Settlement and Blockchain Equilibria

Zahra Ebrahimi[1]
Bryan R. Routledge[2]
Ariel Zetlin-Jones[3]

[February 14, 2019]

Extended Abstract

Blockchain technology is a set of protocols that facilitate a public and decentralized database. An important component of blockchain technologies is a token that can be used as a method of payment. For some blockchains like Bitcoin, the token is a cryptocurrency intended to act as money. Since typical blockchains feature neither a central trusted authority (like a bank or government) nor the ability to store or secure physical assets (like a bar of gold or a $100 dollar bill), the viability of the cryptocurrency associated with a blockchain as a store of value and as a medium of exchange depends on the protocols underlying the blockchain.

Here we focus on Bitcoin as both the largest (market capitalization) cryptocurrency and a canonical example of a blockchain equilibrium. The Bitcoin blockchain ledger is a record of every transaction. This ledger establishes the providence of each Bitcoin. To drive agreement on transactions and their order (i.e., which ledger is "the ledger") and hence agreement on balances, Bitcoin follows a "proof-of-work" protocol. New transactions are recorded in blocks by independent miners (accountants) and added to the longest chain. Miners follow this convention since they are paid for mining with Bitcoin recorded in their newly-formed block and hence have an incentive for their block to be part of the consensus ledger. The proof-of-work protocol is an equilibrium—see (Biais, Bisiere, Bouvard, and Casamatta 2018).

One much discussed limitation of the Bitcoin "proof-of-work" protocol is its vulnerability to a "51% attack" to steal Bitcoin.[4] Here, a miner might change an old transaction then create new subsequent blocks yielding the longest chain. Of note, first, to create a long chain requires "doing the work" (producing blocks) faster than the rest of the network working on the original chain. This requires having a majority of the computing power—hence the name with"51%"

[1] Tepper School of Business, Carnegie Mellon University; zebrahim@andrew.cmu.edu.

[2] Tepper School of Business, Carnegie Mellon University; routledge@cmu.edu.

[3] Tepper School of Business, Carnegie Mellon University; azj@cmu.edu.

[4] See: "Coinbase Suspends Ethereum Classic After Blockchain History Rewrites" Jan 7, 2019. https://www.coindesk.com/coinbase-suspends-ethereum-classic-after-blockchain-history-rewrites?amp.

referring to the proportion of the computing power needed. Second, creating blocks is expensive (electricity) but finite and this can put an upper bound on the value of a Bitcoin—as argued in (Budish 2018). Third, and the critical consideration underlying our analysis, to be effective the attack must occur on an "old" block where settlement of the related non-Bitcoin good has already happened (the real goods or services that were previously exchanged for the Bitcoin).

Settlement lags—the time between the agreement and execution of a trade—are common in many consumer settings (Amazon.com) and finance transactions (stocks). For blockchains, settlement lags arise from the underlying protocol. The randomness in block creation (guessing a hash) and the distributed nature of the ledger results in "forks" where there are several longest blockchains that differ (only) in the last few blocks (typically one or two). Once one of the chains is unambiguously the longest, transactions in orphaned blocks drop back into the pool and eventually are incorporated in a later block. This structure creates a settlement lag whereby those who receive Bitcoin necessarily wait to deliver non-Bitcoin goods or services until they are convinced their Bitcoin transaction is recorded in the unambiguously longest blockchain.

The norm (not a formal rule) with Bitcoin is that a seller receiving Bitcoin wait at least six blocks (about one hour) before delivering the non-blockchain goods. This ensures (high likelihood) the block holding the transaction will not be orphaned and is on the longest chain. The settlement lag also increases the cost of undertaking a 51% attack as more computational work is required to create a new, longest chain. As a result, the settlement lag plays a key role in securing the Bitcoin blockchain.

In this paper, we demonstrate how incorporating settlement into the blockchain protocol expands the set of equilibria and allows for equilibria that eliminate "51% attacks." This proposed modification to the Bitcoin protocol equilibrium increases the security of the blockchain—thereby allowing the theoretical transaction value of Bitcoins to grow larger than previously studied—and is, we will show, straightforward to implement. We then use our framework to examine optimal settlement lags that tradeoff blockchain security with the usefulness of Bitcoins as a medium of exchange.

References

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2018): "The blockchain folk theorem," Toulouse University Working Paper.

Budish, E. (2018): "The Economic Limits of Bitcoin and the Blockchain," National Bureau of Economic Research Working Paper.

Mailath, G. J., and L. Samuelson (2006): *Repeated games and reputations: long-run relationships*. Oxford university press.