Mechanism Design: Referee Report #1

The Economic Limits of Bitcoin and the Blockchain by Eric Budish

Due on Due March 21, 2019

Professor Brian Baisa

Siqing (Alex) Liu

1 Paper Description

Budish argues that there are critical economic limits on the potential for blockchain namely that the system as is will require high implicit tax rates and discourage small transactions. His key argument is laid out in the first section, where Budish establishes two key conditions that an anonymized, decentralized blockchain such as Bitcoin must satisfy in equilibrium, namely a Zero-Profit condition and an Incentive Compatibility condition.

First, there must be a Zero-Profit condition amongst 'honest' miners, who are assumed to be participating in a free-entry rent-seeking competition to be the first to add the next block in the chain. Let P_{block} be the reward a miner wins for adding the next block, and c the per-block cost of one unit of computational power. If N is the number of units of computational power on the network, then the equilibrium amount N^* is characterized by

$$N^*c = P_{block} \tag{1}$$

Second, there must be an Incentive-Compatibility condition, namely that the cost of an attack must exceed its benefits. Budish considers a critical and well known attack, the majority attack, whereby the attacker gains a majority of the computational power. He analyzes the potential costs as following. If an attacker would need to pay $N^*c + \epsilon$ when there are already N^* honest blocks, then an expenditure of AN^*c per block would yield a super-majority of $\frac{A}{A+1}$ super-majority for the attacker. Assume that there is a reward of V_{attack}, with an expected cost to the attacker net of block rewards αN^*c. If an attack takes t blocks worth of time, and receives t blocks as reward, then the total cost net of block rewards is $AtN^*c - tP_{block}$, thus using equation (1) we get $\alpha = (A-1)t$. Therefore, for a blockchain system to be incentive compatible against an attack:

$$\alpha N^*c > V_{attack} \tag{2}$$

This equation simply argues that the cost of manipulating the blockchain must be greater than its benefits. Budish first stresses that this is related to the *flow* cost of capital, and not the *stock* cost. Second, Budish stresses that costs only increase linearly, whereas many other computer security mechanisms impose exponentially increasing costs.

Combining (1) with (2) we get the following equilibrium constraint:

$$P_{block} > \frac{V_{attack}}{\alpha} \tag{3}$$

This equation argues that the per block reward must be greater than the cost of attacking the blockchain network.

Budish in section 2 then mainly examines a feasible method of profiting from an attack, the "double-spending" method, in order to substantiate the values V_{attack} and α. Budish assumes that there are k

transactions per block, the attacker engages in the full k transactions, the average value of each transaction is $\bar{v}_{transaction}$ (can be interpreted as a statistic on the highest value transactions in the Bitcoin system), merchants wait an escrow period of e periods, and that the attack does not impact the value of Bitcoins.

Defining the value of the attack as $V_{attack} = k\bar{v}_{transaction}$ and the per-transaction reward as, $p_{transaction} = \frac{P_{transaction}}{k}$ we then get the equation

$$p_{transaction} > \frac{\bar{v}_{transaction}}{\alpha} \tag{4}$$

This equation argues that the per transaction cost must be greater than a proportion of a statistic on the highest value transactions in the blockchain system. Budish then runs simulations to find values for α, assuming the likelihood of a successful attack declining exponentially with escrow period e, and modelling for different values of computing power A and escrow period e. He argues that the results for α means that the system will require implicit tax rates too high for small transactions.

Budish further details the cost and benefits of an attack by examining if cryptocurrencies experience a deterioration in value after an attack. While a small decrease would require a large implicit tax, a large decrease would make the system vulnerable to a sabotage attack. A sabotage attack would attempt to destroy rather than profit from the cryptocurrency value itself.

Budish in section 3 then examines different cost structures and collapse scenarios. He argues that since currently the technology for mining is specific, i.e. non-repurposable, and that an attack devalues said technology, it may be appropriate to not charge a *flow* cost but instead a *stock* cost. Budish then argues that the loosest constraint is if the the attack is a sabotage attack and destroys all the value of the stock, yielding the condition $N^*C > V_{sabotage}$. This condition is the least constraining given that flow costs are estimated on the order of a few million dollars, whereas the value of current Bitcoin mining equipment is around. 1.5 - 2 billion dollars.

2 Comments

I enjoyed this paper because it laid out formal and rigorous theoretical constraints on the hype surrounding blockchain systems in an easy to understand manner. Although I have taken relevant courses such as Game Theory, the arguments are intuitive enough to be understood by someone without an advanced economics education. Moreover, Budish, by fitting blockchain systems in a game-theoretic economic framework, provides an example that can guide further applications of formal economic theory to the seemingly unprecedented innovation of blockhain. While it seems that the paper was received well in the economics community, blockchain devotees argued Budish's arguments lacked novel insights and are incongruent with empirical behavior of current blockchain systems.

However, I believe that we need to focus on the larger implications of Budish's paper. The blockchain community is vibrant and dynamic, with new protocols springing up left and right. This organic heterogeneity and innovation is providing large-scale economic experimentation that Game Theorists and Mechanism Designers can often only dream of. Budish's paper is an important step in bridging the gap between academia and practitioners and an important attempt at establishing authoritative academic analysis in the Wild West of blockchain.

- Budish's argument, while tight and concise, fails to account for how other forms of digital crime might offer better risk adjusted returns. Major cryptocurrencies are prominent and highly transparent. Furthermore, such an attack would also entail a high upfront cost of acquiring enormous amounts of computational power. Thus attacking major cryptocurrencies such as Bitcoin or Ethereum might be simply too complicated and risky versus other forms of digital crime.

  We cannot silo blockchain systems from national and international protections, and need to recognize that cryptocurrencies are free-riding on the public provision of law enforcement. For example, Bitfinex was able to recover $120,000 worth of Bitcoin from US law enforcement. [Zmudzinski, 2019] In Japan, bitcoin is considered legal tender, and enjoys robust regulatory and political oversight. [Rooney, 2018b]

- A key component of Budish's criticism regarding blockchain security is that the cost of an attack rises linearly with the size and value of the system. Critics have pointed out however that the cost of coordination may rise in a non-linear fashion. However, mining is currently highly centralized in large pools. A recent academic study found that: "...in Bitcoin, the weekly mining power of a single entity has never exceeded 21% of the overall power. In contrast, the top Ethereum miner has never had less than 21% of the mining power. Moreover, the top four Bitcoin miners have more than 53% of the average mining power. On average, 61% of the weekly power was shared by only three Ethereum miners..." [Gencer et al., 2018].

  Nonetheless, coordination costs could come from other areas. Negotiations on how to split the spoils from a successful attack could be enormously difficult with existing mining pools, as often many of the computational power is provided by individual owners.

- The fact that the parties coordinating large pools of mining power in major cryptocurrencies are also invested heavily in other areas of the blockchain system destablizes Budish's two constraints and may explain why there have been many attacks on minor currencies but no systemic attack against major cryptocurrencies such as Bitcoin or Ethereum. For example, online block trackers have noted that Bitmain, which controls two of the largest mining pools, already breached the 51% bound before. [Wilmoth, 2018] However, Bitmain is also one of the world's largest producers of specialized mining hardware, and raked in 750 million dollars of profit on 2.8 billion of revenue in the first half of 2018. [Rooney, 2018a]

  Thus, players such as Bitmain demonstrate that the clean and tidy assumptions behind (1) and (2) may not hold. Bitmain mines cryptocurrencies, purchases cryptocurrencies, and sells mining hardware. This destabilizes (1) because these complementary lines of business mean that the assumption of a perfect competition market may be materially incorrect. Furthermore, the example of Bitmain also destabilizes (2), for the cost of attacking the system to a player like Bitmain is not simply $\alpha N^* c$. While Budish considers stock value as well, such an extension does not fully capture the benefits and costs of significant and complex players such as Bitmain.

- Budish gives shorting Bitcoin using Bitcoin futures as a key example of how a private actor may have both the means and profit to sabotage the Bitcoin system. He argues that if Bitcoin futures grow beyond their relatively tiny size, this could make constraint (2) difficult to sustain as it increases the value of V_{attack}. Critics, however, have argued that Budish overlooks the complications of such an attack, for the "...the attacker would have to use a regulated broker in order to establish a position on CME or CBOE, leaving a trace there as well. Sure, the attacker could establish a very large short position on an exchange such as Bitmex, which doesnt have a proper clearing house, but in that case there is really no reliable mechanism to force the longs to pay a massive amount of money if they dont have the funds." [Kogan, 2018]

  However, while an actual attack may not happen if constraint (2) is breached, a perceived breach or potential for a breach would worry holders of Bitcoin, which could increase volatility. While the amount of volatility that a financial instrument such as Bitcoin can sustain is a whole other debate, significant volatility would impact Bitcoin's chances of becoming a true 'store-of-value' versus alternatives such as gold.

References

Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert Van Renesse, and Emin Gün Sirer. Decentralization in bitcoin and ethereum networks. *arXiv preprint arXiv:1801.03998*, 2018.

Michael Kogan. Bitcoin and academic economists, Jun 2018. URL https://hackernoon.com/bitcoin-and-academic-economists-75269003c2ec.

Kate Rooney. Cryptocurrency giant bitmain reveals profits and ipo plan despite slump in bitcoin, Sep 2018a. URL https://www.cnbc.com/2018/09/26/cryptocurrency-giant-bitmain-reveals-profits-and-ipo-plan.html.

Kate Rooney. Your complete guide to crptocurrency regulations around the world and where they are headed, Mar 2018b. URL https://www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html.

Josiah Wilmoth. Bitmain's mining pools now control nearly 51 of the bitcoin hashrate, Jun 2018. URL https://www.ccn.com/bitmains-mining-pools-now-control-nearly-51-percent-of-the-bitcoin-hashrate.

Adrian Zmudzinski. Bitfinex's stolen funds partially recovered and returned by us law enforcement, Feb 2019. URL https://finance.yahoo.com/news/bitfinex-stolen-funds-partially-recovered-115200441.html.