Battles of the bitcoin

In a world full of momentous separations, the split of the bitcoin into bitcoin cash and bitcoin classic on 1 August hardly drew a whimper. And yet, the future of a pioneering cryptocurrency with over $40 billion in circulation is at stake. A simple game illustrates the conflict that lies at the heart of the breakup. But first, a bit about the bitcoin.

In traditional monetary systems, money is created by repeated rounds of credit creation built upon on a given monetary base, either real like gold or notional like currency and coins in circulation. In the bitcoin world, starting with a small initial stock, additional bitcoins are created as payments to “miners” who facilitate transactions being carried out with existing bitcoins. Miners are record keepers who compete with each other to be the first to write code to add a “block” of transactions to the “chain” of already existing transactions that form part of an encrypted public ledger called the “block chain”. Those miners who succeed earn newly minted bitcoins, which can be used for further transactions.

Just as the growth of a traditional currency depends on the people’s willingness to borrow money to use it for transactions as well as the size of the monetary base, the growth of the bitcoin economy depends on its acceptance as a medium of transactions as well as the speed with which miners can generate new bitcoins. In the early days of the bitcoin, since its introduction in 2009, the bottleneck was its low level of acceptance. But over the last two years, with greater acceptance by the general public and even by governments, the speed with which miners can add transactions has become the determining factor for the growth of the currency.

The size of the file that is uploaded by miners to add a block to the block chain is 1 MB. This allows only seven additional transactions to be uploaded in 10 minutes. In contrast a network like Visa can handle thousands of transactions in this time. Due to the low capacity, bitcoin users have had to pay up to $5.50 on average to get a transaction dealt with speedily.

Competition between miners has intensified with relative computational power being the critical success factor. Because bigger mining operations have an advantage over smaller ones, miners have come together to form mining pools and the industry has become highly concentrated. More than 60% of mining power is thought to be generated in China, where electricity is cheap and data centres easy to build. This is a far cry from the founder Satoshi Nakamoto’s vision of mining as a fragmented activity, done by individual bitcoin holders.

We know that markets with a limited number of firms are prone to cartelization. This is reflected in the synchronized behaviour of Chinese mining pools which have a veto power on the new rules that get implemented. What is not emphasized enough is that such markets are equally prone to inter-corporate warfare going beyond acceptable tactics of competition. Since 2011, mining pools have frequently been targeted by distributed denial-of-service (DDoS) attacks initiated by competitors. Of 49 mining pools, 12 experienced DDoS attacks, often repeatedly. At least one mining pool, Altcoin.pw, appears to have shut down due to such attacks. Attackers have two primary objectives when initiating DDoS attacks on mining pools. First, the operations at competing mining pools are slowed down which might give a decisive advantage in the race for the next bundle of bitcoins. Second, individual miners might become discouraged and decide to leave “unreliable” mining pools as the result of these attacks

The systematic incentive to initiate attacks can be explained by a game which shares some characteristics of the prisoners’ dilemma. Assume there are only two mining pools, each with equal initial computational power. Each can either invest in additional computing resources, or trigger a costly DDoS attack to lower the expected success outlook of its competitor. If it triggers

an attack, the competitor cannot mine any bitcoins over the time horizon of the game. The attacker also fails to increase its own computation power but enjoys monopoly power on account of having neutralized its rival.

In this game it is a (weakly) dominant strategy for each mining pool to initiate an attack when both would be better off building their computing power. In general, if small mining pools have the power to damage large pools to a degree far beyond their relative sizes, while their ability to grow their own computational power is proportional to their size, they could have an incentive to neutralize large networks rather than building up their own capacities. It is possible, therefore, that in equilibrium, only a small percentage of the computational power, representing the capacity of smaller firms, survives.

The warfare between miners combined with the already low capacity of the system to service transactions provides an opportunity to competition outside the bitcoin. It is no surprise that a whole host of other options like ethereum have emerged.

The peculiar bottlenecks in the bitcoin and the current split reflect a divide between those who see it as a store of value like gold, which does not require frequent transactions, and those who see it as a medium of exchange. Preserving the idealism of the early days given rapid adoption and growing competition may well prove to be a bridge too far. The founders of the bitcoin may need to seek solace in the wisdom of Bob Dylan who sang: *She knows there's no success like failure, and that failure's no success at all.*

Rohit Prasad is a professor at MDI, Gurgaon, and author of Blood Red River*. Game Sutra is a fortnightly column based on game theory.*

END