from the technical perspective as well, it might be fruitful to focus first on the most basic function of blockchain technology (monetary property) to assess its potential impact on the legal frameworks and other normative structures in society. It is also reasonable to engage first in a descriptive analysis of blockchain technology to see what functions it might have in the social context, before we move on the normative assessment of its role.

As an illustrative case bitcoin and other cryptocurrencies present a flagship example of new normative structures of property that can function independently of legal institutions. The ground-breaking novelty of this approach to monetary transactions was suggested in the first paper by the pseudonymous author Satoshi Nakomoto (2008), who proposed a mechanism that essentially replaces third-party authority with the decentralized ledger. In practice it means that the copies of the ledger containing information about monetary transactions are held on different computers on the peer-to-peer network. In itself, a decentralized network holding information on monetary transactions is nothing new; the uniqueness here is in the fact that all functions traditionally executed by third parties, such as currency issuance, authorization of account holders, and so forth, are built in the network protocol. In that sense the bitcoin network is indeed a complete institution of monetary property functioning alongside traditional institutions.

To understand the scale of such a claim, it is necessary to clarify the concept "institution" itself, since it can refer to a number of social phenomena. In the most general sense institutions can be defined as normative entities, as kinds of social structures embodied by human agents, governed by rules, conventions, and predefined ends. Miller (2001) points out that institutions can take different forms, such as organizations, systems of organizations, or even systems without organizations, like language, depending upon the scale of the institution and its purpose. I argue that the true novelty of the blockchain technology lies in the capacity not just to create new types of property but also to create social institutions that can be either complementary or competitive with regard to existing institutions.

Bitcoin protocol as an instance of blockchain technology provides an example of such an institution: namely, an institution of property on a transnational scale. In that sense it can be characterized as a meta-institution, a system governing relations between individuals, organizations, and other institutions. In that capacity it may not only reshape or enhance existing legal institutions of digital property, as suggested by Fairfiled (2015), but rather meet all criteria of a parallel normative structure. Furthermore, rights and duties constituted by such an institution of property can operate in a different modality compared to

legal rights and duties, thus providing a qualitatively new system of property relations.

2. Normative and Descriptive Theories of Property

What can be drawn from the conceptual scheme of the bitcoin protocol, at first glance, is a peculiar analogy between the chronological structure of the bitcoin ledger and both the property theory of first occupancy and Locke's labour justification for property rights. The very first record in the bitcoin ledger, called the "genesis block," is essentially a starting point from which all the ensuing transactions take their legitimacy. This conceptual scheme is reminiscent in particular of the idea that all property rights can be traced back to the very first property owner (Pufendorf 1993 [1653]). In the other sense there is also a reminder of the Lockean (1993) argument that property rights are granted first to those who mix their labour with raw material. With some stretch of the imagination it is also possible to say that bitcoin miners consuming electricity and applying computer power gain some new property titles, effectively justifying their property rights over newly issued coins. In all fairness, though, these observations, entertaining as they may be, hardly provide any insights into the philosophical aspects of blockchain technology.

The most helpful observation that can be taken from this analogy is that the system of property rights in bitcoin has a bottom-up normative justification, similar to the theories of Pufendorf and Locke. Such justification stands in contrast to top-down approaches to property, such as Hume's, where the state grants its citizens property rights purely in virtue of its authority, and thus the very institution of property is seen as deriving from the power of the state (Waldron 2013). This, however, does not constitute a qualitatively new observation, since early in the history of its development bitcoin was largely seen as a libertarian enterprise, aiming to promote the ideals of free markets and individual freedom (Karlstrom 2014). Thus it might be helpful to take a look at theories of property providing more substantial analysis on the necessary and sufficient criteria of property.

Despite being a straightforward idea in everyday life, in academic research the concept of property is anything but simple. This is hardly surprising, taking into consideration the interdisciplinary nature of the concept of property, but conceptual disparity also persists within the field of legal philosophy (Merrill and Smith 2001). Waldron (1990), looking at the possibility of a general idea of property, suggested a broad definition of property as the concept of rules governing access to and control of material resources. Waldron, focusing on the issues of moral justification of property, does not, however, look deeper into the

definition of property in its most abstract sense, arguing that locating the family resemblance of concepts is sufficient for his goals.

The same can be said about other theories focusing on the normative aspects of property institutions. Nozick (1974), in the vein of a Lockean approach to property, defines property rights as the right of an owner to determine what should be done with property X, as bilateral permission between individuals concerning the use of things. Arguably this definition does not provide us with a sufficient and necessary set of criteria that can be applied to determine whether X is property or not. Penner (1997), analysing Waldron's definition of property, suggests that subtle evasions of thinking about why some things are objects of property and others are not are in fact quite common for many normative philosophical treatises on property. Thus if one has to address the question whether blockchain technology applications fall into the category of property, it might be helpful to focus first on descriptive theories of property.

Broadly speaking, two main descriptive approaches to the theory of property stemming from different motivations can be found in the contemporary philosophy of property. On the one hand there is a bundle theory of property suggested by some legal scholars who aim to address the issue of how property should be conceptualized within the legal framework, and on the other there is an essentialist approach that aims to address the more abstract issue of the philosophical definition of property. Munzer (1990), one of the most prominent theorists of the bundle approach, distinguishes between a popular, simple conception of property as things and a sophisticated conception of property as relations of persons to things, defining the legal understanding of property. The idea of property according to Munzer involves a catalogue of tangible or intangible things and a catalogue of various relations that the owner has with regard to such things as claim rights, liberties, duties, and liabilities and other basic legal concepts borrowed from the legal works of Hohfeld (1917) and Honore (1961). These relations as "sticks" constitute a bundle that is called a property, hence the name of the bundle approach.

Penner (1997) suggests an alternative approach to the conceptualization of property, aiming to distinguish an essential characteristic of property, which he derives from the core right to exclude. In the broad conceptual sense, property according to Penner can be considered a system of moral standards institutionalized in the legal system. Both Penner and Munzer trace the legal theory of property back to Hohfeld-Honore legal vocabulary, drawing from Honore's distinction between norms *in personam* and norms *in rem*. Norms *in personam* capture the rights of behaviour of some particular person, thus binding specific individuals, as in contractual obligations. Norms *in rem* on the other hand bind "all the world," that is, all subjects of a legal system,

such as preventing all except the landowner A from trespassing on land. In Penner's interpretation the norm *in rem* is a rule that applies to owners of property simply by virtue of their ownership. Furthermore, everyone's relation to A (in regard to property) is *through* A's property, when the identity of A is irrelevant to the imposition of negative duties on non-owners, as opposed to norms *in personam*. This approach is also sometimes characterised as an exclusion theory of property (Merrill and Smith 2001), as it captures the essential idea of property as the right to exclude non-owners from the use of resources.

It may be argued that both the bundle and the essentialist approaches can be helpful to clarify the role and impact of blockchain technology on social norms and legal institutions. The bundle approach as argued by Munzer (2013) aims to grasp a variety of rights beyond exclusion, such as rights to use and alienate, but also the liabilities of property owners, thus better understanding the complexities of legal property systems, unlike the essentialist exclusion approach. Furthermore, argues Munzer, it is difficult to derive the complexity of these rights from a single exclusion right, as suggested by Penner. Application of bundle theory in this respect may be an interesting attempt to see whether property rights might be reduced to contractual obligations with the implementation of blockchain technology, as Wright and De Filippi (2015) suggest. This step, however, would first require an analysis of the blockchain as a form of property, and this entails a more abstract conceptualization of property above a practical understanding of the legal system. Whether one or another approach is better at grasping the complexities of legal systems is arguably not relevant to the scope of the current paper; however, the preceding discussion suggests that the application of Penner's essentialist theory of property might be a preferable preliminary step for the analysis of blockchain technology, for two reasons.

First, any attempt to grasp a new normative structure (blockchain) within the conceptual framework of an old normative structure (law) may fail to highlight some significant qualitatively new aspects. Indeed, if we want to examine Wright and De Filippi's claims that legal property rights can be replaced by "technological ownership," it might be helpful to move up from the legal level of abstraction and look at the philosophical conceptions of property, in order to avoid dead-end metaphorical reasoning. As Van Hoecke (2011) argues, legal research has rather narrow explanatory power, as the explanation taking place is largely an internal enterprise when nothing is "explained" in an analytic sense, but instead values or principles are postulated, or some interpretation of a higher rule is posited, in order to legitimate them. The same critique can be applied to Fairfield's (2014) theory of bit-property, which highlights some novel epistemic aspects of a public

ledger but largely sees blockchain technology as a mean to reinforce the existing legal frameworks of digital property rights.

The second argument stems from the technical analysis of blockchain technology, which is built on the cryptographic primitives. The very basic primitive aspect of blockchain (and cryptocurrencies) is the digital signature, essentially a message encryption method that excludes everybody except the owner of a private key from modifying the content of a message (Nakamoto 2008). In a general sense all the added functionality is built on top of this principle in the logic of blockchain. And as in Penner's approach, the actual identity of a bitcoin owner is irrelevant, so long as the digital signature serving as a proof of ownership is valid. However, before we can apply Penner's theory of property to the blockchain, we need to take a brief look at the basic concepts and principles of blockchain technology illustrated through the bitcoin blockchain.

3. A Short Technical Explanation of Blockchain

Bitcoin is a good example of the practical implementation of blockchain technology, being the most successful basic application of it, and the most researched. At its core are basic principles called cryptographic primitives, which can be considered the conceptual building blocks of the blockchain function. Two such principles are the "hash function" and the "digital signature," which are among the basic technical elements that need to be explained for a proper understanding of bitcoin technology (Nakomoto 2008; Koblitz and Menezes 2016).

The first cryptographic primitive hash function is essentially a mathematical function of the data input of any size that produces an output of limited size that can be efficiently computable (in a reasonable amount of time). The hash function has several important properties (Paar and Pelzl 2009), of which the following three are particularly useful for the implementations of cryptocurrencies like bitcoin. First, the hash function is collision resistant, which means that two distinct inputs do not produce the same output.[2] In practice this means that the hash function can be used as a message digest, a tool to verify that a copy of a message is identical to the original. The second property is hiding, which means that given only the output no one can infer the value of the input. This property translates into the application of a binding commitment, similar to putting a message into an envelope and committing to its content without revealing it. Once the message is put into the envelope, I cannot change my mind and alter its content.

[2] This does not mean that two distinctive inputs producing a single output do not exist; rather, we believe that finding such a collision is not possible in practice, and the hash function is good enough.

The third property is puzzle friendliness, meaning that the hash function can be presented in the form of a mathematical puzzle, where we try different inputs for a given hash function to get an output with a predetermined value.

The first and second properties of hash functions are employed to build complex data structures using simple data structures—hash pointers as building blocks. Puzzle friendliness is not a necessary requirement for a data structure itself, but it is necessary for cryptocurrency. A pointer in computer science in general and in data structures in particular is essentially a reference pointing out where information is stored, similar to the code in a library catalogue. The hash pointer in turn is a reference complemented with the short digest of the information it refers to, helpful for verification. Using hash pointers, it is possible to build a data structure in the form of a blockchain, giving the name to the technology itself (Narayanan et al. 2016).

Real blockchain structures implemented in the bitcoin protocol are more complex than this scheme, but for the purposes of this paper the given scheme can be considered sufficient.[3] It gives a general idea of a so-called public ledger, a tamper-evident (sometimes called immutable) data structure that may exist in the number of copies, and there is a reasonable (from the computational perspective) method of verifying that all copies and their respective elements are identical. The concept of a ledger is crucial for the general understanding of bitcoin functioning.

The second cryptographic primitive used in the logic of blockchain architecture is a digital signature. As indicated by the name, it is functionally a cryptographic method of signing a message digitally. In order to do so, the digital signature method uses asymmetric/two-key encryption. To draw an analogy, two-key encryption is essentially a lock with a pair of keys, of which one only opens and the other only locks. Now in digital form the opening key can be made public, while the locking key is kept private. Thus if someone encrypts a message with a private key and provides the resulting output "signature" together with a copy of the original message, anybody with a public key can decrypt the signature to verify that the message was indeed signed by the private key holder (Paar and Pelzl 2009; Hoffstein et al. 2008). Because there might be only one private key, which only one person knows, this signature method provides a verifiable identity. Using a key pair and hash function it is possible to generate bitcoin "addresses," which are essentially hashes of the public part of the key pair.

The combination of these two rather simple cryptographic methods allows for the essential construction of digital currency or cryptocurrency.

[3] Comprehensive study of the bitcoin architecture can be found in the excellent handbook *Bitcoin and Cryptocurrency Technologies* by Narayanan et al. (2016).

To illustrate in a simplified way how this tool can be used for digital monetary transactions, let's consider a monetary transaction between Alice and Bob. First, Alice, using a generated key pair, can create a digital message saying that she owns ten coins and can sign it with a private key. Next, in order to make a transaction to Bob she adds another message to the existing one, which says that she is sending ten coins to him, using his public key as a name for the transaction recipient. This, however, hardly counts as money yet, since all this rests merely on the convention between Alice and Bob, who agree to treat it as a transaction. What is necessary here is a guarantee of some sort that this digital cheque signed by Alice will be good once Bob wants to give it to somebody else (Koblitz and Menezes 2016).

In a traditional monetary system, the guarantor of cheque validity is a third party—a bank holding a record of all transactions and guaranteeing their validity, essentially co-signing Alice's cheque. The crucial function of the bank is to prevent double spending, that is, to prevent Alice from giving a copy of the same cheque to multiple people. To ensure this, the bank holds a record that, first of all, Alice has only ten coins and that she gave these coins to Bob. The bank (if it is a central bank) also acts as an issuer of new money; this means that Alice cannot write a message "Alice has ten bitcoins" out of nowhere but has to write it above the verified message "The bank gave Alice ten coins." This is in fact rather similar to how online banking works, as the bank computer holds records of all transaction. Of course in reality Alice might use other types of verification and the bank might have multiple servers holding copies of the ledger, but the principle of a single authority holds.

Bitcoin replaces third-party authority with the distributed ledger built on the blockchain. The novelty of this approach to monetary systems is that in practice the ledger holding information about monetary transactions is on different computers on the peer-to-peer network. The blockchain data structure guarantees that all these copies are identical across that network, and the validity of any new transaction has to be guaranteed by the multiple nodes (computers running bitcoin client software) on the network. A ledger holding the records of all transactions that ever took place guarantees that Alice indeed has the money she wants to send. The validity of the new transaction is verified not only on the basis of previous records about Alice's money but also by her signing with her private key (Narayanan et al. 2016). This is a very simplistic depiction of how new transactions are accepted on the ledger, but it sketches the general conceptual framework of bitcoin.

Another ingenious aspect of bitcoin is the mechanism for the issuance of new coins, which is tied to the process of how new transactions get recorded in the ledger. This can be explained through the puzzle friendliness of the hash function. Bitcoin protocol requires that all

records on new transactions have to be combined in data blocks of fixed sizes and properties, such as that the hash of a particular block has some predefined values. The search for such output crudely speaking is a puzzle, of how to achieve this output by using existing inputs (transaction data). Some nodes of the bitcoin network may try to solve this puzzle by trying different solutions to achieve the desired output, and may propose this block for the whole network to be accepted as the newest record on the ledger. The node that succeeds in first solving the puzzle gets a reward of fixed size according to the rules of the protocol, essentially creating new coins. The size of a reward is a value decreasing in time while the difficulty of puzzles is increasing progressively, thus by design the supply of bitcoins is limited, and the issuance of new coins will eventually stop. Some other technical aspects outside the scope of the current paper present interesting points of philosophical and ethical enquiry, such as fairness of mining capacity distribution, whether the bitcoin network can truly be decentralized,[4] and whether identity based on digital signature is truly anonymous.[5] However, this short schematic illustration of bitcoin mechanics is sufficient to say whether the blockchain protocol can provide the function of property institutions.

4. Applying the Theory of Property to the Blockchain

Realisation of the idea of property, according to Penner (1997), is a legal structure of property laws serving as the individuation of duties, powers, rights, and permissions relating to fundamental interests or interactions of fundamental interests. While Penner does not elaborate on the underlying theory of interests, it is possible to say that by interest he means a function of a legal right to further the right holder's interests. Thus, in order to grasp the idea of property one has to understand the interest behind property ownership to highlight its conceptual essence. Such interest, argues Penner, is the interest in exclusively determining the use of things. Following from this the essence of property is exclusion of non-owners from the determination of property use.

[4] In theory, concentration of 51 percent of hashrate power in the hands of a single agent can allow him or her to control which blocks are accepted first, creating the possibility of double spending. Though in practice this scenario is largely considered economically unviable, since such an agent would have to bear significant costs accumulating hashrate power, which would not be covered by such a double-spend attack.

[5] Bitcoin users can in fact be de-anonymized at the moment, but this can be seen as temporary state of affairs, since greater obfuscation of user identity can be built on top of the bitcoin protocol. Significant research efforts in this area also bring new cryptocurrency protocols, providing greater anonymity, such as monero (https://getmonero.org/) and zerocash (https://z.cash/).

Penner also highlights that it is a negative liberty that serves only to the extent that freedom from the interference of others does.

This essential idea of property allows Penner to derive the answer to the question of what "things" are property—sufficient and necessary criteria. The first criterion for property is characterized by Penner as an exclusion, a thesis that states that the right to property is a right to exclude others from things that is grounded in the interest we have in the use of things. Here use and exclusion are two sides of the same coin, as on the one hand exclusion is not a goal unto itself but rather reflects an owner's purposeful dealing with things and on the other permits an owner to exclude non-owners from the use of these things. Accordingly, property rights, in Penner's view, are *in rem* rights, creating negative duties for all non-owners even if they have no contractual relations with the property holder.

The application of this criterion to the concept of coin ownership on the bitcoin blockchain is rather straightforward. Indeed, the core idea behind basic cryptographic tools is to exclude non-authorized individuals from the use of encrypted data, be it a message, database, or bitcoin wallet. A significant distinction here is in the modality of property rights. While a legal framework creates a duty for non-owners not to interfere in the sense of permissibility (Penner 1997; Ripstein 2013), property rights implemented in the blockchain protocol operate in the sense of possibility. Two-key asymmetric encryption used in bitcoin digital signatures essentially guarantees a right to the holder of the private key to exclude others from using coins. Exclusive use here means that the owner of bitcoins can have sole right to dispose of them, transfer them using the blockchain, sell them for other currency, or give them away as a paper wallet (with the key pair printed on the physical media).

This corresponds to the analysis by Penner of the mechanistic aspect of the social use of property, which he compares to a gate rather than a wall. He also notes that the right to exclude others in real legal practice is not necessarily full liberal ownership: that is, it is not absolute and can be overridden by legitimate state power. This observation highlights an interesting aspect here, since cryptographic ownership is certainly much closer to this ideal liberal ownership than any legal ownership, as modalities of permissibility and possibility rights conflate on the blockchain. Of course, precedents of confiscating bitcoins from infamous Silkroad dark-market owners by the U.S. government show that having bitcoins in practice does not necessarily constitute absolute ownership (Kharif 2014). It is necessary to point out, however, that this example is rather a case of security breach; in theory bitcoin owners who keep their real-life identity separate from their bitcoin addresses kept offline can enjoy pretty much absolute ownership (insofar as necessary infrastructure exists).

The second key criterion for property Penner calls the "separability thesis": that is, ownership of things that count as property is contingent or conditional. Ownership of property does not presuppose any special immutable relationship with it, unlike, say, ownership of a talent. This, argues Penner, makes property rights transferable, because when property rights are transferred from one person to another this does not alter the nature of the property and the duty of all other non-owners to remain excluded from it. Indeed, one can exclude others from enjoying one's singing talent, but that hardly means that the given talent itself is one's property. Thus separability in Penner's view constitutes a necessary criterion supplemental to the exclusion thesis. "Thing" here is a conceptual criterion that restricts the application of property rights to those things in the world that are contingently related to us, which contingency may change given the changing personal, cultural, or technological circumstances. Bitcoin fully satisfies the separability criterion, offering multiple modes of ownership change, not only in the form of transactions on the blockchain, but also in the form of the physical transfer of the key pair (on an external hard drive or even paper).

It is possible to say that from Penner's point of view coins on the bitcoin blockchain do count as a property in all senses of the word, since bitcoins satisfy both the exclusivity and the separability criterion. This does not, however, fully explain all aspects of blockchain property, for one important reason. As I mentioned earlier, in theory cryptographic ownership can be an absolute ownership, which excludes anybody from interference in ownership rights. This is nicely illustrated by the ongoing debate over privacy, smart phone encryption, and the right of government institutions to interfere with it. Apple iPhone encryption, which recently became a centre of government lawsuits and media attention, uses a cryptographic key built into the physical architecture of the device, which makes the key unique (Zetter 2016). Thus only the owner of the device with the knowledge of the password can use it, effectively excluding anybody, even the manufacturer and government agencies, from interference.

Here cryptographic ownership effectively trumps some of the legal ownership rights. Nevertheless, government agencies, such as the police, can take physical possession of a device, thus effectively excluding the person with the password from using it. A bitcoin owner in contrast (if he or she implements the necessary security measures) may enjoy absolute non-interference from anybody else.

To get a better idea of the absolute possession of property, it might be helpful to turn to a historical conception of property developed by Hegel (1991). Unlike other historical philosophical conceptions of property, such as the Lockean theory, which is largely normative, Hegel's account of property developed in *Elements of the Philosophy of Right* can be considered as much a descriptive theory as it is normative

(Waldron 1988). From a general point of view, Hegel's theory of property is also a bottom-up justification of property, where property rights occur when the will of an individual is placed in the "thing," being derived from an individual freedom and not from the government authority; thus the starting point in Hegel's reasoning is to define the idea of property in its absolute form (Waldron 1988; Penner 1997). It is important to notice that Hegel does not suggest on this basis that property rights are absolute and can overrule state interest (Brudner 2013), but it can be argued that his normative considerations on the structure of law do not constrict the explanatory value of his descriptive analysis.

The key interest for us presents a nature of property ownership as suggested by Hegel. He distinguishes three modes of possession for things. Physical seizure is the immediate mode of possession, but subjective, temporary, and limited in scope, followed by the second mode, which entails giving something a form that extends the presence of will from immediate time and space. The third mode of possession is an indication, the marking of a thing with one's will, and according to Hegel this is the most complete mode of all (Hegel 1991, § 58). Completeness means that my marking a thing is an ultimate sign to others that I am excluding them and showing them that I have put a will in the thing. This mode turns mere possession into property. It is an elaboration on the statement that for a thing to count as a property, it has to be recognized by others as such (Hegel 1991, § 51). In *Philosophy of Mind* Hegel (2007) draws this conclusion from the idea that a person's freedom and independence come into existence through the being of other persons, relation to them, and recognition by them. Property for Hegel is another externalization of a person's will and freedom coming into existence through recognition by others (Brudner 2013).

This thesis highlights probably the most significant aspect of blockchain ownership, as, in addition to exclusion and separability, bitcoins have this third important aspect—universal recognition by other users of the blockchain as property. This seemingly trivial observation unpacks not only the similarity of bitcoin to other types of property but also its uniqueness. In a simple sense, all kinds of property can be regarded as a social convention, involving recognition of the property rights of owners and negative duties of non-owners (Waldron 1988). Implementation of such a convention in a complex society requires some kind of universal access to the knowledge about property rights of each individual. Government and other legal institutions providing access to this knowledge perform this function of epistemic access for citizens within the apparatus of the institution of property.

The uniqueness of blockchains is twofold: not only do they eliminate a need for a third-party authority to enforce exclusion rights, they also

provide a system of universal access to the knowledge about property rights of all bitcoin owners.[6] Together with exclusion and separability, this in fact makes blockchain technology a self-sufficient alternative institution of property existing independently of any legal institutions. In that sense all the collusions and contradictions of bitcoin with legal systems are understandable, since they can be seen as competing normative structures. The true scope of such a blockchain institution of property is yet to be seen, but it can already compete with global intermediaries serving as trusted third parties guaranteeing international monetary transactions, such as Swift (Skinner 2016). This also explains why most attempts on the national scale to regulate blockchain technology targeting miners and exchanges are likely to be unsuccessful, since organization of this kind is only an element of a larger normative structure.

For future analysis it is also crucial to clearly disentangle norms and ideas present in specific implementations of blockchain technology from the very capacity of a technology to deliver these norms as an institution. Indeed, as with any other institution embodied by human agents, it can also incorporate the norms and beliefs of the individual members or organizations constituting it. But in its design capacity the blockchain protocol is essentially agnostic towards social or moral norms, which can be delivered or ignored by the implemented system.

5. Conclusion

Looking at the blockchain as an institution of property helps to grasp the uniqueness and novelty of this technology in the social context. Of course, it is still very early to conclude that some of the blockchain applications will be able to replace legal norms and property rights. Yet it is already possible to see how some aspects of property relations in society are being replaced with the blockchain. One example of such a hybrid institution of property is a distributed ledger that can hold information about intellectual property of right holders instead of a centralized government database (Ha 2016). One next possible step is the implementation of property rights for physical objects such as Internet of Things applications, which can eliminate some functions of third-party authorities for the enforcement of property rights (Brody and Pureswaram, 2014).

[6] Access to ledger records does not have to be completely open for functioning cryptocurrency. Unlike a bitcoin ledger, which is fully transparent, the privacy-focused Monero blockchain works differently. It uses a different protocol, Cryptonote, where nodes check only group identities of addresses, which helps to conceal individual users; nevertheless the principle of a public ledger holds (see Van Saberhagen 2013).

In this respect some of the forecasts by Wright and De Filippi look more and more plausible. My only point of disagreement with them is their hypothesis that wider blockchain implementation can lead to the disappearance of property rights. Whether wide adoption of a share economy will affect the distribution of property in society is of course an open question, with no clear answer as yet. But the blockchain technology in itself does not necessarily lead to the dissolution of property rights in society. On the contrary, the blockchain may help to extend and enforce individual property rights in new domains, such as the ownership of private data (Zyskind, Nathan, and Pentland 2015). There is of course no denying that the blockchain may pose a significant threat to the existence of some legal institutions of property in the future, but in the bigger picture blockchain technology should, among other things, be regarded as a new type of property institution, as another implementation of the philosophical idea of property rights.

TU Delft
Ethics and Philosophy of Technology
Jaffalaan 5
2628 BX Delft
The Netherlands
g.ishmaev@tudelft.nl

Acknowledgments

I would like to thank Mark Alfano for helpful comments on earlier drafts of this paper, and Seamus Miller for insightful conversation on the conceptualizations of social institutions. Also, I would like to thank anonymous reviewers, and Taylor Stone, whose comments greatly enhanced the quality of the paper.

References

Aristotle. 1958. *The Politics of Aristotle*. Translated by Ernest Barker. London: Oxford University Press.

Brody, Paul, and Veena Pureswaran. 2014. *Device Democracy: Saving the Future of the Internet of Things*. IBM. http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/

Brudner, Alan. 2013. "Private Property and Public Welfare." In *Philosophical Foundations of Property Law*, edited by James Penner and Henry Smith, 68–98. Oxford: Oxford University Press.

Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform." White Paper. https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper.

Campbell, Rebecca. 2016. "IRS at a Standstill with Bitcoin; Users and Tax Professionals Remain in the Dark." *Cryptocoinsnews*. October 8. https://www.cryptocoinsnews.com/irs-standstill-bitcoin-users-tax-professionals-remain-dark/

CFTC. 2016. Docket No. 16–19. "Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, as Amended, Making Findings and Imposing Remedial Sanctions." June 2. http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfbfxnaorder060216.pdf

De Filippi, Primavera. 2014. "Bitcoin: A Regulatory Nightmare to a Libertarian Dream." *Internet Policy Review* 3, no. 2:43–56.

Dittus, Martin. 2017. "Exploring the Darknet in Five Easy Questions." *Oxford Internet Institute Blog*. September 12. https://www.oii.ox.ac.uk/blog/exploring-the-darknet-in-five-easy-questions/

Fairfield, Joshua A. 2014. "BitProperty." *Southern California Law Review* 88 no. 4:805–74.

Greenspan, Gideon. 2016. **"**Smart Contracts and the DAO Implosion.**"** *Multichain Blog*. June 22. http://www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/

Ha, Anthony. 2016. **"**Blockai Uses the Blockchain to Help Artists Protect Their Intellectual Property.**"** *Techcrunch*. March 14. https://techcrunch.com/2016/03/14/blockai-launch/

Haber, Stuart, and W. Scott Stornetta. 1990. **"**How to Time-Stamp a Digital Document.**"** In *Advances in Cryptology-CRYPT0 '90*, edited by A. J. Menezes and S. A. Vanstone, 437–55. doi: 10.1007/3-540-38424-3_32

Hegel, Georg Wilhelm Friedrich. 1991. *Hegel: Elements of the Philosophy of Right*. Cambridge: Cambridge University Press.

Hegel, Georg Wilhelm Friedrich, and Michael Inwood. 2007. *Hegel: Philosophy of Mind*: Translated with Introduction and Commentary. Oxford: Oxford University Press.

Hertig Alyssa. 2016. **"**Ethereum's Two Ethereums Explained.**"** *Coindesk*. July 18. http://www.coindesk.com/ethereum-classic-explained-blockchain/

Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman. 2008. *An Introduction to Mathematical Cryptography*, vol. 1. New York: Springer.

Hohfeld, Wesley Newcomb. 1917. "Fundamental Legal Conceptions as Applied in Judicial Reasoning." *Yale Law Journal* 26, no. 8:710–70. doi:10.2307/786270

Honore, Anthony Maurice. 1961. "Ownership." In *Oxford Essays in Jurisprudence*, edited by A. G. Guest, 107–47. Oxford: Clarendon Press.

Hendrickson, Joshua R., Thomas L. Hogan, and William J. Luther. "The Political Economy of Bitcoin." *Economic Inquiry* 54, no. 2: 952–39. doi: 10.1111/ecin.12291

Karlstrøm, H. 2014. "Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin." *Distinktion: Scandinavian Journal of Social Theory* 15, no. 1:23–36. https://doi.org/10.1080/1600910X.2013.870083

Kharif, Olga. 2014. "Bitcoins Seized from Silk Road Offered in Second Auction." *Bloomberg*. December 14. https://www.bloomberg.com/news/articles/2014-12-04/bitcoins-seized-from-silk-road-offered-in-second-auction

Koblitz, Neal, and Alfred J. Menezes. 2016. "Cryptocash, Cryptocurrencies, and Cryptocontracts." *Designs, Codes and Cryptography* 78, no. 1:87–10. doi: 10.1007/s10623-015-0148-5

Locke, John. 1993. *Two Treatises of Government*. Edited by Mark Goldie. London: Everyman.

Lorenzetti, Laura. 2014. "Bitcoin Seized from Silk Road Offered in Second Auction." *Fortune*. December 4. http://fortune.com/2014/12/04/bitcoins-seized-from-silk-road-on-offer-in-a-second-auction/

Kruithof, Kristy, Judith Aldridge, David Décary Hétu, Megan Sim, Elma Dujso, and Stijn Hoorens. 2016. **"**The Role of the 'Dark Web' in the Trade of Illicit Drugs.**"** Rand Corporation. doi: 10.7249/RB9925

McMillan, Robert. 2014. **"**The Inside Story of Mt. Gox Bitcoin's $460 Million Disaster.**"** *Wired*. March 3. https://www.wired.com/2014/03/bitcoin-exchange/

Melendez, Steven. 2016. "Amid Arrests and Prosecutions Rules Around Selling Bitcoin Remain Fuzzy." *Fastcompany Magazine*. May 20. https://www.fastcompany.com/3059770/selling-bitcoin-could-land-you-in-jail-but-rules-remain-fuzzy

Merrill, Thomas W., and Henry E. Smith. 2001. "What Happened to Property in Law and Economics?" *Yale Law Journal* 111, no. 2:357–98. http://www.yalelawjournal.org/essay/what-happened-to-property-in-law-and-economics

Miller, Seamus. 2001. *Social Action: A Teleological Account*. Cambridge: Cambridge University Press.

Munzer, Stephen R. 1990. *A Theory of Property*. Cambridge: Cambridge University Press.

———. 2013. "Property and Disagreement." In *Philosophical Foundations of Property Law*, edited by James Penner and Henry Smith, 289–319. Oxford: Oxford University Press.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." http://bitcoin.org/bitcoin.pdf

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press.

Nozick, Robert. 1974. *Anarchy, State and Utopia*. New York: Basic Books.

Paar, Christof, and Jan Pelzl. 2009. *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin: Springer.
Penner, James E. 1997. *The Idea of Property in Law*. Oxford: Oxford University Press.
Pufendorf, Samuel. 1994. *The Political Writings of Samuel Pufendorf*. Translated by Michael J. Seidler. Oxford: Oxford University Press.
Reuters. 2016. **"**Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong.**"** *Fortune*. August 3. http://fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/
Ripstein, Arthur. 2013. "Possession and Use." In *Philosophical Foundations of Property Law*, edited by James Penner and Henry Smith, 156–81. Oxford: Oxford University Press.
Shcherbak, Sergii. 2014. "How Should Bitcoin Be Regulated?" *European Journal of Legal Studies* 7, no. 1:45–91. http://hdl.handle.net/1814/32273
Skinner, Chris. 2016. "Will the Blockchain Replace Swift?" *American Banker*. March 8. https://www.americanbanker.com/opinion/will-the-blockchain-replace-swift
Swan, Melanie. 2015. *Blockchain: Blueprint for a New Economy*. Sebastopol, Calif.: O'Reilly Media.
Szabo, Nick. 1997. "Smart Contracts: Formalizing and Securing Relationships on Public Networks." *First Monday* 2, no. 9:n.p. doi: https://doi.org/10.5210/fm.v2i9.548
Tu, Kevin V., and Michael W. Meredith. 2015. "Rethinking Virtual Currency Regulation in the Bitcoin Age." *Washington Law Review* 90, 271–347. https://ssrn.com/abstract=2485550
Van Hoecke, Mark. 2011. "Legal Doctrine: Which Method(s) for What Kind of Discipline?" In *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline*? edited by Mark Van Hoecke, 1–18. Oxford: Hart.
Van Saberhagen, Nicolas. 2013. "Cryptonote v 2. 0." https://cryptonote.org/whitepaper.pdf
Vardi, Noah. 2016. "Bit by Bit: Assessing the Legal Nature of Virtual Currencies." In *Bitcoin and Mobile Payments*, edited by Gabriella Gimigliano, 55–71. Basingstoke: Palgrave Macmillan.
Waldron, Jeremy. 1988. *The Right to Private Property*. Oxford: Clarendon Press.
———. 2013. "To Bestow Stability upon Possession: Hume's Alternative to Locke." *Philosophical Foundations of Property Law*, edited by James Penner and Henry Smith, 1–12. Oxford: Oxford University Press.
Wright, Aaron, and Primavera De Filippi. 2015. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia." https://ssrn.com/abstract=2580664

Zetter, Kim. 2016. "Apple's FBI Battle Is Complicated: Here's What's Really Going On." *Wired*. February 18. https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/

Zyskind, Guy, Oz Nathan, and Alex Pentland. 2015. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." In *2015 IEEE Security and Privacy Workshops (SPW)*, 180–84. doi: 10.1109/SPW.2015.27