The Techno-Economic Content of Your Crypto Wallet

Bronwyn E. Howell, School of Management, Victoria University of Wellington, bronwyn.howell@vuw.ac.nz

Petrus H. Potgieter, Dept of Decision Sciences, University of South Africa, potgiph@unisa.ac.za

12th June 2019

Prepared for delivery at the Workshop on the Ostrom Workshop (WOW6) conference, Indiana University Bloomington, June 19–21, 2019 in the themed panel *Blockchain: Innovation in Distributed Governance in the Cryptosphere*.

Abstract

This paper considers some technical details around the control and use of crypto currency assets and how these reflect the ordinary understanding of ownership. It provides a non-technical summary of notions in cryptology that are required for the analysis as well as a brief review of the distributed ledger concept. Finally, it reflects on how the ownership concept with respect to supposed property that is loosely called a crypto wallet could be seen in the light of Ostrom's scholarship.

Keywords

Blockchain, distributed ledger, crypto currency wallet.

1 Introduction

The focus in this paper is on the property arrangements for crypto currency rather than particular resource attributes of the distributed ledger. For the sake of brevity and also since this is still the largest crypto unit, the focus is on Bitcoin. The also very widely used Ethereum presents many interesting challenges and opportunities arising from its smart contract facility which reflect on notions of ownership. This will be examined in detail in a future paper.

The common resource (the distributed ledger) is critical to the exchange of the crypto currency but in fact this affects mainly the access aspect of the usual notion of property and not the exclusion aspect. The latter is more strictly technical, which is the main topic of the paper. We shall briefly look also at the meaning of crypto assets held on exchanges, which is a dual-layered ownership. Ostrom and Hess (2007) write "where many individuals will work, live, and play in the next century will be governed and managed by mixed systems of communal and individual property rights", referring perhaps rather to *this* century.

We start by reviewing the relevant background concepts from cryptology in the subsequent section. Then, we analyse the way these constructs are employed to construe ownership arrangements for the crypto currency. Then, certain issues arising out of specific technical features are discussed. Finally, we review the notion of crypto asset property in the light of the technical execution as well as an economist's view.

2 Background

In order to form a proper understanding of the operation of a crypto currency on a distributed ledger, it is necessary to have a basic comprehension of the key concepts from cryptology[1]

2.1 Computational complexity

The science of modern cryptography is based in large part on the theory and techniques of computational complexity, another subfield of theoretical computer science. We try to provide a fairly intuitive explanation of the important facts here.

One of they key insights in this area has been to realize that there are problems

1. for which a solution candidate (when given) can be quickly and efficiently verified or proven to be incorrect; and others
2. for which a solution can be quickly and efficiently found.

If problems have unique solutions then all those of the second type are of course also of the first type. Computational complexity has also identified problems as being of the first type but not known and believed to possibly not be of the second type.

To put it in more mathematical terms, there are functions f for which, given x and y it easy easy to give a yes/no answer to the question

$$y =^{?} f(x)$$

but for which the question of finding x if y is given, by solving the problem

$$y = f(x^{?})$$

is not easy and, in fact, very difficult. We say that f is easy to compute but difficult to *invert*.

Note that in general x need not simply be a number but can be a list of numbers and so on, depending on the application. Furthermore, there are functions (or, problems) f for which the calculation of an x such that $f(x) = y$ becomes very rapidly more difficult as the size of y increases while the difficulty of having a computer check a given answer does not increase significantly. This means that the x can be made more 'secret' by working with larger y.

2.2 Hash functions

A hash function is a function f with the properties above. In the case of hash functions, x can be any text and $f(x)$ is an output value of fixed length. It follows that there are always infinitely many x_1 and x_2 such that $f(x_1) = f(x_2)$ but hash functions are difficult to invert so that given any y computed by some hash function f, it is very difficult to determine any x so that $y = f(x)$. It is of course not impossible and the proof-of-work basis of Bitcoin is that miners have to find solutions to problems of this kind.

Hash functions further have the property that if x_1 and x_2 differ little, there hash values $f(x_1)$ and $f(x_2)$ will generally differ a great deal. That is, a small change in the text will result in a large change of the hash value. Also, given a specific x_1 and a computed $f(x_1) = y$ and a search procedure for determining x_2 such that $f(x_2) = y$ it will be extremely unlikely that $x_2 = x_1$ even if such x_2 is found. This should, in itself, not be very easy.

The hashing of a given text is therefore a process that is practically impossible to invert. As a consequence, the hash value of a text is a good characterisation of it but it is nevertheless not practical to recover the original text. Given any two texts, the probability that they will have the same hash value is extremely small.

[1] In this work, we are not very careful about distinguishing between *cryptology* (which should be understood to include the study and analysis of cryptography) and *cryptography* itself.

2.3 Public/private key pairs

A public/private key pair is an (x, y) that is connected via a function f as above. Hence $y = f(x)$ and x is the private key and y the public one. There are functions f and encryption and decryption schemes under which a person in position of y is able to encrypt a message (using y) in such a way that knowledge of the public key y is not sufficient for decrypting the message. Decryption requires knowledge of x. This is asymmetric cryptography which is the basis also of secure communication on the Internet, for example. The public key is generally published by the user who will however jealously guard the private key since possession of the private key is equivalent to full control over the identity or role with which it is associated.

Public/private key pairs are usefully generated using a random number generator. Typically, one might pick the private key using some randomised process and compute the associated public key. Very good random number generators are required for this part of the process to be safe. Indeed, the assumption is that the keys are chosen from such a large sample space that the probability of two different users picking the same keys, is negligible.

2.4 Digital signatures

Electronic signatures have well-defined legal status or juristic persons in lieu of an ordinary signature. The use of electronic agreements dates back to at least 1869, when a court in New Hampshire determined that a valid contract could be formed by telegraph (Hill 2018). A common feature of an electronic signature is that it has to be established very clearly that it is tied to a specific natural person.

Digital signatures are a specific implementation of the technical part of electronic signatures, using cryptographical methods. A digital signature need not be tied to a specific natural person or juristic entity – or any entity at all, in fact. A subset of digital signatures qualify in certain jurisdictions (e.g. South Africa or the European Union) (Eiselen 2015) as advanced electronic signatures which are digital signatures that serve as valid electronic signatures for the purpose of concluding legally enforceable agreements.

Advanced electronic signatures are generated using a public/private key pair. The public key is used to verify a signature and the private key is used to generate it. A user typically announces the public key and can be identified by it. Other parties use this public key to validate transactions signed in this way by the user. Should someone obtain the private key, they would be able to fully impersonate the original user in any action which is authenticated using the key pair.

2.5 Distributed ledgers

A distributed ledger (DL) is a database (or file) spread across several nodes or computing devices. Each node in a network has access to (and probably saves) an identical copy of the entire ledger. The concepts of an electronic *ledger* and *distributed ledger* are very well described by Anta et al. (2018). By ledger we mean, as in usual parlance, an object which starts empty and grows through records being appended to it. Note that this does not necessarily imply that the records are appended in a linear fashion, so the ledger itself need not appear strictly linear. It can, for example, be a tree. In traditional accounting (based on physical books) the objects are generally linear and of course the data objects that constitute different kinds of ledgers are also linearly representable so the distinction is actually unimportant as long as the records being appended can themselves be represented in a linear fashion. The linear order can, trivially, be implied by the time of addition of an item (which may included a description of its relation to preceding items).

Blockchains are a specific kind of distributed ledger where the common rules for changing the data object are of a particular kind. Every blockchain is a distributed ledger but not vice versa. The technological characteristics of blockchain systems are well documented (Narayanan et al. 2016). Considerable faith has been placed in the technology as a means of revolutionising digital transacting (Mulligan et al. 2018; Crosby et al. 2015; Czepluch, Lollike, and Malone 2015; Swan 2015), due to their promise of transparent, tamper-proof and secure systems enabling novel business solutions (Andoni et al. 2019).

3 Operations

The Bitcoin blockchain is a distributed ledger which is a comprehensive record of transactions of the (simplified) form

> A gives B an amount of C

that have been accepted as valid. This presupposed, of course, that A can be said to have had at least C to give and C is an ordinary number with a fixed decimal expansion, akin to a dollar (or euro or rand) amount with the difference that Bitcoin uses not 2 but more decimal places. Since the ledger does not record balances, in order to determine the possible validity of the transaction, it is in principle necessary to determine whether A's incoming minus outgoing valid transactions from inception to that point, amount to at least C.

In this section, we look closer at how A and B are designated in the actual process. Both will in fact be *valid* addresses and in the crypto currency world, possession amounts to control of an address. An entity (whether biological or mechanical) that controls an address is able to nominate transactions of the form above and nothing else. Unlike bank accounts and bank balance where in principle (at least up to now) the content is convertible into banknotes and coins, crypto currency cannot be converted into anything tangible or otherwise, except by trading it on an exchange or bartering it for something. That is, there is no tangible representation of crypto currency. This would be analogous to a fiat currency system in which there is no longer any physical cash.

In order to record a valid transaction in the ledger, it is necessary to verify that the transaction is authorised and not just non-contradictory (in the sense that A might be said to have at least C). In order to do this, the transaction request should be accompanied by some tokens of authenticity produced by A. More precisely, these tokens have to be produced by the entity submitting the transaction and should demonstrated that this entity exercises control over the address A.

The *Genesis* block of Bitcoin made certain allocations and further mining generates allocations of new Bitcoin. Famously, no more than 21 million Bitcoin can be issued. Like cash, Bitcoin can be irretrievably lost (or destroyed) when an entity loses control over an address. Although the address might still be said to have Bitcoin allocated (nett) to it, those funds can effectively no longer be disbursed. It has been reported that up to one third of Bitcoin issued to date have been lost although this is impossible to verify. Estimates are obtained by looking at the allocations to addresses that have been inactive over a long period although it it impossible to conclusively determine whether this inactivity derives from lost control or a longer term investment strategy.[2]

Incidentally, Maesa, Marino, and Ricci (2016) used the Bitcoin user graph of December 2015 to reveal the presence of important 'bridge' nodes or addresses through which a large number of transactions flowed. They also demonstrated the presence of a "Matthew effect"[3]

3.1 Transactions

The Bitcoin distributed ledger records blocks of transactions of the form

> {list of input addresses and amounts} –> {list of output addresses and amounts}

where the sum of the input amounts has to be at least as large as the sum of the output amounts. The difference between the input total and the output total can be collected as fees by a miner who verifies the transaction and who generates the block (containing this transaction) that is accepted by blockchain community. Other ways of compensating miners and the consensus mechanism itself, is explored in more detail by Howell, Potgieter, and Sadowski (2019).

Every address is a 34 character string, the first character of which is normally 1 or 3 – currently used to indicate whether it is an ordinary (1) or script (3) address. In either case, the substantive part of the address is a hash value.

3.2 Ordinary addresses

An ordinary Bitcoin address is simply the hashed public part of a public/private key pair (Tschorsch and Scheuermann 2016). Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm for the key pair. ECDSA is a

[2] One of the authors have a significant number of acquaintances who claim to have lost control over substantial but not spectacular sums.

[3] From "For to every one who has will more be given, and he will have abundance; but from him who has not, even what he has will be taken away." (The Bible, Matthew 25:29)

general method that requires specification of a specific curve. Bitcoin uses a curve called secp256k1.[4] This is not one of the curves regarded as suspect because it is endorsed by the US National Institute of Standards and Technology (NIST). The application of any ECDSA method requires the generation of good pseudo-random numbers. In 2013, a bad random number generator in Android caused users to lose control of private keys, for example.[5]

The Bitcoin addressed is produced by taking the public key and hashing it, first using the algorithm SHA-256 and then using RIPMD-160 and then encoding the final output as a character string and prefixing 1. An example of a valid and active address is

1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g

which is currently in use. It is actually a very active and perhaps notorious address.[6]

3.3 Script addresses

A script address is the hash value of a Bitcoin script and the spending requires at least the presentation of the script itself (Bistarelli, Mercanti, and Santini 2018). Unlike the Ethereum programming language Solidity, the Bitcoin scripting language is not Turing-complete, i.e. it is not a general purpose computation tool.[7] The script is actually provided by the submitter of a transaction and the processor would execute the script plus any additional data in order to determine whether the input bitcoin can be spent.

One of the extremely useful types of script is for M-of-N transactions, i.e. where at least M from a set of N valid signatures are required. This is a hard encoding into a 'smart contract' type instrument of a traditional management arrangement. The casual observations of the authors is that payments from and to script addresses now amounts to a substantial proportion of all transactions on Bitcoin.

3.4 Crypto currency wallets

Very importantly, a *crypto wallet* is simply a piece of software that stores private keys associated to addresses controlled by the wallet user (Bistarelli, Mercanti, and Santini 2018). It does not, in any other sense, enclose the crypto currency coins or units themselves. As with any data, a perfect copy of a digital wallet is in fact identical to the original and can be produced at virtually no cost if one has access to the original wallet. It is simply the copying of data.

In order to exercise rights of ownership associated with crypto currency, the holder therefore has to not only guard a copy of the wallet (or just of the private keys) but also has to prevent others from accessing it (even passively). If the 'owner' of a wallet suffers a malicious party gaining access to the wallet content (the private key), they might be as little aware of this as one might be of someone having taken a photograph of one. The only way the integrity of the key can be checked is by constantly monitoring the blockchain for unauthorised transactions involving these keys. A wallet holder who suspects that their keys might have been compromised, can always 'spend' their coins by assigning them to a new address – possible holding the associated keys elsewhere. This would incur a transaction cost but would at least reset the situation. It would be fair to say that the only proof that one actually possesses some bitcoin is to spend it.

The case of accounts in crypto exchanges and the associated 'wallets' is a different one which we briefly address below. Confusion around this is one of the major problems around exchanges and since so much of crypto currency holdings is linked to exchanges, scandals arising in this way have been responsible for the lion's share of crypto currency-related problems (as perceived by the public). We discuss this in another paper.

4 Ownership

In this section, we consider specific further aspects of the notion of ownership, as it relates to crypto currency holdings. As seen above, the nature of transactions in crypto currency is that sufficient proof of holding the private keys (or inputs to a

[4] https://www.johndcook.com/blog/2018/08/14/bitcoin-elliptic-curves/

[5] https://bitcoin.org/en/alert/2013-08-11-android

[6] https://coinwrath.com/1b-worth-of-bitcoin-are-currently-on-the-move-from-a-suspicious-wallet/

[7] Which has many advantages since all general purpose computation is subject to the halting problem constraint (Potgieter 2006).

script) amounts to full authorisation of the power to dispose of the stake by spending it. It does not require volition or any other recorded consent.

4.1 Accounts on exchanges

The authors believe that most crypto currency 'holdings' on exchanges are actually promises to pay, in the following sense. Exchanges accept fiat currency from users and assign a notional amount of crypto currency to them. When users seek to withdraw crypto (to make payments, for example) the exchange might mediate a transfer of crypto from the exchange's wallet to the recipient. Should an exchange user seek to receive crypto, the exchange might assign a private/public key pair to the user. The private part of the key pair is stored centrally by the exchange and not by the user so that the user retains access through their normal exchange logon. This is again a source of problems but/and it evades one of the key features of crypto currencies like Bitcoin – that it is possible to lose crypto holdings by losing the private keys.

The exchange Kraken has an address 1AnwDVbwsLBVwRfqN2x9Eo4YEJSPXo2cwG for example[8] which is active and which contained over 23,000 bitcoin (worth over 170 million US dollars, at time of writing). We would argue that this is the equivalent of an ordinary bank balance sheet asset. Problems related to exchanges are therefore akin to problems at banks and not in the underlying currency.

4.2 Dependence on mathematical art

As will be clear from the introduction, background and description of blockchain operations, these are critically dependent on assumptions about the functioning of the standard tools of mathematical cryptography (Giechaskiel, Cremers, and Rasmussen 2016). It is assumed, for example, that it is difficult to compute the public key that corresponds to the address hash 1AnwDVbwsLBVwRfqN2x9Eo4YEJSPXo2cwG of the previous subsection, which controls a substantial fortune in bitcoin. Further, it is assumed that even if one were in possession of the public key that it would then be very difficult to compute the corresponding private keys. If both if these assumptions were false, then it would be easy for a 'non-legitimate' actor to spend the bitcoin in that address. That this has not happened yet is a a fairly good indication that no-one has so far been able to find the corresponding private keys.

Recall that this is not an impossibility – merely a practically infeasible difficult task, we believe. Quantum computing is one of the possible threats and although a wiki with contingency plans has been set up by the Bitcoin community, these are not very well developed (Giechaskiel, Cremers, and Rasmussen 2016). Specifically, the community (like anyone using modern cryptology) relies on certain specific key sizes being safe. Giechaskiel, Cremers, and Rasmussen (2018) describe in detail how the various tools in crypto currencies are sensitive to the integrity of the cryptographic protocols.

5 Ostrom's Law

Fennell (2011) encapsulates as Ostrom's Law the principle

> a resource arrangement that works in practice can work in theory.

The Ostrom principles (EtAl 2019) for governance arrangements that are stable have been discussed by Howell and Potgieter (2019).

Crypto currencies work in practice although the size of their impact is still unclear. As we have seen above, the ownership arrangement is mathematical rather than legal. However, pay to script hash (P2SH) addresses in Bitcoin for example, enable ordinary legal arrangements to be meshed with mathematical arrangements in a fascinating way. Our work in another paper shows, using the Ostrom Institutional Analysis for Development framework, that distributed ledger governance arrangements are very imperfectly aligned with the Ostrom principles for stable arrangements. Nevertheless, the ownership notions described above are, we believe, at least clear and clearly functional.

Wide acceptance of these ownership arrangements might depend on a societal understanding and interpretation of the relatively technical and mathematical nature of the same. This is not necessarily any different from many other

[8] https://www.walletexplorer.com/address/1AnwDVbwsLBVwRfqN2x9Eo4YEJSPXo2cwG

interpretations and re-interpretations that have been required over time as human society has adopted new technologies and ways working, however.

6 Conclusion

One should take care when impugning ordinary notions of ownership and transaction between natural and/or juristic persons to the entries in a crypto currency blockchain. In the usual understanding of a transaction, there is intent and consent involved from all parties and the presentation of fraudulent credentials would invalidate a transaction. For crypto currency, this is not the case at all and in this sense (possibly intentionally), they really do resemble cash and

> possession is three thirds of the law

might be taken as the guiding principle. Parties that transact are credentialed in a predetermined and uniform way – by presentation of the private key pairs corresponding to a given public key. The 'asset' itself is also located in a different way. Ordinary cash is identical with its physical manifestation (although its value depends on much else) whereas the content of a crypto currency 'wallet' consists only of the keys required to manifest ownership (through transfer) on a blockchain which is an entirely separate entity.

Nevertheless, the multi-signature wallets and smart contracts on blockchains such as Bitcoin and Ethereum represent a technical innovation that do allow for distributed consent for transactions to be fully automated in a completely transparent fashion.

References

Andoni, Merlinda, Valentin Robu, David Flynn, Simone Abram, Dale Geach, David P. Jenkins, Peter McCallum, and Andrew Peacock. 2019. "Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities." *Renewable and Sustainable Energy Reviews* 100 (February). Elsevier Limited: 143–74. doi:10.1016/j.rser.2018.10.014.

Anta, Antonio Fernández, Kishori Konwar, Chryssis Georgiou, and Nicolas Nicolaou. 2018. "Formalizing and Implementing Distributed Ledger Objects." *ACM SIGACT News* 49 (2). Association for Computing Machinery (ACM): 58–76. doi:10.1145/3232679.3232691.

Bistarelli, Stefano, Ivan Mercanti, and Francesco Santini. 2018. "An Analysis of Non-Standard Bitcoin Transactions." In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE. doi:10.1109/cvcbt.2018.00016.

Crosby, Michael, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. 2015. "Blockchain Technology: Beyond Bitcoin." *Sutardja Center for Entrepreneurship & Technology*. http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

Czepluch, Jacob Stenum, Nikolaj Zangenberg Lollike, and Simon Oliver Malone. 2015. "The Use of Block Chain Technology in Different Application Domains." *The IT University of Copenhagen, Copenhagen*.

Eiselen, S. 2015. "Fiddling with the ECT Act Electronic Signatures." *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad* 17 (6). Academy of Science of South Africa: 2805. doi:10.4314/pelj.v17i6.16.

EtAl, Howell. 2019. "Governance of Blockchain and Distributed Ledger Technology Projects."

Fennell, Lee Anne. 2011. "Ostrom's Law: Property Rights in the Commons." *International Journal of the Commons* 5 (1). Uopen Journals: 9. doi:10.18352/ijc.252.

Giechaskiel, Ilias, Cas Cremers, and Kasper B. Rasmussen. 2016. "On Bitcoin Security in the Presence of Broken Cryptographic Primitives." In *Computer Security ESORICS 2016*, 201–22. Springer International Publishing. doi:10.1007/978-3-319-45741-3_11.

———. 2018. "When the Crypto in Cryptocurrencies Breaks: Bitcoin Security Under Broken Primitives." *IEEE Security & Privacy* 16 (4). Institute of Electrical; Electronics Engineers (IEEE): 46–56. doi:10.1109/msp.2018.3111253.

Hill, Richard. 2018. "The Future of Internet Governance: Dystopia, Utopia, or Realpolitik?" *Sociology and Anthropology*

6 (4). Horizon Research Publishing Co., Ltd.: 392–423. doi:10.13189/sa.2018.060406.

Howell, Bronwyn E., and Petrus H. Potgieter. 2019. "Governance of Blockchain and Distributed Ledger Technology Projects."

Howell, Bronwyn E., Petrus H. Potgieter, and Bert M. Sadowski. 2019. "Governance of Blockchain and Distributed Ledger Technology Projects." *SSRN Electronic Journal*. doi:10.2139/ssrn.3365519.

Maesa, Damiano Di Francesco, Andrea Marino, and Laura Ricci. 2016. "Uncovering the Bitcoin Blockchain: An Analysis of the Full Users Graph." In *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*. IEEE. doi:10.1109/dsaa.2016.52.

Mulligan, CJ, Z Scott, S Warren, and JP Rangaswami. 2018. "Blockchain the Hype." In *World Economic Forum. Http://Www3. Weforum. Org/Docs/48423_Whether_Blockchain_WP. Pdf. Accessed*. Vol. 2.

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

Ostrom, Elinor, and Charlotte Hess. 2007. "A Framework for Analyzing the Knowledge Commons." In *Property Law and Economics*, edited by Charlotte Hess and Elinor Ostrom. Chapters. MIT Press. https://www.jstor.org/stable/j.ctt5hhdf6.

Potgieter, Petrus H. 2006. "Zeno Machines and Hypercomputation." *Theoretical Computer Science* 358 (1). Elsevier BV: 23–33. doi:10.1016/j.tcs.2005.11.040.

Swan, Melanie. 2015. *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc.

Tschorsch, Florian, and Bjorn Scheuermann. 2016. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies." *IEEE Communications Surveys & Tutorials* 18 (3). Institute of Electrical; Electronics Engineers (IEEE): 2084–2123. doi:10.1109/comst.2016.2535718.