An Economist's Perspective on the Bitcoin Payment System

By Gur Huberman, Jacob D. Leshno, Ciamac Moallemi*

I. The novelty of Bitcoin

In its most basic form Bitcoin is (i) an append-only, publicly viewable collection of records (i.e., a database or a ledger) and (ii) a protocol, i.e., a set of rules governing the ledger's organization and updates. The Bitcoin system consists of a decentralized network of computers, each maintaining and updating a copy of the ledger in accordance with the protocol. Such distributed computer systems were in use for decades, but required reliance on a trusted party.

The design of such a system without a trusted party is the novelty in Nakamoto (2008).

In Nakamoto's blockchain design, the system is operated by a decentralized network of so-called miners, i.e., computers that maintain the ledger and update it according to users' requests. The protocol outlined in Nakamoto (2008) guides the actions of miners. They organize protocol-admissible requests into blocks, which are batches of ledger updates. Each miner spends computational resources in a process called proof of work (PoW) to participate in a lottery that selects the ledger's next block and its issuer. A miner's probability of winning the lottery is proportional to the resources he spends. All miners verify that an issued block is deemed valid by the protocol, and reject invalid blocks. Thus, miners collectively maintain a common ledger that is updated only with valid blocks.

In lieu of trust, the design relies on incentives to motivate the miners to follow the protocol. The system compensates miners who assemble the ledger-augmenting block. The promise of this reward motivates the miners to spend resources to maintain a copy of the ledger, assemble valid blocks, perform PoW, and verify the validity of blocks produced by other miners.

In order to compensate the miners, the system needs a coin or a method of value transfer. In fact, the rules specifying which updates are valid enable the ledger to be a record of users' coin balances and to facilitate payments. A coin transfer is a ledger update. It is valid if it is cryptographically verified to be authorized by the coin's owner and the transfer is capped at the amount owned. Standard accounting rules dictate the evolution of balances and prevent negative balances. The balances and transfers are all in the system's native coin – bitcoin.

The emergence of the native coin demonstrates Bitcoin's success in creating a trusted accounting system from a network of untrusted computers. Bitcoin's update validity rules facilitate the native coin. There is a long history of databases whose reliability depends on trusted parties. Bitcoin is complex and costly to run because it is designed to deliver the same functionality in the absence of a trusted party.

For Bitcoin's incentive scheme to function, the system must have access to a money-like instrument. The native coin can provide that role if coin recipients are willing to provide a good or a service when their balance increases. These recipients provide the good or service against the coin presumably because they believe that they will be able to exchange the coin in the future for a good or a service they will desire. Such a belief, if widely held, renders the coin a medium of exchange and a store of value.

II. A market for transaction processing

The interpretation of Bitcoin as a platform with two active constituencies, users and miners, is the starting point of Huberman, Leshno and Moallemi (2017) (hence-

* Huberman: Columbia Business School, email: gh16@gsb.columbia.edu. Leshno: University of Chicago Booth School of Business, email: jacob.leshno@chicagobooth.edu. Moallemi: Columbia Business School, email: ciamac@gsb.columbia.edu. The authors advise FinTech companies.

forth, HLM). The rules of the platform are fixed by a computer protocol. Assuming bitcoin carries value, the platform functions as a payment system, referred to as the Bitcoin Payment System (BPS). HLM asks who pays for the platform, how and how much. It compares the operations of the BPS with those of a familiar payment systems, e.g. PayPal. Finally, it applies the analysis to suggest design improvements.

HLM observes that the blockchain design of the BPS has the following features, which are key elements of its economics: Miners can enter or leave the system as they see fit. Each active miner can select the transactions he includes for processing in his block. Miners are rewarded with protocol-determined block rewards and transaction fees offered by the users. The latter will be essential to the system's revenue model because the former vanish over time. Users choose the transaction fees they pay.

The protocol calls for an upper limit on block sizes and for stochastic block creation times. The block creation times have a fixed long-run average independent of the aggregate resources spent by miners. Therefore, the system has limited capacity to process updates. This limited capacity and the stochastic arrival rate of users' updates imply the possibility of delays.

HLM offers a model of the BPS in which (i) delays are costly to users; (ii) miners are profit maximizers; (iii) miners can freely enter or exit the system.

A. Equilibrium transaction fees

HLM finds that the BPS is well described by an equilibrium in which users attach transaction fees to their entries to gain processing priority over other users; miners process the entries which offer the highest fees per byte up to block capacity. Nobody dictates the equilibrium fee schedule. It is an auction without an auctioneer.

Beyond arguing that the system prices delays, HLM offers closed-form formulas for the equilibrium fees and waiting times. The formula shows that total transaction fees depends on three parameters: maximal block size, congestion or load (transaction arrival rate divided by system's capacity), and the distribution of user delay costs.

When the system is not congested, the fees are low and essentially insensitive to its utilization; expected transaction processing delay is similar across transactions. As the system's utilization approaches the capacity limit, fees and cross-transaction variation in processing delays rise rapidly. The fee schedule satisfies the VCG property – each transaction's fee is equal to the externality it imposes on the transactions that offer lower fees.

Figure 1 summarizes (i) the theoretical fee schedule under the assumption that delay costs are distributed $U[0,1]$, and (ii) the correspondence of actual fees to the theory. The data begins in April 1, 2011, roughly when transaction fees per block started exceeding 1 USD. The end on June 30, 2017, shortly before the implementation of a protocol amendment which increased the maximal block size. Actual and model predicted transaction fees are given in USD.

On the miners' side, HLM shows that potential entry disciplines all miners to price-taking. That is all miners – even a miner who controls a large fraction of mining resources – cannot profitably affect the transaction fees paid by users. In fact, the canonical policy of processing all the highest fee per byte transactions, up to block capacity is optimal for all miners. (If there are too many transactions relative to the block size, then the lowest fee transactions will be excluded from the current block.) The argument underlying the surprising price-taking result accepts that a large miner can affect users' transaction fees by not including low fee transactions in his blocks, leading some users to pay higher fees. The argument notes that nonetheless, a miner will never find it profitable to do so because entry of additional miners will dissipate the additional revenue associated with the higher fees. (The result is valid as long as no miner can attack the system as described e.g. in Nakamoto (2008) and Eyal and Sirer (2014)).

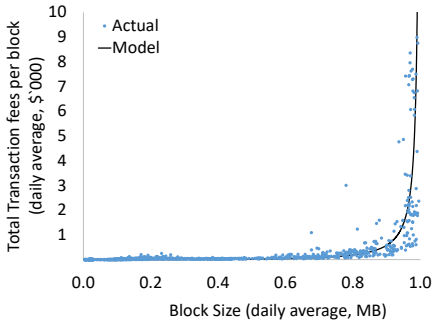

FIGURE 1. CONGESTION AND TRANSACTION FEES

Notes: The relation between transaction fees and congestion. The solid line is the theoretical prediction, the dots are daily observations of average block sizes (proxy of congestion) and corresponding fees. Transaction fee and block size data is from `http://blockchain.info`, the number of blocks per day is from `https://data.bitcoinity.org` (retrieved August 3rd 2018).

B. A comparison with a profit maximizing firm

Pricing under the BPS is structurally different from pricing under a profit maximizing firm. A firm would price its services to exclude the lowest willingness to pay customers, whereas the BPS raises revenue without excluding anybody. Unless users' delay costs are correlated with their willingness-to-pay, a firm will process transactions with no delays. Thus the firm sells service at a single price. In the BPS, delays are essential to fee generation, and therefore to the BPS's long-run revenue model. Thus the BPS sells service speed by offering a speed–price menu.

There is no mechanism that drives the level of mining to an efficient level, however defined. Newly minted coins and transaction fees fund the miners who acquire mining resources in USD-denominated markets. The protocol predetermines the block reward in the system's native coin; its USD-value fluctuates with the coin's exchange rate. HLM shows that the USD-valued transaction fees fluctuate with the system's load, i.e., the ratio of transaction arrival rate to transaction processing capacity (which is independent of the mining level). Controlling for the load, USD-valued transaction fees are independent of the exchange rate. Neither the block reward nor the transaction fees reflect the users' preferences over mining levels, and both fluctuate over time. Thus the funding of the miners could fluctuate over time, resulting in mining levels which are too small (rendering the system vulnerable) or too large (which is wasteful).

C. Design suggestions

HLM suggests an alternative design to address some of the weaknesses in the BPS protocol. The recommendation is a protocol rule that mandates a dynamic capacity that is a constant multiple of the transaction arrival rate, thus keeping the load approximately constant so as to generate a constant USD-valued transaction fee revenue.

The analysis of HLM also implies that for the same aggregate fees, lower block size and correspondingly higher service rate will result in lower delays. The preference for lower block size should be tempered by engineering considerations such as network latency and nonlinearity of propagation speed gain for smaller blocks.

III. Governance considerations

A. Governance by a protocol

Familiar organizations and their employees are physically able to betray the trust

vested in them. Some do just that when the incentive to betray the trust is strong. Society's threat of detection and subsequent punishment is usually an effective deterrent. In the BPS, there is no trust in any individual component; instead, the system overall is trusted because no component has the physical possibility to betray the trust. No external monitoring or punishment is required.

HLM focuses on the BPS as a value transfer system. In the absence of trust of external (i.e., state-issued) money, the transfer must be in the Bitcoin's native coin - bitcoin. Thus, the BPS must enable the storage of that native coin.

Governed by a protocol, the BPS is committed to (i) a fixed coin issuance schedule, (ii) a fixed pricing scheme, (iii) security of transactions and balances, (iv) anonymity of holdings and transfers. Moreover, the system is a publicly available resource which no single entity, not even its creator, can shut down. The commitment offered by the protocol promises levels of reliance and stability. Such a commitment encourages users' specific investments, thereby enhancing welfare.

A commitment also entails reduced flexibility to react to new circumstances. Protocol designers are challenged to anticipate future technological developments and how these technologies will be used. A hierarchical governance structure affords an effective reaction to such changes.

Coordination is required to switch from one set of rules to another. In the absence of a hierarchy, such coordination is difficult to achieve even when the incumbent protocol is widely recognized as flawed. The Bitcoin protocol has been amended, which indicates the presence of governance, however loose.

Indeed, self-organized Bitcoin communities discuss and try to coordinate possible protocol amendments. Developers propose amendments to the incumbent protocol, which miners can decide to implement. The value users attributed to the amended system determines its value the and the value of its coin. Different factions may fail to reach agreement, resulting in failures to update the system or a fork that splits the system. Bitcoin Cash is an example. It forked from Bitcoin after failure to agree on amendments that would increase the system's capacity.

The short history of the DAO (Decentralized Autonomous Organization) offers another example of a fork. The DAO was developed on Ethereum, a system that expands the functionality of Bitcoin. Ethereum allows users to control funds with computer code (so-called "smart contracts") that runs on the its decentralized computing network. The DAO's creators envisioned it as the manifestation of a new form of governance offered by Ethereum's decentralized computing capabilities. The DAO was to serve as a venture capital fund that would select projects through investors' voting. In contrast to traditional funds, it would not rely on any external legal regime. Ethereum's coin would support fund raising; code running on Ethereum would enforce DAO's governance rules on voting and project funding. More than 11,000 investors contributed the equivalent of $150 million to DAO in May 2016, representing about 15% of the total value of Ethereum's coin.

On June 17, 2016, an attacker exploited vulnerabilities in the DAO's code to transfer about one third of the DAO's holding to his possession, subject to a 28 day freeze as dictated by the DAO code. A lively debate followed. Arguing that "code is law" one camp supported honoring the transfer, however unethical. Another camp argued that returning the funds to their original owners was feasible and the right thing to do. Vitalik Buterin, Ethereum's founder, was a prominent supporter of the second camp.

The debate ended with a hard fork: Ethereum Classic is a coin that accepts the vulnerability-exploiting transfer; Ethereum is a coin which reversed the transfer.

B. Price and its forward looking component

The coexistence of Bitcoin and Bitcoin Cash calls for a price comparison between the two coins. Both have been secure and reliable. Both have very similar features,

but Bitcoin Cash has larger block size and lower transaction fees. They trade at different prices, with bitcoin's price ranging between 5 and 10 times the price of bitcoin cash. The feature comparison and the absence of an explanation for these relative prices call for further research. Variation in the governance of the two coins and perception of that variation could account for the difference in the value of the two coins.

The value assigned to a coin is a social convention. Similarly, the values assigned to gold and to fiat money are a social convention. The social convention relies on the future usefulness of these means of payment. In contrast to gold or paper money, bitcoin can only be used within the decentralized system that maintains it. (Bitcoin miners maintain the system, unlike gold miners.) Assigning value to Bitcoin requires confidence in the future of the system and its future evolution.

REFERENCES

Eyal, Ittay, and Emin Gün Sirer. 2018. "Majority is not enough: Bitcoin mining is vulnerable." *Communications of the ACM*, 61(7): 95–102.

Huberman, Gur, Jacob D Leshno, and Ciamac C Moallemi. 2017. "An economic analysis of the bitcoin payment system."

Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system."

Wikipedia contributors. 2018. "The DAO (organization) — Wikipedia, The Free Encyclopedia." *https://en.wikipedia.org/w/index.php?title=The_DAO_(organization)&oldid=871650313*, [Online; accessed 31-December-2018].