Cryptocurrencies as Marketplaces

Jacob Leshno, University of Chicago

Nakamoto (2008) introduced Bitcoin, a computer protocol establishing a decentralized system that allows users to hold balances and make transfers one to another. Computer systems that provided similar services have existed for decades, but required a trusted party to control and operate them. For example, PayPal Holdings Inc. provides such services to users of its online payment system. The company is responsible for maintaining the required computer infrastructure, and is able to charge usage fees to fund its activities and make profits.

In contrast, Bitcoin is a decentralized system. Instead of having a company which is responsible for maintaining the system's infrastructure, Bitcoin is operated by a decentralized network of computers called miners. Much like Uber and Lyft allow anyone with a proper car to provide transportation services in return for compensation, Bitcoin allows anyone with a proper computer to provide the payment processing infrastructure in return for compensation. In that, Bitcoin eliminates the need for centralized provision of infrastructure by creating an open marketplace.

But Bitcoin is unlike Uber and Lyft in that no entity is in control of the marketplace. Uber can change the price paid to drivers, add or remove the option to tip, and charge fees from the participants in its market. In contrast, Bitcoin is governed by its protocol, which no single entity can change (making changes to Bitcoin is akin to changing communication protocols as TCP/IP). The computer protocol dictates the rules that govern the system and its implied marketplace, setting the rules that determine how miners are compensated and the fees users pay.

The viability and success of Bitcoin, and the many other cryptocurrencies that followed, requires that the protocol establishes a functioning marketplace. In addition to standard engineering challenges,

cryptocurrencies cannot control the miners who provide the infrastructure, and incentives are required to get miners to follow the desired behavior [eyal2018majority, carlsten2016instability]. Miners provide their services at will, and can withdraw from the system at any time, or try to exploit the system for profit and jeopardizing the security of the system [budish2018economic, auer2019beyond]. Game theory provides tools to understand how miners and users will behave in such an environment, and determine whether the system is secure.

Since Bitcoin is not integrated with (and does not wish to rely on) other financial services, payments to miners can only be done with the systems native coin, bitcoin. The value of the native currency bitcoin is determined by financial markets, bringing in questions from monetary theory [schilling2019some]. These elements and others differentiate cryptocurrencies from traditional computer systems, and makes them economic objects, akin to marketplaces.

Monopoly without a monopolist

Assuming bitcoin is valuable, Bitcoin functions as a payment system, referred to as the Bitcoin Payment System (BPS). Users send transaction and pay fees who fund the miners who provide the infrastructure for the system. This interpretation is the starting point of [huberman2019economic] (henceforth, HLM) who study the properties of this marketplace for transaction processing. In particular, they ask who pays for the costs of operating the platform, how and how much. They compare the BPS with a traditional payment system (for example, PayPal) and ask whether the decentralized design offers new benefits. While they focus on Bitcoin's design, their analysis also applies to the many cryptocurrencies who share similar design features.

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 they process, and are rewarded with protocol-determined block rewards and transaction

fees offered by the users (transaction fees will become more important over time, as they eventually become the only form of payment to miners). Users who issue a transaction choose the transaction fees they pay when the transaction is processed.

The system processes transaction in batches which are called blocks. To ensure a block is prorogated throughout the network before the next one is issued, the protocol limits block size and frequency. Therefore, the system has limited transaction processing capacity. Because of stochastic elements in the system, the system can get periodically congested and transaction can be delayed.

HLM offers a simplified economic model of the BPS that allows an analysis of the implied marketplace. Some key elements of the model are (i) some users are willing to pay to expedite the processing of their transactions; (ii) miners are profit maximizers; (iii) miners can freely enter or exit the system.

Transaction fees are determined in equilibrium

HLM finds the BPS is well described by an equilibrium in which users choose a transaction fees to gain processing priority over other users; miners process the entries which offer the highest up to capacity. Nobody dictates the equilibrium fee schedule. Fees are set in an implicit auction without any explicit 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 willingness to pay to reduce transaction processing delay.

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 by increasing their delays.

A comparison with a profit maximizing firm

Pricing under the BPS is structurally different from pricing under a profit maximizing firm. A firm sets a price, and denies service to users who are unwilling to pay that price. When the BPS has sufficient capacity, the BPS can raise revenue without denying service to anybody - users who are willing to bear delays can have their transaction processed even if they are unwilling to pay transaction fees. The miners collectively operate the system, but because they compete with each other, the miners cannot profitably affect the level of fees paid by users. This provides users protection from price increases, even if the system becomes a monopolist (in the sense that users have no alternative payment methods) users will still pay a low competitive transaction fee. In that, the decentralized nature of the system may provide economic benefits to users.

However, the design has several weaknesses. Transaction processing delays are essential to fee generation, and therefore to the BPS's long-run revenue model. The amount of infrastructure consumed by the system is determined in equilibrium, and there is no mechanism that ensures an efficient level of infrastructure. The amount of energy consumed by Bitcoin has received much media attention. It varies depending on the demand for transaction and the bitcoin to USD exchange rate, and the system design does not indicate a desired level or a way of reaching such a level.

Design suggestions

HLM provides a design that can partly address these concerns. That design modifies an existing component of the current protocol so that instead of maintaining a constant capacity, the protocol scales capacity (within a feasible region) according to demand to ensure that utilization is kept at a moderate level. This ensures that total transaction fees and the level of infrastructure are kept at a

constant level. The analysis also implies that smaller block sizes allow the system to raise revenue more efficiently, in that a smaller block size allows the system to raise the same amount of revenue with less transaction processing delays.

Governing a decentralized system

Limitation of the Bitcoin protocol, such as its limit transaction processing capacity, motivated much subsequent research and development of other decentralized systems ([chen2016algorand, bentov2016snow]). To update existing systems, agreement much be reached on a new protocol. The absence of an entity that controls the system, such agreement can be difficult to achieve. The implied rigidity of the system can be useful to users, who are guaranteed continuation of service at the same terms (and no ratcheting of fees). But it also reduces the system's ability to react to new circumstances, which is especially important given the early stage of the technology. Game theoretic analysis can shed light on governance issues and help design systems accordingly [barrera2018blockchain].

Conclusion

Through a combination of cryptographic tools and economic incentives, Bitcoin and its many followers showed that it is feasible to create a decentralized system, controlled by no one. Services that could only be provided by a trusted firm can now be provided by a community coordinated by a protocol. This allows for new exciting economic models for how such services should be operated and funded. The interdisciplinary nature of these systems calls for exciting future collaboration.

References

[1] Raphael Auer. Beyond the doomsday economics of'proof-of-work'in cryptocurrencies. 2019.

[2] Cathy Barrera and Stephanie Hurder. Blockchain upgrade as a coordination game. 2018.

[3] Iddo Bentov, Rafael Pass, and Elaine Shi. Snow white: Provably secure proofs of stake. IACR Cryptology ePrint Archive, 2016:919, 2016.

[4] Eric Budish. The economic limits of bitcoin and the blockchain. Technical report, National Bureau of Economic Research, 2018.

[5] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. On the instability of bitcoin without the block reward. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 154–167. ACM, 2016.

[6] Jing Chen and Silvio Micali. Algorand. arXiv preprint arXiv:1607.01341, 2016.

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

[8] Gur Huberman, Jacob Leshno, and Ciamac C Moallemi. An economic analysis of the bitcoin payment system. Columbia Business School Research Paper, (17-92), 2019.

[9] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[10] Linda Schilling and Harald Uhlig. Some simple bitcoin economics. Journal of Monetary Economics, 2019.