The Double-Spending Problem and Cryptocurrencies

19th December, 2017

Usman W. Chohan, MBA

School of Business and Economics

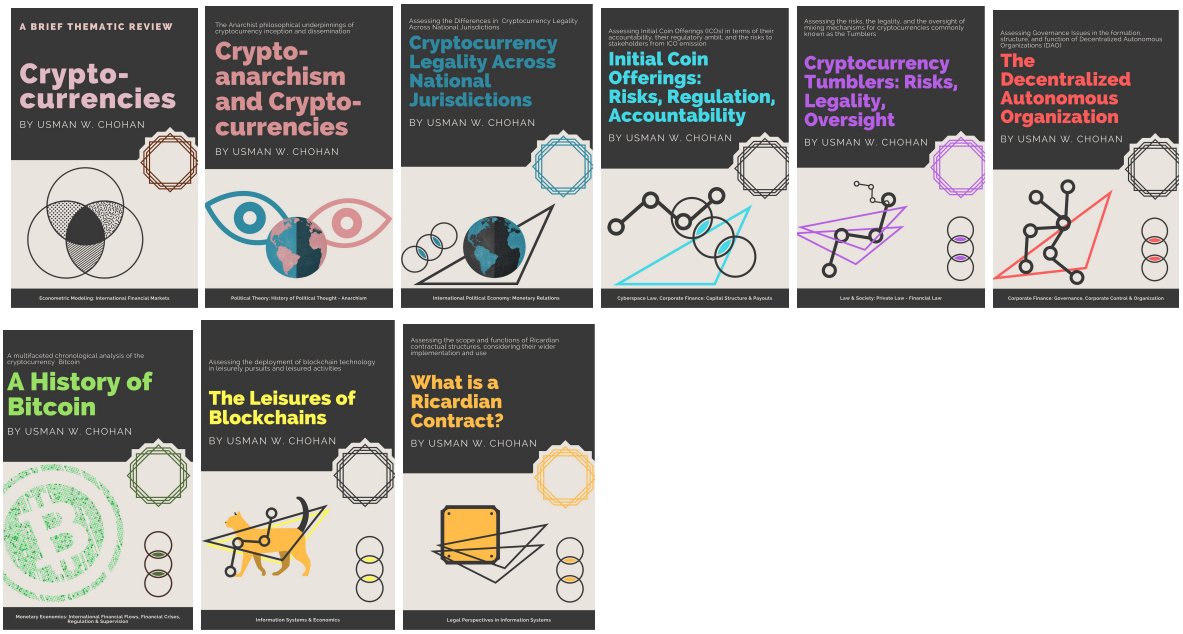
University of New South Wales, Canberra

Discussion Paper

Discussion Paper Series: *Notes on the 21st Century*

Abstract: At the core of the economic logic of cryptocurrencies lies the problem of surmounting the double-spending problem, which poses an accounting and accountability challenge that effective cryptocurrencies have sought to overcome. This discussion paper reviews the salient literature so as to better inform academic and practitioner inquiry on the double-spending problems in cryptocurrencies.

Also in this series available on **SSRN**:



The Double-Spending Problem and Cryptocurrencies

At the core of the economic logic of cryptocurrencies lies the problem of surmounting the double-spending problem, which poses an accounting and accountability challenge that effective cryptocurrencies have sought to overcome (see also discussions in Decourt et al., 2017; Chohan 2017a, 2017b, 2017c, 2017d, 2017e, 2017f, 2017g, 2017h, 2017i, 2017j). This discussion paper reviews the salient literature so as to better inform academic and practitioner inquiry on the double-spending problems in cryptocurrencies with a slight bent towards governance & accountability issues (see also governance & accountability discussions in Chohan 2017k, 2017l, 2017m, 2017n), because as Karame et al. (2015) note, serious accountability issues are raised by the "misbehaviour in Bitcoin." For the purposes of definition, the **double spending problem** is a potential flaw in a cryptocurrency or other digital cash scheme whereby the same single digital token can be spent more than once, and this is possible because a digital token consists of a digital file that can be duplicated or falsified. The originator of Bitcoin, Satoshi Nakamoto, was keenly attuned to the double spending problem, and included it in the seminal white paper which outlined the deployment of Bitcoin (2008). Therefore, the double spending problem raises questions about the protection of digital currency in the same way that traditional currencies are to be protected from fraud or counterfeit, with a subjacent accountability issues in the protection of digital information. As Rosenfeld (2014) notes "While the qualitative nature of this system is well understood, there is widespread confusion about its quantitative aspects and how they relate to attack vectors and their countermeasures." Analogously to counterfeit traditional money, the double spending problem exerts an inflationary pressure by creating a new supply of fraudulent

currency that hadn't previously existed, thereby debasing the digital currency's value relative to the general price level (or other monetary units of comparison). In turn, this compromises the governance and accountability associated with user trust in the currency, and can jeopardize user willingness to retain the currency, which can deter the circulation of the currency supply. To combat this double spending problem, various cryptographic techniques can and are deployed, which form part of the literature review of this discussion paper. The originator of Bitcoin, Satoshi Nakamoto, was keenly attuned to the double spending problem, and included it in the seminal white paper which outlined the deployment of Bitcoin (2008), indicating that it could be resolved "solved using a P2P distributed timestamp server to generate computational proof of the chronological order of transactions." However, as far back as 1993, Brands outlined a method for cryptographic processes known as *restrictive blind signatures*, which forms the backbone for the cryptocurrency gamut. After contrasting the one-show blind signatures with the method of wallets with observers, he postulated restrictive blind signatures "in conjunction with the so-called representation problem in groups of prime order" which would give rise "to highly efficient off-line cash systems that can be extended at virtually no extra cost to wallets with observers under the most stringent of privacy requirements. The workload for the observer is so small that it can be performed by a tamper-resistant smart card capable of performing the Schnorr identification scheme" (Brands 1993). Ferguson (1993) stressed that, instead of using many terms, each for a single bit of the challenge, a better system would use a single term for a large number of possible challenges, and so instead of using a withdrawal protocol with cut-and-choose methodology as with earlier systems, a better system would use a direct construction. Medvinsky et al. (1993), while postulating electronic cash ("Netcash") emphasized the need for robust access protocols in

such architecture. Krsul et al. (1998) patented a method of electronic payments that would counter the double spending problem by introducing “A method of generating electronic monetary tokens” wherein the creation of every “electronic token halves by a financial services provider and begins in response to a request from a buyer to generate electronic monetary tokens to be used with an identified seller.” In this process, the financial services provider would “generate a multiplicity of electronic monetary token” and then “split each electronic monetary token into two electronic token halves and associates with each the same serial number,” (Krsul et al., 1998). These electronic token halves, when combined, would recreate the electronic monetary token from which they were generated, but themselves neither electronic token half would have any value, nor could either electronic half by itself be used to create the electronic monetary token without the token half's mate. After distributing the halves among the buyer and seller parties, it would be possible for the buyer and seller to engage in multiple transactions off-line of the financial services provider (Krsul et al., 1998). Around this time, Pointcheval et al., in the *Journal of Cryptology*, recognized that a cryptographic algorithm that can withstand cryptanalytic attacks for several years is often considered as a kind of validation procedure, but that “a much more convincing line of research has tried to provide ‘provable’ security for cryptographic protocols,” even as provable security came at an efficiency cost (2000), which is why they proposed a focus on concrete cryptographic objects, such as hash functions, with ideal random objects and to use arguments from relativized complexity theory, which is known as the “random oracle model” and was driven by hard algorithmic problems such as factorization or the discrete logarithm. Pointcheval et al. (2000) offered security arguments for a large class of known signature schemes, looking in particular at the security of blind signatures (in use today), which they argued were “the most important

ingredient for anonymity in off-line electronic cash systems," with the focus being on "an appropriate notion of security related to the setting of electronic cash."

Karame et al. studied the double-spending problem in the context of Bitcoin specifically, and noted correctly that "the Bitcoin payment verification scheme is designed to prevent double-spending, our results show that the system requires tens of minutes to verify a transaction and is therefore inappropriate for fast payments" (2012a, 2012b). This problem is, as of this writing, highly accentuated by the extremely high pressure on the bandwidth of the Bitcoin network (Chohan 2017a-d). Karame et al., also found in the course of their research that, unless appropriate detection techniques were integrated in the Bitcoin implementation architecture, "double-spending attacks on fast payments succeed with overwhelming probability and can be mounted at low cost," (2012a, 2012b), and as a corollary "measures recommended by Bitcoin developers for the use of Bitcoin in fast payments are not always effective in detecting double-spending", which is why even if their recommendations were integrated in future Bitcoin implementations (as they have), "double-spending attacks on Bitcoin will still be possible" (Karame et al., 2012a, 2012b). Rosenfeld correctly observed that "While the qualitative nature of this system is well understood, there is widespread confusion about its quantitative aspects and how they relate to attack vectors and their countermeasures," and so attempted to outline and detail the stochastic processes underlying typical attacks and their resulting probabilities of success (2014). Karame et al. (2015) conducted an important study of the "misbehaviour in Bitcoin," pointing out the accountability issues that arose therefrom. As they note, "unavoidably, in such a setting, the security of transactions comes at odds with transaction privacy. Motivated by the fact that transaction confirmation in Bitcoin requires tens of minutes," [which as of this writing has extended to 4-6

hours for confirmation, see also Chohan 2017a-f], they analyzed the conditions for performing successful double-spending attacks against fast payments in Bitcoin, where the time between the exchange of currency and goods is short, arguing that “unless new detection techniques are integrated in the Bitcoin implementation, double-spending attacks on fast payments succeed with considerable probability and can be mounted at low cost,” which is why they proposed a “new and lightweight countermeasure that enables the detection of double-spending attacks in fast transactions.” Their most important insight was that, in light of misbehavior, “accountability becomes crucial,” and that in the specific case of Bitcoin, “accountability complements privacy,” (Karame et al., 2015). This discussion paper launches from this point of departure in stressing accountability in bitcoin as one of the important underexplored facets of Bitcoin and Cryptocurrencies more generally (see Chohan 2017a-m), emphasizing that future literature on cryptocurrencies must seek to incorporate a greater amount of accountability-oriented thought. The double spending problem helps illustrate one of the fundamental problems that cryptocurrencies have sought to overcome, and two decades of literature have elucidated various means of doing so, but the stress on accountability is one front where future research must lay greater emphasis.

References

1. Brands, S. (1993, August). Untraceable off-line cash in wallet with observers. In *Annual International Cryptology Conference* (pp. 302-318). Springer, Berlin, Heidelberg.
2. Chohan, U.W. (2017a). Cryptocurrencies: A Brief Thematic Review. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330
3. Chohan, U.W. (2017b).Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042248
4. Chohan, U.W. (2017c). A History of Bitcoin. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875
5. Chohan, U.W. (2017d). Cryptoanarchism and Cryptocurrencies. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3079241
6. Chohan, U.W. (2017e). Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080098
7. Chohan, U.W. (2017f). The Cryptocurrency Tumblers: Risks, Legality and Oversight. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361
8. Chohan, U.W. (2017g). The Decentralized Autonomous Organization and Governance Issues. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055
9. Chohan, U.W. (2017h). The Leisures of Blockchains: Exploratory Analysis. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3084411
10. Chohan, U.W. (2017i). Blockchain and Securities Exchanges: Australian Case Study. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085631
11. Chohan, U.W. (2017j). What is a Ricardian Contract? SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085682
12. Decourt, R.F.; Chohan, U.W.; Perugini, M.L. (2017). "Bitcoin returns and the Monday Effect." *Conference Proceedings of the 14th Convibra: Administração (Brazil).* November. http://www.convibra.com.br/upload/paper/2017/33/2017_33_14675.pdf

13. Ferguson, N. (1993, May). Single term off-line coins. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 318-328). Springer, Berlin, Heidelberg.
14. Krsul, I. V., Mudge, J. C., & Demers, A. J. (1998). *U.S. Patent No. 5,839,119*. Washington, DC: U.S. Patent and Trademark Office.
15. Karame, G. O., Androulaki, E., & Capkun, S. (2012a, October). Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 906-917). ACM.
16. Karame, G., Androulaki, E., & Capkun, S. (2012b). Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. *IACR Cryptology ePrint Archive*, *2012*(248).
17. Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Čapkun, S. (2015). Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC)*, *18*(1), 2.
18. Medvinsky, G., & Neuman, C. (1993, December). NetCash: A design for practical electronic currency on the Internet. In *Proceedings of the 1st ACM conference on Computer and communications security* (pp. 102-106). ACM.
19. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
20. Pointcheval, D., & Stern, J. (1996). Provably secure blind signature schemes. In *Advances in Cryptology—ASIACRYPT'96* (pp. 252-265). Springer Berlin/Heidelberg.
21. Pointcheval, D., & Stern, J. (2000). Security arguments for digital signatures and blind signatures. *Journal of cryptology*, *13*(3), 361-396.
22. Rosenfeld, M. (2014). Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*.