Bitcoin Disruption in Payments – Winners and Losers

Nikhil Malik, Manmohan Aseri, Param Vir Singh
Tepper School of Business, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213
{nmalik1, maseri, psidhu}@andrew.cmu.edu

Bitcoin is a cryptocurrency which allows financial transactions between users, independent of financial intermediaries such as a payment processing providers like Visa/Master Card. Bitcoin validates transactions through a distributed consensus mechanism which circumvents the need for a financial intermediary; this allows it to have potentially low transaction fees. Using a game theory model involving Bitcoin, traditional channels of verification, and users, we study how Bitcoin would disrupt the payments processing industry. There are a few subtle but important differences between the value propositions offered by Bitcoin and traditional channels. For example, post-transaction services (e.g., reversal of an unintended or fraudulent transaction), which are readily available on traditional channels are not present on Bitcoin. We show that owing to this difference, the presence of Bitcoin leads to a filtering effect - the proportion of transactions needing post-transactions services increases on the traditional channel in the presence of Bitcoin. Since it is costlier to process such transactions, the transaction fee charged by the traditional channel increases. We also find that Bitcoin pricing mechanism makes is more suitable for high value transactions as users compete fiercely to use its limited throughput. Developers have been investing significantly to increase capacity and achieve a solution that allows micro payments. We show limited throughput is not a technological shortcoming but a key property that keeps the platform stable. Overall, the transactions of small sizes, which are not suitable for Bitcoin and need to use Visa/Master Card, have to pay a higher transaction fee on the traditional channel in equilibrium. Therefore, paradoxically, even though Bitcoin increases competition in the payments processing industry, the users who need to process transactions through the traditional channels end up paying higher transaction fees.

Key words: Blockchain, Cryptocurrencies, Bitcoin, Visa, Game Theory.

1. Introduction

Blockchain is touted to be a technological revolution equivalent to the Internet (The Wall Street Journal 2018). In a nutshell, a blockchain is a distributed consensus protocol which enables a common ledger to be used for recording activities (e.g., transactions) and, therefore, removes the need of several intermediaries. This solution can be applied in a variety of settings (Bresnahan and Trajtenberg 1995), including the verification of financial transactions. In this paper, we focus on the application of blockchain in the verification of financial transactions.

Bitcoin is the first cryptocurrency that utilizes blockchain technology. Bitcoin uses cryptographic techniques to regulate the generation of bitcoins and validation of transactions among users. Bitcoin validates transactions through a clever design of distributed consensus – *proof of work*. The original premise behind Bitcoin was to reduce the transaction fees and enable micropayments through the removal of financial intermediaries. While Bitcoin has already started appearing as a viable alternative for processing financial transactions, with ubiquitous adoption it could potentially have a disruptive effect on the tradition players. Facing potential competition from Bitcoin, Visa and Master card have recently increased the transaction fees by 5% for purchasing Bitcoin using Visa and Master Card (TechCrunch 2018).

The emergence of Bitcoin as an alternative for processing financial transactions raises a number of interesting questions about the future of payments processing industry. Would it allow micro payments? How would Visa/Master Card react to the entry of Bitcoin? Finally, is the entry of Bitcoin, good or bad for the consumers? We specifically study transaction *pricing mechanism* and *irreversibility* that differ between Bitcoin and traditional alternatives to answer these questions.

Bitcoin's small throughput (3 transactions / sec) relative to a traditional payment network such as VISA (2000/sec) has often been cited as a key weakness. Unlike VISA, users on Bitcoin compete by offering high transaction fees in order get their transactions added on the chain faster. High transaction fees and large wait times have discouraged businesses from using Bitcoin as a mode of payment. Developers have been investing significantly in technological solutions - larger block sizes, efficient networks and *sharding* (Jordan 2018) to increase the blockchain capacity. Our model shows that limited throughput is not a technological shortcoming but a key property that keeps the platform stable. An overall low level of transaction fee collection would risk concentration of Bitcoin mining power into fewer hands and thus eroding the primary value proposition of decentralization.

Secondly, we analyze reversibility offered by traditional channel such as refunds and dispute resolution. For example, a user makes a transaction with a fraudulent online store. If s/he made the transaction through Visa she would get assistance to receive a refund. Creator of Bitcoin - Satoshi Nakamoto - had pointed out this cost of mediation in traditional payment networks as a problem (Nakamoto 2008). Early adopters and observers have since clamoured for Bitcoin and other cryptocurrencies to eliminate all such costs by creating disintermediated protocols. This leads to a filtering effect – low risk users that do not foresee need for reversing their transactions benefit by moving to Bitcoin. These users are subsidized by the remaining users on VISA/Master Card. As the transaction pool of Visa/Master card becomes riskier, they would raise transaction fees to account for the increased risk.

We model a sequential game between Bitcoin designer, traditional payment processing firm (VISA) and users. Overall we find that, contrary to the popular belief, in equilibrium, Bitcoin transaction fees would be so high that it would not be viable for small or micro payments. In fact, the entry of Bitcoin imposes a negative externality on small value transactions. Counterintuitively, the entry of Bitcoin, though increases competition for payment processing, would lead the traditional players to raise their transaction fees.

2. Bitcoin (Blockchain) Overview

Users wanting to perform financial transactions using a cryptocurrency[1] need verification for these transactions. These users represent the demand side of a blockchain. On the supply

[1] Bitcoin and cryptocurrency are used interchangeably in this paper.

side, we have cryptocurrency *miners* who provide the required verification and are rewarded by blockchain platform for that. At any point in time, there are several transactions waiting to be verified. For the sake of efficiency, the cryptocurrency protocol allows a block of several transactions to be verified together. However, most protocols have a limit on the size of such a block, referred to as *block-size*. Block size for Bitcoin is 1 Megabyte (equivalent to 2000-2500 transactions). A miner (verifier) selects a set of transactions from the pool of unverified transactions and creates a new block to be verified. After verifying the transactions in a block, the miner competes with other miners to append that block in the blockchain (the chain of all previous blocks) to receive the reward associated with the block. To successfully append the block in the blockchain, the miner needs to find the hash of the block, using something called *nonce*. However, not all nonces are acceptable, and finding the correct nonce is equivalent to guessing. Specifically, a nonce which results in the hash value of the block lower than a pre-specified number is acceptable. Figure 1[2] pictorially depicts a typical blockchain. The hash value of each block depends on (i) hash of the previous block, (ii) time-stamp, (iii) hash of transactions in the block, and (iv) nonce.

It is easy to see that more computing power deployed by a miner results in that miner being able to guess the correct nonce faster. Therefore, most blockchain protocols adjust the difficulty level of nonce-guessing in such a way that the average time taken to guess the correct nonce is fixed. This fixed block-time is required to allow sufficient time for propagating the block over the network of user nodes. For Bitcoin, the block-time is 10 minutes; thus, every 10 minutes only one block can be added in Bitcoin blockchain, on an average. Because of the reward associated with each block, several miners compete to verify these blocks. When a miner finds the correct nonce and adds the block in the blockchain,

[2] Source: `https://commons.wikimedia.org/wiki/File:Bitcoin_Block_Data.png`

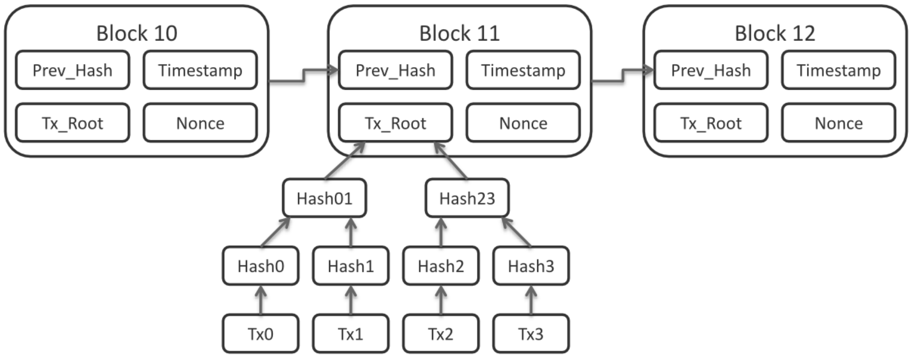

Figure 1 A typical blockchain: Only those blocks are acceptable whose hash value is lower than a pre-specified number. The corresponding value of nonce which results in such low hash value for the block is the correct nonce.

the update about the blockchain is broadcasted to all other miners. All other miners must now decide whether to race to add the next block on top of the old head of the blockchain or the new. They choose the latter if they consider the new block of transactions as valid. Any attempt by a dishonest miner to add blocks with incorrect transactions results in majority of honest miners to ignore their block and therefore keep it out of the single longest chain. Thus, any dishonest miner trying to add an incorrect transaction in the blockchain will have to possess atleast 51% of mining power. However, since the miners are competing, each miner procures a substantial amount of computational power. Thus, in such an ecosystem, procuring more than 51% of mining power is prohibitively expensive.

The reward for miners consist of the following two components:

- **Block reward:** A fixed number of cryptocurrency units, freshly created in the blockchain, are paid to the miner who adds the new block.
- **Transaction fees:** This is a fee decided by the user to be paid to the miner. A transaction with a higher fee is likely to be verified soon because miners are more incentivized to verify such transaction. Thus, they prefer to pick such transactions from the pool of unverified transactions, to create a new block.

Most cryptocurrency protocols are designed such that the fixed block reward decreases over time and vanishes eventually. Thus, in the long run, a cryptocurrency is expected to be entirely supported by transaction fees paid to miners.

Miners play the role of a financial intermediary. The community of anonymous miners gains trust by their lack of concentrated power. However, academic researchers and industry practitioners have questioned this. In practice, miners can form pools, and cryptocurrency mining is executed by a handful of mining pools, leading to the centralization of the blockchain. Recent work on dishonest attacks by mining pools that hold 51% or even minority computing power has shown weakness in face of collusion: see e.g., Sompolinsky and Zohar (2015), Nayak et al. (2016), Natoli and Gramoli (2017), Babaioff et al. (2012), Vasek et al. (2014), Eyal and Sirer (2014), and Courtois and Bahack (2014).

Cryptocurrency mining has also become a very expensive undertaking over time. Total bitcoin mining is estimated to consumed 30 TWh of electricity annually (Digiconomist 2018) or 0.13% of world's electricity. A body of research looks at alternate complex problems instead of cryptographic puzzles that have some positive social output to show the commitment of computing resources (O'Dwyer and Malone 2014, Miller et al. 2014). More recently industry practitioners have attempted to move away from the profligate mining altogether.

The concept of blockchain originally proposed in Nakamoto (2008) has attracted significant amount of attention in various academic disciplines. Goldfeder et al. (2017) show that in the presence of third-party trackers, users can be identified with sufficient accuracy. Da Conceição et al. (2018) propose a smart contract based data management architecture to address the conflicting objective of improving accessibility while maintaining privacy in electronic health records. Conti et al. (2018) provide a comprehensive survey on security and privacy issues in bitcoin.

The recent work has also addressed the economic issues in the blockchain ecosystem. Cong et al. (2018) model mining pool formation and analyze the forces acting in favor and against centralization. Biais et al. (2018) model the proof-of-work protocol as a stochastic game between miners and find that in equilibrium miners over-invest in computing capacity. Easley et al. (2017) explain how transaction fee emerges as an outcome of strategic behavior of users and miners. Bonneau (2018) analyze the stability of the consensus protocol against an attacker with a non-monetary objective. Kroll et al. (2013) argue that bitcoin will eventually need some regulation to survive the adversaries. Athey et al. (2016) model the adoption of bitcoin in the presence of high volatility in its exchange prices. Huberman et al. (2017) use queuing game to explain the equilibrium transaction fee. Ma et al. (2018) model bitcoin protocol as a dynamic game as an extension of model of R&D racing. Our work contributes to the literature by analyzing the impact of cryptocurrencies on users and traditional channels of verification. We model the key differences between Visa and cryptocurrencies to understand their adoption by users. The strategic reaction by Visa enables us to analyze the impact of cryptocurrencies on Visa. Our analysis leads us to make recommendations for a cryptocurrency designer.

3. Model

Let N represent the total number of users who want to perform some kind of transaction. Assuming that each user performs exactly one transaction per second, N transactions are needed to be verified per second. Let v represent the monetary value of a transaction. We assume that transactions are heterogeneous in terms of their value. Specifically, we assume that $v \sim U[0,V]$. We assume that α fraction of users need post-transaction services such as reversing an unintended transaction or disputing a fraudulent transaction. Thus, $\bar{\alpha} := 1-\alpha$ is the fraction of those transactions which do not require any post-transaction service. One should note that such services are typically not provided by a cryptocurrency.

We consider a cryptocurrency designer (e.g., the community of blockchain developers) who wants to decide the optimal capacity of the cryptocurrency.[3] Let S represent the number of transactions per second, which we refer to as the capacity of the cryptocurrency and decided by its designer. Let f_c represent the transaction fee charged by the cryptocurrency. Note that on Bitcoin a user decides what transaction fee he/she is willing to pay for her transaction to get processed. At the same time, the miners choose which transactions to include in their block to validate. High transaction fees generally get the transaction considered immediately whereas low transaction fees may not get the transaction considered for a very long time. Hence, f_c can be viewed as the minimum transaction fee to be paid by the user to get her transaction included in the current block. Unless specified otherwise, the units of all monetary quantities (e.g., transaction value, transaction fee etc.) are in USD.

A transaction that can be performed using a cryptocurrency can also be performed using a traditional verification channel such as Visa. Thus, we consider such a traditional verification channel, and without loss of generality we refer to this channel as *Visa*. The decision for Visa is to choose a transaction fee f_v. Consistent with the practice, we assume that this transaction fee is a fraction of the total value of the transaction, i.e., a transaction of value v will be charged a transaction fee of vf_v. We assume that the cost incurred by Visa to process a transaction of value v which needs (resp., does not need) post-transaction services is vC_h (resp., vC_l), where $C_h, C_l \geq 0$. We also assume that $C_h \geq C_l$ to reflect the idea that it is more costly to process a transaction which requires post-transaction services. Table 1 summarizes our main notation.

We setup the problem as a sequential game between (i) a cryptocurrency designer, (ii) Visa, and (iii) users. Figure 2 depicts the sequence of events of the game. Each user

[3] While a cryptocurrency designer decides the protocol rules (e.g., capacity) upfront, no person or entity has control over these settings once the platform is live.

Notation	Description
v	Monetary value of the transaction.
V	Maximum possible monetary value.
N	Total number of transactions per unit time.
f_c	Transaction fee charged by cryptocurrency.
f_v	Transaction fee charged by Visa (in percentage).
α	Fraction of transactions requiring post-transaction services. $\bar{\alpha} := 1 - \alpha$.
S	Number of transaction that can be verified per unit time.
C_h	Visa's cost of verifying transactions which need services later.
C_l	Visa's cost of verifying transactions which do not need services later.
m	Equilibrium number of miners.
C_m	Cost of mining.

Table 1 The main notation for our analysis

needs to make a choice between Visa and cryptocurrency to make its transaction. Since post-transaction services are only available on Visa, all the users requiring post-transaction services use Visa. We know that there are αN such users.

On the other hand, all those users who do not require any post-transaction service choose either Visa or cryptocurrency on the basis of transaction fee charged by each channel. A user, who does not need post-transaction services, will use cryptocurrency for making a transaction of value v if

$$v - f_c \geq v(1 - f_v)$$

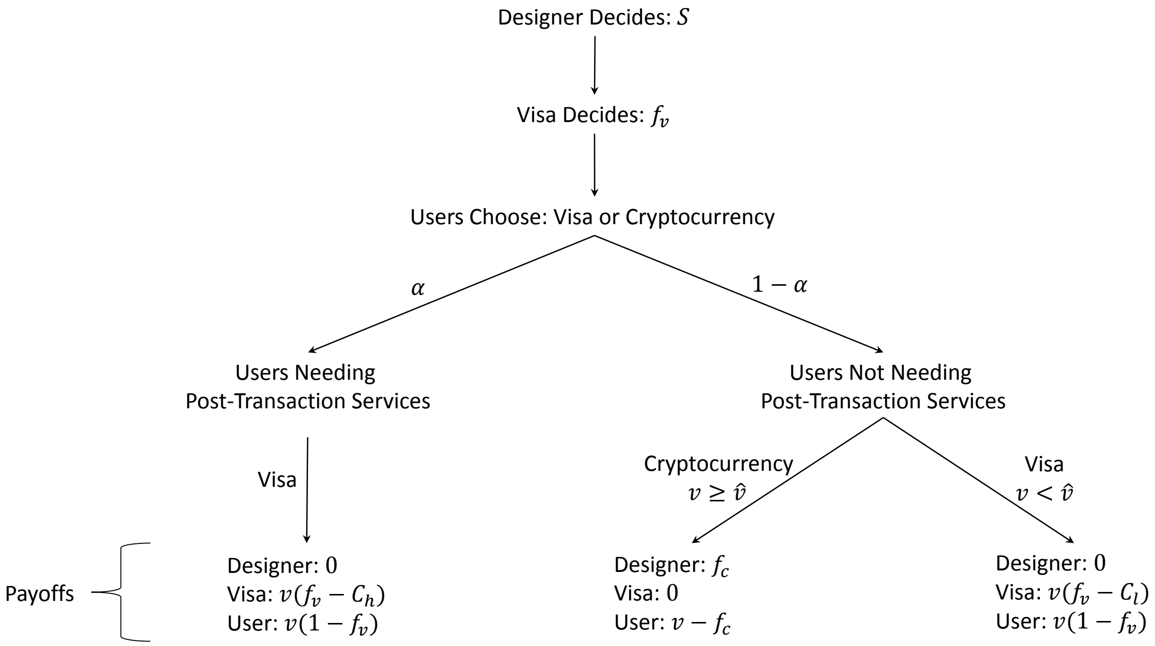

Figure 2 **The sequence of events of the game: First the cryptocurrency designer decides S. Then, Visa decides f_v and users of both types decide whether to use Visa or cryptocurrency for their transactions.**

or

$$v \geq \hat{v},$$

where $\hat{v} = \frac{f_c}{f_v}$.

An immediate consequence of the above analysis is that cryptocurrencies are suitable for high-value transactions ($v \geq \hat{v}$). This result is consistent with our observation that the average value of transactions in bitcoin is very high.[4] We formally state this result in the theorem below.

Theorem 1 *It is optimal for a transaction of value higher than $\hat{v}$ to use the cryptocurrency for verification. Thus, cryptocurrencies are suitable for transactions of high value.*

[4] `https://bitinfocharts.com/comparison/transactionvalue-btc.html`

Using the above analysis, it is easy to see that the demand for cryptocurrencies is $N\bar{\alpha}\left[1-\frac{f_c}{Vf_v}\right]$. We assume that the capacity of the cryptocurrency is less than the maximum demand for it. That is, $S \leq N\bar{\alpha}$. We use the solution concept of *rational-expectations equilibrium* to obtain the equilibrium transaction fee f_c for the cryptocurrency. Thus, users *rationally* anticipate the transaction fee f_c and make their decisions. When all the users make their decision in this manner, an equilibrium transaction fee f_c is realized, which is consistent with the transaction fee anticipated by all the users. Since the cryptocurrency system cannot process more than S transactions per unit time, it adjusts the transactions fee f_c such that it attracts only as many transactions as it can process. Thus, we have

$$N\bar{\alpha}\left[1-\frac{f_c}{Vf_v}\right]=S.$$

Using the above expression we can obtain the equilibrium transaction fee on cryptocurrency. Therefore, we have

$$f_c = Vf_v\left[1-\frac{S}{N\bar{\alpha}}\right]. \tag{1}$$

We note that the transaction fee on the cryptocurrency, i.e., f_c, is inversely proportional to it capacity S. Intuitively, as the capacity of the system increases, the system is able to attract more transactions by reducing the transaction fee. We also note that the transaction fee charged by cryptocurrency is proportional to the transaction fee charged by Visa. The intuition behind this result is that if the transaction fee charged by Visa increases, then more transactions want to use cryptocurrency for processing. However, given the limited capacity, the cryptocurrency will also increase its transaction fee such that it attracts only as much demand as it can process. We formally state this result in the theorem below.

Theorem 2 *The equilibrium transaction fee charged by the cryptocurrency f_c is decreasing in S and increasing in f_v.*

We now proceed to analyze the problem faced by Visa.

3.1. Problem for Visa

For a given value of f_c, the equilibrium transaction fee charged by the cryptocurrency is given by (1). Let $Cost_{Visa}$ represent the total cost incurred by Visa to process its transactions. We know that all the transactions needing post-transaction services will use Visa, and all other transactions of values lower than $\hat{v}$ will also use Visa. Thus, $Cost_{Visa}$ can be written as

$$\begin{aligned} Cost_{Visa} &= \alpha N \int_0^V \frac{vC_h}{V} dv + N\bar{\alpha} \int_0^{\hat{v}} \frac{vC_l}{V} dv, \\ &= \frac{\alpha N C_h V}{2} + \frac{N\bar{\alpha} C_l \hat{v}^2}{2V}. \end{aligned}$$

Since $\hat{v} = \frac{f_c}{f_v}$, using (1), we have

$$\hat{v} = V\left[1 - \frac{S}{N\bar{\alpha}}\right]. \tag{2}$$

Using (2), we have

$$Cost_{Visa} = \frac{NV}{2}\left[\alpha C_h + \bar{\alpha} C_l \frac{\hat{v}^2}{V^2}\right] \tag{3}$$

Let Rev_{Visa} represent the revenue obtained by Visa. Then, we have

$$\begin{aligned} Rev_{Visa} &= \alpha N \int_0^V \frac{vf_v}{V} dv + N\bar{\alpha} \int_0^{\hat{v}} \frac{vf_v}{V} dv, \\ &= \frac{\alpha N f_v V}{2} + \frac{N\bar{\alpha} f_v \hat{v}^2}{2V}. \end{aligned}$$

Using (2), we have

$$Rev_{Visa} = \frac{f_v N V}{2}\left[\alpha + \bar{\alpha}\frac{\hat{v}^2}{V^2}\right]. \tag{4}$$

The services provided by Visa and its competitors (e.g., Mastercard, Discover, American Express etc.) are very similar. Thus, for the simplicity of analysis, we assume that Visa operates under perfect competition, which leads to zero profit for Visa (Rochet and Tirole 2003). Therefore, the revenue of Visa equals its cost. Thus, using (3) and (4), we have

$$f_v = \frac{\alpha C_h V^2 + \bar{\alpha} C_l \hat{v}^2}{\alpha V^2 + \bar{\alpha} \hat{v}^2}. \tag{5}$$

Note that $S = 0$ represents the pre-cryptocurrency world, i.e., the time before the advent of cryptocurrencies. It is easy to verify that $\frac{\partial f_v}{\partial S} \geq 0$. Thus, the transaction fee charged by Visa increases in the post-cryptocurrency world. We formally note this result in the theorem below.

Theorem 3 *The transaction fee charged by Visa increases after the advent of cryptocurrencies. More generally, the transaction fee charged by Visa increases as the capacity of cryptocurrencies increases.*

The advent of cryptocurrencies leads to a filtering effect: the transactions not requiring post-transaction services consider cryptocurrencies as an alternative channel for performing that transaction. However, the transactions needing post-transaction services consider only Visa as a verification channel. Since the transactions needing post-transaction services are costlier than the other kind of transactions, the cost of processing transactions increases for Visa. This leads to an increase in the transaction fee charged by Visa. This result is surprising because typically entry of a competitor (cryptocurrency in the case of Visa) should lead to a reduce the transaction fee.

We now proceed to analyze the problem faced by the cryptocurrency designer.

3.2. Problem of Cryptocurrency Designer

The stated goal or mission statement of most cryptocurrencies is to achieve highest level of decentralization,[5] which is equivalent to maximizing the number of miners. To this end, we

[5] `https://bitcoinfoundation.org/about/`

consider a cryptocurrency designer whose objective is to choose S, i.e., the capacity of the cryptocurrency, in order to maximize the number of miners. Let m represent the equilibrium number of miners on the cryptocurrency. We assume that all these miners are identical in terms of their computing power and incur cost C_m for mining. Let Rev_{Crypto} represent the revenue of the cryptocurrency per second. Then, we have

$$Rev_{Crypto} = f_c S.$$

We know that $\hat{v} = \frac{f_c}{f_v}$. Using (5), we have

$$f_c = \frac{\hat{v}(\alpha C_h V^2 + \bar{\alpha} C_l \hat{v}^2)}{\alpha V^2 + \bar{\alpha}\hat{v}^2}. \tag{6}$$

Thus, we have

$$Rev_{Crypto} = \frac{S\hat{v}(\alpha C_h V^2 + \bar{\alpha} C_l \hat{v}^2)}{\alpha V^2 + \bar{\alpha}\hat{v}^2}. \tag{7}$$

Since all miners are identical, each miner receives a revenue of $\frac{Rev_{Crypto}}{m}$. We assume that miners are perfectly competing with each other and, therefore, spend the entire revenue as a cost of mining. Thus, we have

$$\frac{Rev_{Crypto}}{m} = C_m$$

or

$$m = \frac{Rev_{Crypto}}{C_m} = \quad \frac{V}{C_m}\left(1 - \frac{S}{\bar{\alpha}N}\right)S \quad \times \quad \underbrace{f_v(S)}_{f_v(0)>0,\ \frac{df_v(S)}{dS}\geq 0} \quad . \tag{8}$$

We see that maximizing the number of miners is equivalent to maximizing the revenue generated by cryptocurrency. Intuitively, to attract a large number of miners, the cryptocurrency system needs to generate enough revenue to make up for the cost of mining.

Recall that we assume $S \leq N\bar{\alpha}$. Thus, the feasible values of S are in between 0 and $N\bar{\alpha}$. The problem for the cryptocurrency designer is to choose S to maximize m. It is easy to see that m is a highly non-linear function of S. Thus, it is difficult to obtain the closed-form expression for the optimal value of S. However, it is easy to verify that the value of m at the boundary values of S is zero. Thus, $S = 0$ or $S = N\bar{\alpha}$ cannot be an optimal solution. This insight is important given the ongoing debate about increasing the capacity of cryptocurrency to increase throughput. Our results suggest that increasing the capacity of cryptocurrency too much might hurt the ecosystem of the blockchain. This is because an increased capacity will lead to a lower transaction fee. A lower transaction will eventually disincentivize miner to participate in the cryptocurrency blockchain. We formally state this result in the theorem below.

Theorem 4 *The optimal value of S is not a boundary solution.*

We now proceed to conclude with a discussion of our main findings and some directions for future work.

4. Conclusion and Future Work

Cryptocurrencies have emerged as an alternative method for verifying financial transactions, which were hitherto performed by traditional channels like Visa, Mastercard, or Banks. We analyze the interaction between a cryptocurrency designer, a traditional channel of verification, and users. Using the framework of a sequential game, we find that the presence of a cryptocurrency imposes a negative externality on the transactions of small sizes. Overall, in the presence of a cryptocurrency, the transactions of small sizes are penalized and the transactions of large sizes are rewarded.

We argue that there are a few subtle but important differences between the value propositions offered by a cryptocurrency and traditional channels. For example, post-transaction services (e.g., reversal of an unintended or fraudulent transaction) which are readily available on traditional channels are not present on cryptocurrencies. We show that owing to this difference the transaction fee charged by traditional channel increases in equilibrium, when a cryptocurrency enters the market. The increase in transaction fee by traditional channel after the entry of a competitor (cryptocurrency) is surprising, because typically the entry of a competitor reduces the fee charged by an incumbent. The presence of a cryptocurrency leads to a filtering effect: the number of transactions needing post-transactions services increases on the traditional channel in the presence of a cryptocurrency. Since it is costlier to process the transactions needing post-transactions services, the transaction fee charged by the traditional channel increases. We also find that the difference in the underlying technology between a cryptocurrency and Visa leads to a very different pricing structure on both these verification methods. This difference in pricing structure makes cryptocurrency more suitable for transactions of large sizes. Overall, the transactions of small sizes, which are not suitable for cryptocurrency and need to use Visa, have to pay a higher transaction fee on the traditional channel in equilibrium.

Our analysis also shows that the limited capacity of cryptocurrency helps in keeping the transaction fee high. Therefore, increasing the capacity can lead to more transactions, but it can decrease revenue per transaction. Overall, increasing the capacity of cryptocurrency too much might hurt the ecosystem of cryptocurrency, because it might reduce the total revenue.

Typically, atleast two parties (sender and receiver) needed to perform a financial transaction on a platform like Visa or Bitcoin. Thus, the utility of a platform for its users increases as the number of users of the platform increases. Therefore, these platforms inherently operate under network effects. Modeling network effects is a natural extension of our paper and, therefore, is a promising direction for future work. Apart from this, in our current model setup, the transaction fee charged by Visa increases at a constant rate, f_v, with the value of a transaction. This leads to a loss of market share of transactions of high value for Visa. However, to retain this market, Visa can charge a lower rate for the transactions of high value. This kind of discriminatory tiered pricing presents an interesting avenue for future work.

References

Athey, S., I. Parashkevov, V. Sarukkai, and J. Xia. 2016. Bitcoin Pricing, Adoption, and Usage: Theory and Evidence.

Babaioff, M., S. Dobzinski, S. Oren, and A. Zohar. 2012. On Bitcoin and Red Balloons. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, 56–73. ACM.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta. 2018. The Blockchain Folk Theorem.

Bonneau, J. 2018. Hostile Blockchain Takeovers (Short Paper). In *Bitcoin18: Proceedings of the 5th Workshop on Bitcoin and Blockchain Research.*

Bresnahan, T. F., and M. Trajtenberg. 1995. General Purpose Technologies 'Engines of Growth'? *Journal of Econometrics* 65 (1): 83–108.

Cong, L. W., Z. He, and J. Li. 2018. Decentralized Mining in Centralized Pools.

Conti, M., S. Kumar, C. Lal, and S. Ruj. 2018. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*.

Courtois, N. T., and L. Bahack. 2014. On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency. *arXiv preprint arXiv:1402.1718*.

Da Conceição, A. F., F. S. C. Da Silva, V. Rocha, A. Locoro, and J. M. Barguil. 2018. Eletronic Health Records Using Blockchain Technology. *arXiv preprint arXiv:1804.10078*.

Digiconomist 2018. Bitcoin Energy Consumption Index. Available at: `https://digiconomist.net/bitcoin-energy-consumption` (Accessed June 23, 2018).

Easley, D., M. O'Hara, and S. Basu. 2017. From Mining to Markets: The Evolution of Bitcoin Transaction Fees.

Eyal, I., and E. G. Sirer. 2014. Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In *International Conference on Financial Cryptography and Data Security*, 436–454. Springer.

Goldfeder, S., H. Kalodner, D. Reisman, and A. Narayanan. 2017. When the Cookie Meets the Blockchain: Privacy Risks of Web Payments via Cryptocurrencies. *arXiv preprint arXiv:1708.04748*.

Huberman, G., J. D. Leshno, and C. C. Moallemi. 2017. Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System.

Jordan, R. 2018. How to Scale Ethereum: Sharding Explained.

Kroll, J. A., I. C. Davey, and E. W. Felten. 2013. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In *Proceedings of WEIS*, Volume 2013, 11.

Ma, J., J. S. Gans, and R. Tourky. 2018. Market Structure in Bitcoin Mining. Technical report, National Bureau of Economic Research.

Miller, A., A. Juels, E. Shi, B. Parno, and J. Katz. 2014. Permacoin: Repurposing Bitcoin Work for Data Preservation. In *Security and Privacy (SP), 2014 IEEE Symposium on*, 475–490. IEEE.

Nakamoto, S. 2008. Bitcoin: A Peer-To-Peer Electronic Cash System.

Natoli, C., and V. Gramoli. 2017. The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium. In *Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on*, 579–590. IEEE.

Nayak, K., S. Kumar, A. Miller, and E. Shi. 2016. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*, 305–320. IEEE.

O'Dwyer, K. J., and D. Malone. 2014. Bitcoin Mining and Its Energy Footprint.

Rochet, J.-C., and J. Tirole. 2003. Platform Competition in Two-Sided Markets. *Journal of the European Economic Association* 1 (4): 990–1029.

Sompolinsky, Y., and A. Zohar. 2015. Secure High-Rate Transaction Processing in Bitcoin. In *International Conference on Financial Cryptography and Data Security*, 507–527. Springer.

TechCrunch 2018. Update: Visa Issuers and Mastercard Make It Harder to Buy Bitcoin and Other Cryptocurrencies. Available at: `https://techcrunch.com/2018/02/05/visa-and-mastercard-make-it-harder-to-buy-bitcoin-and-other-cryptocurrencies/` (Accessed June 28, 2018).

The Wall Street Journal 2018. Blockchain and the Promise of an Open, Decentralized Internet. Available at: `https://blogs.wsj.com/cio/2018/02/23/blockchain-and-the-promise-of-an-open-decentralized-internet/` (Accessed June 23, 2018).

Vasek, M., M. Thornton, and T. Moore. 2014. Empirical Analysis of Denial-Of-Service Attacks in the Bitcoin Ecosystem. In *International Conference on Financial Cryptography and Data Security*, 57–71. Springer.