Near Zero Bitcoin Transaction Fees Cannot Last Forever

Kerem Kaşkaloğlu
Özyeğin University
Istanbul, Turkey
kerem.kaskaloglu@ozyegin.edu.tr

ABSTRACT

Under Bitcoin protocol and payment scheme, anyone can send any amount of bitcoins that he owns to anywhere in the world via internet, near instantly for near zero fees. While the popular crypto-currency enjoys low transaction fees, a feature that is highly promoted and is working fine for the current state of the Bitcoin ecosystem, we argue that in an unforeseeable future, zero or infinitesimal transaction fees will not be sustainable. We apply a financial reasoning via depicting the interrelation of fees with mining, securing the network against 51% attacks, scarcity of supplies and the price of bitcoin, which in addition are the essential parameters involved in the problem of setting the right transaction fee in the future that we briefly discuss.

KEYWORDS

Bitcoin, crypto-currency, crypto-economics, transaction, fee.

1 AN OVERVIEW OF BITCOIN

Bitcoin[1] is invented in late 2008 [1] and launched in 2009. Since then it slowly gained popularity and strong media attention lately in 2013 and 2014 as well as drawing attention of academics.

The implications of Bitcoin are huge. Various experts, politicians, groups and people in general public react differently to Bitcoin. There are harsh criticisms mostly from financial professionals such as [2] and in general it is regarded as "*highly risky*" as an instrument of investment, as in [3]. The payment processing and money transfer companies and even banks as a means of storing and transferring value are in the obvious group of direct competition and have the risk to be outpaced in the long run if Bitcoin functions as it is supposed to be and if the surrounding services around Bitcoin prove to be useful. We do not intent to scrutinize the controversial aspects such as whether Bitcoin satisfies the often loosely-defined attributes of a 'currency' regarding acceptance of general public.

Although Bitcoin is intended to be a peer-to-peer digital currency, it is currently quite risky to store and use Bitcoin on a device connected to internet as it requires a tremendous amount of precautions such as managing backups, and preferably some encryption for safeguarding in order not to be target of hackers and not to lose bitcoins. Such factors are argued to make Bitcoin not necessarily suitable for an average user so that one needs to be tech-savvy or trust third parties to store her bitcoins. On the other hand, about 45% of the online exchanges are reported to fail and in the current mainly unregulated and possibly premature phase of Bitcoin, exchange sites should be used with high caution as warned in [4].

Regulations for recognition of Bitcoin as a means of storing and transferring value[2] as well

[1] The general consensus is to write Bitcoin (singular with an upper case letter B) to label the protocol, software, and community, and bitcoins (with a lower case b) or BTC to label units of the currency.

[2] New York State regulating bitcoin exchanges and FEC approving bitcoin donations on political parties in the US

as well as recently introduced innovative features such as multisignatures embedded in the latest versions of the client software allows third parties to offer a more secure framework such that now it is more feasible to offer a 2-stage (or n-stage) approval before spending bitcoins.

It is worthwhile to note that Bitcoin is seen by many industry professionals as in its early stages and in analogy with internet in 1990's[3]. The strength of Bitcoin comes from accomplishing a nontrivial task of running a distributed database called *block chain*. The block chain is kept on all nodes that run a software called *full Bitcoin client* or *bitcoin core*, which means that there is no single point of failure. The block chain contains every transaction ever occurred in the history of the currency. With this information, one can find out how many bitcoins belong to each address at any point in history. In about every 10 minutes, a new block is created and transactions occurring in that period of time are forever encapsulated within. The majority of the runners of Bitcoin protocol is supposedly determined via a practical solution of Byzantine Generals problem. Indeed for this reason, Bitcoin is sometimes promoted to be a "*consensus-driven"* currency, in analogy with democracy, rather than being imposed by a government, like fiat currencies such as US dollar or euro. The main purpose of all this cumbersome-looking structure along with its inefficiencies is to avoid the need of third parties such as banks, institutions whose main purpose of existence is to witness the balance of the accountholder.

The universal parameters of Bitcoin such as 21 million maximum number of bitcoins and the SHA256 hash function used for the protocol is unlikely to change as often stated by the core developers as a change of the 21 million cap would obviously lead to a major disruption and separation among bitcoin users and possibly a hard fork on the block chain. However, some other parameters or specifications of Bitcoin are subject to change and transaction fees may be one of them. Indeed we claim that such a change is inevitable for the reasons we argue in the rest of the paper[4].

The process called *mining*, in analogy with mining gold, has the following main purposes: distribution of wealth by the newly generated bitcoins, forming a backbone to process the transactions and securing the network. Technically, the procedure works via constant readjustments of a parameter called *difficulty*, working in a way that the higher combined hash power the network has, the higher the difficulty becomes so that the average duration a new block is found remains the same. Similarly, the lower the total hash power is, the lower the difficulty becomes, to adjust with the miners leaving the network. Any bitcoin that is in circulation for buying is one that is mined by some miner in the past. As which transactions are included in the next block of the block chain is supposedly decided by the majority of miners which in turn is determined by the majority of the hash power, the combined hash power provided by miners makes the so-called *51% attack* increasingly difficult, thus securing the network. Currently, mining hardware is provided by private companies producing special hardware called ASICs (Application Specific Integrated Circuits) designed specifically for fast SHA256 calculations and an industry with numerous competitors are born. It is the hash power the individual

---

are some of the recent political progressions as of the time of writing the manuscript.

[3] Among various informal events and meetups, one may consider: S. Neville, Presentation, MIT's Premier Bitcoin Expo, http://www.mitbitcoinexpo.org, May, 2014.

[4] The issue is often disregarded by the general public though it is occasionally mentioned for a while in online discussion forums such as https://bitcointalk.org/index.php?topic=3118.msg44789#msg44789

operates, either directly under his control or indirectly through operating a *mining pool*. The pool operator controls the total hash power of the members and distributes the wealth obtained by *block rewards* to the members proportionally. More hash power in the possession of individual essentially means higher number of lottery tickets for winning the prize offered every 10 minutes. Block rewards and transaction fees collected from the current block actually have a special name such as *coinbase transactions.* Coinbase transactions always contain outputs totaling the sum of the block reward plus all transaction fees collected from the other transactions in the same block. Each subsequent block over the block that involves the transaction an individual sends is counted as a *confirmation*, towards the acceptance of the transaction. Each confirmation exponentially decreases the possibility that the transaction will be rejected by the network [1].

For a more comprehensive coverage about how Bitcoin works, many sources such as [5] exist and for known weaknesses of Bitcoin, we refer the reader to [6]. As we introduced some key terms of the basic Bitcoin terminology to the unfamiliar reader in sec.1, we will briefly consider the parameters interrelated with the transaction fees in sec.2. In sec.3, after investigating the relationship between transaction fees and price of a bitcoin, we explain that it is early to set transaction fees other than donations in the current premature environmental conjecture and discuss the problem of setting the right transaction fee in the future as we give a sketch of the ideal case as a minor contribution. Some endnotes are given in sec.4.

2 TRANSACTION FEES

From the official online documentation of bitcoin:

> *"At the moment, many transactions are typically processed in a way where no fee is expected at all, but for transactions which draw coins from many bitcoin addresses and therefore have a large data size, a small transaction fee is usually expected.''*

The current identification is "*donation"* rather than *"fee"*. Nevertheless, the current convention of exchange sites is to impose the user a tiny *"mandatory donation"* which goes to miners and enables the user to avoid from the possibility that the user's transaction is not included in the next block and is not kept delayed in the network until some miner accepts processing it, although a fee as of the time of writing this article is typically not necessary for the transaction to be transmitted. We argue in this paper that donations are financially unsustainable in the long term for bitcoin transactions.

2.1 51% Attack

Actually, the hash power that miners provide does not really do any good per se for Bitcoin to function properly. However, it is the cost of the mining hardware required that disallows a third party to accomplish a 51% attack. This is actually one of the vague parameters of the picture as we are oblivious to the cost that the unknown malicious attacker is willing to pay. There are estimates about the cost of hardware to be bought to establish the attack typically in figures of billions of US dollars and the network is sometimes interpreted to be overly-protected. Essentially, we will refer to *the cost of a 51% attack* as a highly speculative parameter.

Another aspect is that, the 51% attack, being somewhat a misnomer, does not necessarily require the 51% of the total hash power of the network. There is research going on about the minimum percentage of hash power required to establish such an attack but the chance that the

attack succeeds decline dramatically for lower percentages close to 25%. A starting point for related recent research might be [7]. For a game theoretical investigation, we refer the reader to [8,9] and about the detection of the attacker to [10].

Other considerations are that, the 51% attack does not show up in the block chain so that even if it is accomplished, the block chain does not really require a manual cleanup by the core developers. The attacker will be in control for a temporary period of time, and in that period, he can interfere with transactions in such a way that he can prevent them from gaining any confirmations and can perform a so-called *double spend attack* [11], but the attacker cannot reverse other users' transactions forever and cannot prevent transactions from being sent at all (they will show as 0/unconfirmed). Most importantly, the adversary cannot change specifications of the protocol, cannot create coins out of thin air, cannot send coins that never belonged to him and cannot steal somebody else's coins.

The aforementioned double spend attack is a type of counterfeit that is in analogy with that of physical currencies such as US dollar. It may be argued that a currency does not have to be perfect to be practical. US dollar actually has a serious counterfeit rate and many small merchants in the US do not accept 100$ bills for that reason. But this does not stop the general public from using US dollar even outside of the mainland. Similarly, one may argue that an occasional double spend attack may not kill Bitcoin as it is in a loose analogy with counterfeit bills. However, such attacks should be prevented as much as possible and the way this works is the network having a large enough total hash rate and an incentive for miners to provide so. Actually, the reason why users of the system are encouraged to wait for enough many confirmations that are ideally proportional to the amount of BTC they are receiving is given as a precaution in [1] is the possibility of 51% attacks. The likelihood of a 51% attack is also highly related with centralization of mining pools, which is regarded as 'disturbing', and 'dangerous' by the Bitcoin community. That is, in case of mining, pools are focus of attention as possible sources of attacks as briefly considered in [12]. We are ready to consider the problem[5],

> *"The relevance to Bitcoin is a hypothetical market failure that might happen in the far future when the block reward from mining drops near zero. In the current Bitcoin design, the only fees miners earn at this time are Transaction fees. Miners will accept transactions with any fees (because the marginal cost of including them is minimal) and users will pay lower and lower fees. It is possible that the honest miners will be under-incentivized, and that too few miners will mine, resulting in lower difficulty than what the public desires. This might mean various 51% attacks will happen frequently, and the Bitcoin will not function correctly.''*

Imposing a transaction fee is essentially tax revenue of the service provided by the miners. As more hash power that the miner pours in means a more secure network, it is reasonable that the reward of the miner is proportional to the hash power he contributes. However, how users should be charged is not as clear as how the wealth should be collected by the miners. Indeed, determining the right transaction fee as a policy and forcing it in the client software as a regulation is crucial for the future of Bitcoin and similar alternative crypto-currencies. The problem of determining the optimum transaction fees are interrelated with various surrounding aspects.

[5] The problem takes place in the official Bitcoin wiki as of June 2014: https://en.bitcoin.it/wiki/Tragedy_of_the_Commons

2.2 Trade-Off of Supporting Small or Large Transactions

Statistically speaking, the number of transactions per second (tps) of Bitcoin increases over time[6], as well as the wealth carried by the transactions. That is, in the early days of Bitcoin, users usually experimented the protocol by smaller transactions, whereas today, the average value contained in a transaction is significantly higher.

Although the idea that transaction fees should be proportional to the amount of bitcoins transferred would be quite disruptive among some bitcoin users, economically, this is plausible in the sense that the users transferring the largest amount of bitcoins are the individuals that have the most benefit of Bitcoin. This is obvious especially when one considers the daily transaction limits imposed by governments and banks. Such limits, varying by the monetary policy of the country that one lives in, are actually one of the reasons Bitcoin drives so much attention because Bitcoin allows one to simply exceed such limits. That is, there is no transfer limit on Bitcoin protocol imposed by any third party and this is one of the promoted features. It is not uncommon to see transactions in millions of US dollars[7].

On the other side, Bitcoin is currently promoted as the best transfer method for transactions carrying tiny amounts, often regarded as *micro-transactions*. This means that paying a certain fixed minimal fee (such as in magnitude of cents) for each transaction may hinder some possible future usage scenarios of Bitcoin, such as tipping online content providers (videos, forum answers etc.). Regarding this, there are discussions in the community that micro-transactions can be taken off the block chain into newly discussed structures called *side-chains*. However, more research on the topic seems to be required to determine how such a shift from the main block chain would function. Private exchange and online wallet companies may also help providing such a service[8] at the cost of centralization of the transactions.

3 TRANSACTION FEES AND BITCOIN PRICE

The transaction fees and bitcoin price are related as follows. First of all, the supply of new bitcoins is only through the block rewards for miners. There is a periodic halving in the block reward, resulting in a logarithmic supply of wealth, decreasing gradually over time as in monetary base, figure 1. The reason why a linear supply is not offered is to avoid inflation. As no central authority is present, there is no government to mint money. Although the network is still in a temporary low-inflation state, Bitcoin is eventually meant to be deflationary. Currently, there are about 12.5 million bitcoins in circulation as of 2014. In 2033, this number is expected to exceed 20 million and increase slightly each year thereafter until 2140. Such a logarithmic supply of the number of bitcoins in circulation as part of the design is the inflation to diminish shortly after the initial launch[9]. The relation of number of blocks issued at any time (in correlation with time) and the inflation of bitcoins is also illustrated in figure 1. As mentioned before, this inflation of supply is to be replaced by a deflation soon after a point when the accidentally lost bitcoins outnumber the newly minted ones.

[6] Number of transactions per second (tps) currently Bitcoin handles as of the time of this manuscript is about 1 tps, which is significantly higher than 0.2 tps of the last year, same month. source: https://blockchain.info/charts

[7] By the time of the manuscript, the largest known transaction is $147 million worth of bitcoins in 2013.

[8] Currently "Coinbase", a major online bitcoin wallet company, claim to offer zero-fee micro-transactions off the block chain, a service which appears to be the first among online wallets.

[9] As of the time of the manuscript, block 300 is recently issued, indicating the current point in figure 1.

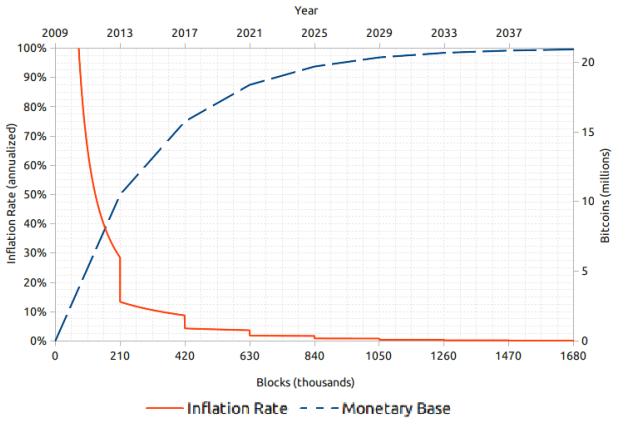

Figure 1. *bitcoin inflation vs. time.*

One may argue that the significant scarcity in the supply of bitcoins might not affect the incentive of miners as the lesser amounts of bitcoins rewarded carry higher and higher value in price as the price of bitcoin dramatically increases over time. In other words, to numerically exemplify, for the price to keep up with the incentive of miners, the tens of thousands of bitcoins produced each year after 2030 should have the same price with the millions of bitcoins produced each year now. However, this assumption cannot be correct. Although it is true that until now the price of a bitcoin has increased dramatically[10], this cannot last forever as even the most optimistic prediction about continuation of price rice involves a slow down after half way as the number of potential users that may adopt Bitcoin in the globe is limited.

Theoretically, the best case scenario about adoption of Bitcoin as a technology is the logistic growth as depicted in figure 2. The graph may arguably apply to both the price of a bitcoin and also the number of users of bitcoin. Actually, these two parameters are correlated as the price of bitcoin is determined by the demand and the limited supply. The increasing demand that emerges from an increasing number of users together with a limited supply naturally causes the price to rise.

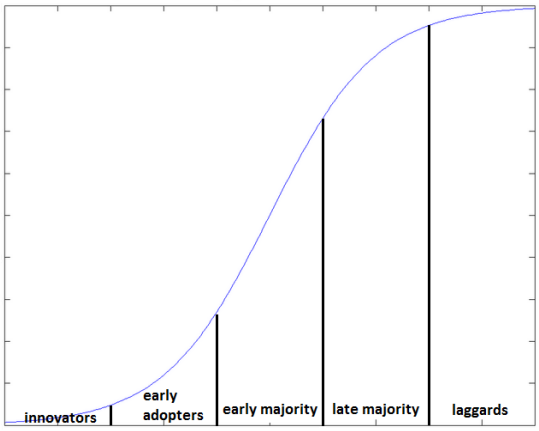

Figure 2. *hypothetical best-case adoption.*

On the other hand, in financial terms, the limited supply over time and the eventual limit on the price of a bitcoin have a combined effect such that the marginal production cost of mining is going to increase dramatically, which must instead be set fairly constant over time.

In the long run, the policy on transaction fees should be set so that enough many miners have incentive to run clients having a good enough combined hash power to protect the network. But on the other side of the coin, the fees that miners collect should not be any higher than sufficient in order not to discourage users from using Bitcoin as a means of transferring money.

3.1 Various Aspects of Securing the Bitcoin Network

Miners with sufficient combined hash power are not the only requirement to secure the network. Another aspect is the number of full nodes, which have a similar level of importance. Full nodes are actually quite "smart" at running the network as they provide lookup of historic blocks, which is necessary for new nodes synchronizing, and they also validate blocks and transactions, and relay them. As the network right now is under trivial load, we do not exactly know how many full

[10] By the time of this text, the price of a bitcoin is $580, whereas in 2010, a bitcoin had no value.

nodes are going to be needed in the future and this is one of the open question requiring further empirical studies. The number of full nodes in the globe dramatically decreases over time and end-users tend to switch to easy-to-run lightweight clients that are intended for personal usage instead of full nodes. However, the exchange and wallet services and other similar service providers will still have to run a full Bitcoin client, and the number of such services tends to increase over time and the indeed full nodes provided by these services only might suffice.

We claim that the solution of setting the right transaction fee in the future is not trivial, and a fixed number (such as $0.41 per transaction) mentioned by a core developer of Bitcoin [13], as a study for cost per transaction, do not apply as a transaction fee right now as the block rewards are currently good enough to keep a sufficient number of miners provide a good amount of hash power to secure the network. The transaction fees collected as donations from each block is a mere fraction of the block reward[11] and this is good enough.

Currently, Bitcoin nodes have the option to exclude transactions that do not donate. In general, there are interesting related technical trade-offs because of the structure of the Bitcoin protocol such as: the more transactions a miner include, the more his reward increases but also his probability to earn any reward decreases because the time needed for his block to reach consensus depends on its size due to network propagation.

3.2 Some Simple Approaches for Setting a Transaction Fee

As mentioned before, fixing the transaction fee and requiring the same small amount such as in [13] would make micro-transactions under that amount too expensive to process.

Limiting the maximum block size so that the maximum number of transactions per block is capped has its own inconveniences. The underlying idea in such an approach is that it makes the number of transactions that can be included so scarce that the ones providing fees under a certain threshold might not reach destination or might face serious delays. Indeed this threshold will be a dynamic one depending on the instantaneous traffic of transactions so that the sender will not be able to figure out whether her transaction will be delayed or not in advance. It is also interesting to note that, [14], in a simplified setting, forcing a mandatory fixed transaction fee is considered to be equivalent to limiting the block size and letting the price per block space be determined on a transaction market as the latter creates scarcity of the space in block chain thus creating a tax-source for miners.

3.3 Ideal Case

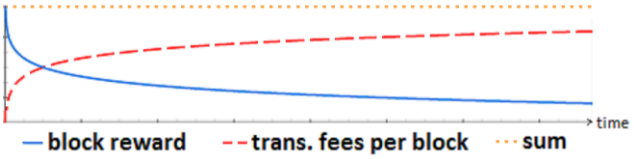

Figure 3. *block reward vs transaction fees*

Figure 3 depicts the case where the sum of block reward and the average transaction fees collected per block remains constant. What it means is that the total transaction fees collected from a block will have to rise up when the price rise of bitcoin slows down to a level that it no longer tolerates the diminishing block rewards occurring inherently in the protocol. If and when someday the price per bitcoin stabilizes to a constant value that is comparable to a fiat currency such as US dollar, then figure 3 describes *the ideal case where the sum of all*

[11] Daily transaction fees collected is about $5000 worth of BTC, where the total block rewards per day constitutes around $2.000.000, resulting in a fraction of 0.0025 as of writing the manuscript. source: https://blockchain.info/charts

rewards per block becomes stable so that the incentive of mining no longer fluctuates and number of miners together with the protection level of the network stabilizes at some point as well. We are aware that the unlikeliness of an immediate occurrence of such a change-free Bitcoin ecosystem, and thus refrain from proposing a specific transaction fee setting methodology whether a percentage of the amount of BTC sent or a fixed fee plus a percentage, as any such attempt is likely to turn suboptimal shortly in this ever-changing dynamic conjectural world of Bitcoin parameters. Furthermore, we argue that together with the price rise, the incentive to mine and thus generate new bitcoins will be likely to suffice for the network to be secure enough to prevent most, if not all of the double spend attacks for a significant period of time[12].

We propose that the possible percentage cut as a transaction fee increases over time in a dynamical manner, to proportionally keep up with the gap of the block rewards and the constant sum as depicted in figure 3.

4 CONCLUSION

We essentially claim that an increase in transaction fees of Bitcoin is inevitable. For analogy, the services around us such as medication, food, accommodation and transportation all have certain costs and are run by fees but not donations. The reason why a mandatory percentage of transaction fees in Bitcoin protocol will eventually be necessary is highly related with the cost of mining and the so-called 51% attack that miners provide a protection against.

Because of the scarcity of bitcoins policy of Bitcoin protocol and the corresponding demand from its users as a necessary requirement of a currency, we claim that the descent in the increase of the number of bitcoins in circulation will eventually turn near zero transaction costs unfeasible after some point no matter what the price of a bitcoin rises up to. As this happens gradually, it is a daunting task to come up with an estimation about when the bitcoin transactions should be charged by 'fees' rather than 'donations'. The reason as we discuss throughout the paper is that the value of the block reward depends highly on the price of a bitcoin, which in turn is related with the adoption of Bitcoin, which in turn is quite a controversial issue that is hard to foresee. A curious estimate without a proof about when the necessity of setting some mandatory transaction fee as a percentage will be solid might be somewhere from 5 to 20 years or so depending on the adoption of Bitcoin.

We discuss the parameters affecting the problem of determining the right fee for bitcoin transactions by bringing together various aspects of the topic. We also consider how these parameters are changing in a dynamic ecosystem of miners, investors and users of Bitcoin network. If the volatility of bitcoin continues to descent and the adoption rate as well as price of one bitcoin stabilizes at some point, the number of miners will no longer fluctuate in correlation with the price of a bitcoin and we may then consider an ideal hypothetical sum of stable and fixed block rewards as described in figure 3.

We finally stress that the problem presented regarding transaction fees may not really require immediate action as securing the network through voluntary hash powers via the incentive of mining rewards is not likely to diminish in the short-term as the block reward halving occurs gradually over time and not instantly.

[12] As the small transaction fees are not currently recognized as a threat, since version 0.9.0 that is launched recently, Bitcoin client is promoted to offer smarter and smaller transaction fees.

5 REFERENCES

[1] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, 2008.

[2] B. P. Hanley, “The false premises and promises of Bitcoin”, Computational Engineering, Finance, and Science, 2013, arXiv:1312.2048.

[3] A. Chowdhury, “Is Bitcoin the 'Paris Hilton' of the currency world? Or are the early investors onto something that will make them rich?”, online manuscript, 2014.

[4] T. Moore, and N. Christin, “Beware the middleman: empirical analysis of Bitcoin-exchange risk”, Financial Cryptography and Data Security, LNCS 7859, pp. 25-33, 2013.

[5] A. M. Antonopoulos, “Bitcoinbook”, draft version, github public repository, 2014.

[6] https://en.bitcoin.it/wiki/Weaknesses, as of June, 2014.

[7] E. Heilman, “One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner”, online preprint, IACR, 2014.

[8] N. Houy, “The Bitcoin mining game”, SSRN, preprint, 2014.

[9] J. A. Kroll, I. C. Davey, and E. W. Felten, “The economics of Bitcoin mining, or Bitcoin in the presence of adversaries”, Proceedings of WEIS. vol. 2013, 2013.

[10] M. Herrmann, “Implementation, evaluation and detection of a double-spend-attack on Bitcoin”, Diss. Master Thesis ETH Zürich, 2012.

[11] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in Bitcoin”, Proceedings of the 2012 ACM conference on Computer and Communications Security, ACM, 2012.

[12] A. Gervais, G. Karame, S. Capkun, and V. Capkun, “Is Bitcoin a decentralized currency?”, online preprint, IACR, 2013.

[13] G. Andresen, “Back-of-the-envelope calculations for marginal cost of transactions”, online technical report.

[14] N. Houy, “The economics of Bitcoin transaction fees”, preprint, SSRN, 2014.