The Double Spending Problem and Cryptocurrencies

6th January, 2021[1]

Usman W. Chohan, MBA, PhD

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.

---

[1] Originally posted on 19th December, 2017 to SSRN

The Double Spending Problem and Cryptocurrencies

Background

Cryptocurrencies are considered a novel monetary instrument in that they proceed from having resolved two fundamental mathematical problems: the *byzantine generals problem* (Lamport et al. 2019; Reischuk 1985; Driscoll et al. 2004), and the *double spending problem*. Both of these are significant achievements in terms of the design of a digital currency. This paper examines the latter double spending problem in greater detail. 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.

Evidently, the ability to spend a single currency in multiple locations would constitute a form of cheating that would collapse any workable system. This problem doesn't exist in traditional (physical) currencies because the transfer of an asset in exchange for money actually requires a physical exchange. However, the sending of a digital code to one person might not preclude someone from sending it to another and claiming a payment for both! This issue stymied many scholars, but as the latter part of this paper discusses, cryptocurrencies have overcome the problem and offered a novel mechanism for digital monetary exchange.

Indeed,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). The mathematical exploration of the white paper regarding the double

spending problem is highly instructive in terms of the advances that emerged through Bitcoin as well as subsequent cryptocurrencies.

Mechanism

Whenever transactions are recorded in a blockchain, once *z* blocks have been appended to the chain, attackers may try to regenerate a new strand of the blockchain. Putting this mathematically, if the honest chain is z blocks faster than an attack chain, and produces a new block in the chain's iteration in the next moment, then there is a distance of +1 between 2 chains. However, if the attacker's surrogate chain produces the new block instead, then the distance of the two chains is -1. In other words, there is a race between the attackers' chain and the honest chain, and if the attackers' surrogate chain works at a more rapid pace than the existing blockchain, then since Bitcoin protocol always selects the longest chain, the attackers will be able to regain the coins that they had spent earlier.

Drawing an analogy with the solution to the *Gambler's Ruin* problem (Kmet and Petkovsek 2002; Rocha and Stern 1999), Nakamoto (2008, p.6) omits the following mathematical proof but provides its solution,[2] such that:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Where:

p: is the probability that an honest node finds the next block,

q: is probability the attacker finds the next block,

---

[2] A detailed breakdown of the derivation of the proof is available here: DxChain (2018), A Deep Understanding of the Double-Spending Problem in Bitcoin. *Medium*.

λ: and the attacker's potential progress will be a Poisson distribution with expected value: $\lambda = z(q/p)$

Earlier Advances

However, as far back as 1993, Brands outlined a method for cryptographic processes known as restrictive blind signatures, which forms the backbone for the gamut of cryptocurrencies now available. 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 electronictoken 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."K arame 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 (Chohan2019a-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 ofBitcoin 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).

The Accounting & Accountability Issues

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 2019a-d], 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).

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 issue 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 users 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. As discussed above, Nakamoto, indicated that it could be resolved "solved using a P2P distributed timestamp server to generate computational proof of the chronological order of transaction," (2008).

As the domain of cryptocurrencies has grown enormously since the release of Nakamoto's whitepaper, the appreciation of the resolution to the byzantine generals problem and the double spending problem has at times been overlooked. Yet it was in the specific advancement of these mathematical challenges that Bitcoin and other cryptocurrencies brought something meaningful to light. However, Bitcoin's solution should also be seen in the context of earlier cryptographic advances, as this paper covers.

References

1. Brands, S. (1993, August). Untraceable off-line cash in wallet with observers. InAnnual International Cryptology Conference (pp. 302-318). Springer, Berlin,Heidelberg

2. Chatterjee, A., Pitroda, Y., & Parmar, M. (2020). Dynamic Role-Based Access Control for Decentralized Applications. *arXiv preprint arXiv:2002.05547*.

3. Chatterjee, K., Goharshady, A. K., & Pourdamghani, A. (2019, May). Probabilistic smart contracts: Secure randomness on the blockchain. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 403-412). IEEE.

4. Chatterjee, K., Goharshady, A. K., & Goharshady, E. K. (2019, April). The treewidth of smart contracts. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing* (pp. 400-408).

5. Chodhury, N. (2019). *Inside Blockchain, Bitcoin, and Cryptocurrencies*. CRC Press.

6. Chohan, U.W. (2019a). Cryptocurrencies and Inequality. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3322329

7. Chohan, U.W. (2019b). Oversight and Regulation of Cryptocurrencies: BitLicense.

8. Chohan, U.W. (2019c). Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. *Cryptocurrencies and Mechanisms of Exchange*. Springer.

9. Chohan, U.W. (2019d). Are Cryptocurrencies Truly Trustless? *Cryptocurrencies and Mechanisms of Exchange*. Springer.

1. Chohan, U.W. (2019e). Are Stable Coins Stable? https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326823

10. Chuen, D. L. K., Guo, L., & Wang, Y. (2017). Cryptocurrency: A new investment opportunity?. *The Journal of Alternative Investments*, *20*(3), 16-40.

11. Ciatto, G., Calegari, R., Mariani, S., Denti, E., & Omicini, A. (2018, June). From the Blockchain to Logic Programming and Back: Research Perspectives. In *WOA* (pp. 69-74).

12. Чахова, Д. А., & Кошелева, А. И. (2018). Проблемы и перспективы развития блокчейн-туризма в регионах РФ (на примере Калужской области). *Региональная экономика и управление: электронный научный журнал*, (2018-53).

13. 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

14. Driscoll, K., Hall, B., Paulitsch, M., Zumsteg, P., & Sivencrona, H. (2004, October). The real byzantine generals. In *The 23rd Digital*

    Avionics Systems Conference (IEEE Cat. No. 04CH37576) (Vol. 2, pp. 6-D).
    IEEE.
15. DxChain (2018), A Deep Understanding of the Double-Spending Problem in
    Bitcoin. *Medium*.
16. Ferguson, N. (1993, May). Single term off-line coins. In Workshop on the
    Theory andApplication of of Cryptographic Techniques (pp. 318-328).
    Springer, Berlin,Heidelberg.
17. 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.
18. Karame, G., Androulaki, E., & Capkun, S. (2012b). Two Bitcoins at the
    Price of One?Double-Spending Attacks on Fast Payments in Bitcoin. IACR
    Cryptology ePrintArchive, 2012(248).
19. Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Čapkun, S.
    (2015).Misbehavior in bitcoin: A study of double-spending and
    accountability. ACMTransactions on Information and System Security
    (TISSEC), 18(1), 2.
20. Kmet, A., & Petkovšek, M. (2002). Gambler's ruin problem in several
    dimensions. *Advances in applied Mathematics*, *28*(2), 107-118.
21. 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.
22. Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals
    problem. In *Concurrency: the Works of Leslie Lamport* (pp. 203-226).
23. Medvinsky, G., & Neuman, C. (1993, December). NetCash: A design for
    practical electronic currency on the Internet. In Proceedings of the 1st
    ACM conference onComputer and communications security (pp. 102-106).
    ACM.
24. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
25. Pointcheval, D., & Stern, J. (1996). Provably secure blind signature
    schemes. InAdvances in Cryptology—ASIACRYPT'96 (pp. 252-265). Springer
    Berlin/Heidelberg.
26. Pointcheval, D., & Stern, J. (2000). Security arguments for digital
    signatures andblind signatures. Journal of cryptology, 13(3), 361-396.
27. Poupko, O., Shapiro, E., & Talmon, N. (2020). Fault-tolerant distributed
    implementation of digital social contracts. *arXiv preprint
    arXiv:2006.01029*.
28. Reischuk, R. (1985). A new solution for the Byzantine generals problem.
    Information and Control, *64*(1-3), 23-42.
29. Rocha, A. L., & Stern, F. (1999). The gambler's ruin problem with n
    players and asymmetric play. *Statistics & probability letters*, *44*(1),
    87-95.
30. Rosenfeld, M. (2014). Analysis of hashrate-based double spending. arXiv
    preprintarXiv:1402.2009.
31. Silvano, W. F., & Marcelino, R. (2020). Iota Tangle: A cryptocurrency to
    communicate Internet-of-Things data. *Future Generation Computer Systems*,
    112, 307-319.