EDISON

Edison Explains

Bitcoin's investment thesis

Part two: Decentralisation of nodes, hashrate and ownership

Negative								Positive
							X	

Cryptocurrencies – irrational hype or financial revolution?

Bitcoin (BTC) and other digital assets have been making the headlines in recent months, polarising the investment community with an equal number of strong advocates and fierce critics (even within the same financial institution or research house). Moreover, valid analysis, backed by in-depth research, is mixed up with ideological, poorly researched conclusions both for and against the theme. We have decided to look at both sides of the same (bit)coin to extract the investment thesis behind this new asset class. Each part of this Edison Explains series looks at one feature of BTC and the broader cryptocurrency landscape (broadly referred to as 'altcoins'). We conclude by summarising our subjective view on how positive or negative we believe the feature is for BTC's investment thesis.

In what way is BTC decentralised?

There are several different types of participants in the BTC network. These include: 1) individuals and institutions who hold and transact in BTC on the network; 2) miners ('hashers'), who are responsible for adding submitted transactions to new blocks and broadcasting blocks to the network; and 3) full nodes hosting and synchronising a copy of the entire blockchain history; they are responsible for validating newly submitted transactions (ie checking whether the sender has sufficient BTC in his/her digital wallet and is not double-spending funds) and verifying/adding new blocks broadcast by miners. Importantly, any network participant can operate a full node at a reasonable cost (a few hundred US dollars), although some do not want to keep the full copy of the blockchain (which is currently c 350GB) and run so-called light nodes (or Simplified Payment Verification (SPV) nodes), which partially rely on the validation capabilities of full nodes or pruned nodes which validate the entire chain but do not store its complete copy. While difficult to measure precisely, there seems to be more than 50,000 operational full nodes on the BTC network at present (quite well spread geographically).

Edison Insight

Bitcoin's decentralised network of full nodes and individual miners constitutes a revolutionary feature underpinning its status as an incorruptible, censorship-resistant system. However, while there are important monetary disincentives to perform a '51% attack' by major mining pools, allowing individual miners who participate in a pool to order transactions would reduce the risk further.

The combination of a distributed network of full nodes and a wide group of miners representing a significant hashrate (computing power used by miners to produce new blocks, currently c 100 exahashes per second), eliminates the need for trust between network participants and, in turn, the requirement for a central trusted entity governing the network and the need for intermediaries. As a consequence, BTC could be viewed as an incorruptible, independent monetary system based on a peer-to-peer network.

But wait, isn't BTC mining centralised?

BTC mining is indeed relatively concentrated within so-called mining pools, which are groups of miners combining their computational power to realise economies of scale by increasing the probability of mining a block and receiving the block reward. The process is managed by pool operators, who are responsible for assigning mining jobs to members of the mining pool, broadcasting/propagating blocks mined, as well as distributing block rewards to pool members based on a predefined payment scheme (eg a pay-per-share (PPS) model or a pay-per-last-n-share (PPLNS) model). Importantly, under the Stratum V1 protocol (developed by SlushPool), currently used by all major mining pools to cooperate with miners, these operators are also responsible for ordering transactions to be added to new blocks mined by 'hashers', which technically grants them the power to censor transactions on the network. In fact, there are already some minor

02/08/21

examples of this, such as the Blockseer Pool, which rejects transactions from blacklisted wallets, or the Marathon OFAC pool, although in the end it withdrew from mining only blocks compliant with the Office of Foreign Assets Control. An upgrade to the protocol (called Stratum V2), which is currently being introduced, would mitigate the censoring risk as it allows miners (rather than pool operators) to order transactions. However, its adoption by mining pools has been slow so far.

The top five mining pools (AntPool, Poolin, Binance Pool, ViaBTC and F2Pool based on the latest weekly data as at 30 July 2021) control c 60% of the total hashrate, while the top10 control c 90%, according to BTC.com data. Moreover, the top 1% miners in the top pools account for c 65% of its hashrate, according to the Cambridge Centre for Alternative Finance. Theoretically, operators of some of the largest mining pools (controlling the majority of BTC's hashrate) could join forces to carry out a so-called '51% attack' and reorganise the blockchain so that they can double-spend funds or systematically censor certain types of transactions (by not adding them to new blocks). However, we note that this would be contrary to the interests of BTC miners, as it would undermine BTC's credibility and almost certainly lead to a crash in BTC’s price, translating into significant losses for them given the considerable investments they made in customised application-specific integrated circuit (ASIC) mining equipment to receive BTC rewards. This represents an opportunity cost for potential attacker(s) and has been already addressed by BTC's creator(s), Satoshi Nakamoto in the white paper published in 2008, where Satoshi highlight(s) that maintaining the value of the mined coins (together with collecting transaction fees) represents a strong incentive to play by the rules. The motivation of the respective miners to be part of a given pool is predominantly monetary and they can switch to any other pool if they conclude that the pool’s manager is not acting in their interests. Nevertheless, we do acknowledge that Stratum V1 results in a certain principal-agent problem.

Moreover, most of the top five mining pools are based in China. While the miners joining them are not necessarily located in China, China-based operations made up a significant part (most likely over 50%) of global BTC mining until recently. This was largely due to cheap electricity and good access to manufacturers of mining equipment (the key producers are in China). However, China's recent crackdown on BTC, including a ban and effective shutdown of local mining operations in recent months, is resulting in a significant shift in the geographical footprint of mining. Here, it is worth pointing out that despite a near-50% decline in the global BTC hashrate (from the peak in May 2021) as a result of the crackdown, the BTC network continued to operate as usual, except for a temporary increase in the average time it took to add a new block to c 15–25 minutes (now back to the previous average of 10 minutes). This illustrates BTC’s resilience as a decentralised network.

Is BTC ownership highly centralised?

According to a recent report by Bloomberg citing Flipside Crypto, 95% of all BTC is controlled by only 2% of all BTC accounts, which would suggest strong centralisation of ownership. This could potentially be harmful for the network’s credibility, for instance by increasing its susceptibility to price manipulation.

However, a subsequently published report by Glassnode (a blockchain data intelligence provider) suggests that this figure is likely to be overstated, primarily because it assumes that a blockchain address is always equivalent to an account belonging to a single individual user. This is not the case for eg addresses belonging to crypto exchanges, miners and custodians. At the same time, network participants may control multiple addresses. Glassnode has prepared its own calculations by excluding known crypto exchange and miner addresses and applying a range of heuristics and clustering algorithms to identify addresses controlled by the same participant. The company concludes that 2% of network entities (ie individuals or institutions that control a set of addresses) hold around 71.5% of all BTC. Moreover, this is not adjusted for: 1) custodians, including eg BTC held in custody on behalf of Grayscale, the largest provider of crypto funds with AUM of US$31.2bn at end-June 2021; 2) lost coins, ie those whose owners have died, lost their private keys or broken the hardware devices storing the coins which, according to Glassnode, could represent c 3m BTCs (ie c 16% of the supply in circulation); and 3) coins held on exchanges, which are more likely to be small holdings of retail investors.

Beyond BTC: Varying degree of decentralisation

Altcoins vary greatly in terms of decentralisation defined as the distribution of entities participating in the network consensus and the degree of influence a single company/organisation has on the network. For instance, according to etherscan.io, there are c 9,000 nodes on the Ethereum network at present (although this figure may also cover light nodes which do not contribute to the network’s decentralisation). Like BTC, anyone can run a full Ethereum node (though at a higher cost versus BTC) and the network is not controlled or overseen by any single entity, but is rather developed by a broader community of developers, users, miners etc, although we acknowledge the influence which the non-profit Ethereum Foundation has on the network’s development.

On the contrary, Ripple (XRP) was introduced by Ripple Labs, a private company developing a blockchain-based payment network for financial institutions (RippleNet), which continues to oversee the XRP Ledger blockchain. The entire XRP supply (100bn coins) was minted by Ripple Labs on network launch in 2012 and the company has subsequently been funding its development via the continuous sale of XRP from its treasury. While anyone can run a Ripple node, each server on the network defines its own list of the nodes it trusts and accepts. Importantly, the

XRP Ledger requires a high degree of overlap between trusted nodes and Ripple Labs publishes its own proposed unique node list (UNL), which currently contains 47 nodes, including a few operated directly by Ripple Labs.