EDISON

Edison Explains

Bitcoin's investment thesis

Part four: Means of payment

Negative **Positive**

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.

Base layer not efficient for micropayments…

By eliminating the need for trusted intermediaries, the Bitcoin network addresses the complexity and inefficiencies of existing legacy payment systems used by banks (which in turn lead to elevated costs), most notably in cross-border payments. Having said that, while it was originally designed as a peer-to-peer system to address the shortcomings of legacy payment systems, it has shortcomings of its own. Its throughput, in terms of transactions the network can handle, has proved to be quite limited and stands at only around seven transactions per second (TPS), which compares to the Visa network at c 1,700 TPS, implicit in the company's statement that it processes 150 million transactions per day on average (it also claims that it can handle more than 24,000 TPS). As a result, it takes about 10 minutes to send a BTC transaction of any amount to another address on the network, which is definitely too long for micropayments (eg buying a cup of coffee).

Edison Insight

Bitcoin's base layer does not have the throughput to process a large volume of transactions per second. However, the Bitcoin Lightning Network (a scaling solution built on top of the main blockchain) is in the early stages of live implementation. Simultaneously, a number of alternative blockchain projects are competing with Bitcoin in challenging traditional payment systems.

Moreover, with the growing appeal of BTC as an investment asset and the resulting increase in transactions, the average fee charged by miners (who take part in the transaction validation process) soared visibly earlier this year and for a brief moment reached more than US$60 per transaction, according to bitinfocharts.com (although they have returned to relatively moderate levels of US$2.0–2.5).

…but still good for larger transactions

Nevertheless, while the base layer of the Bitcoin network is not an efficient system for everyday payments, it may still be considered an interesting alternative for larger transfers which do not have to be processed immediately. In this context, we note that transaction fees on the Bitcoin network are lump-sum payments, ie they do not depend on the amount being transferred. Moreover, the user is free to select a fee below the prevailing average rate if they are willing to wait longer for their transaction to be processed (ie added to a block) by the miners. While the acceptance of BTC and other cryptocurrencies as a means of payment is still at an early stage, there are already some prominent examples, such as the sale of a rare 101.38-carat diamond for c US$12.3m in cryptocurrency by Sotheby's (following the announcement that it will accept BTC or Ether in the auction).

Enter Bitcoin Lightning Network

Importantly, there are alternative payment solutions developed as so-called 'layer 2' solutions, ie built on top of the Bitcoin network, with the Bitcoin Lightning Network being the most prominent. It relies on a network of peer-to-peer connections (called 'state channels'), which can be opened between two parties to execute an unlimited number of

transactions off-chain (ie without being validated on the main blockchain). Only the net result of all these transactions will be recorded on the blockchain once the channel is closed. At present, transaction fees on the Bitcoin Lightning Network are significantly lower than the main chain and for small payment amounts do not normally exceed a few cents per transaction. The fee structure normally includes a minor fixed base fee plus a fee charged as a percentage of the transacted amount rather than a lump sum per transaction. Main blockchain fees are charged only on opening and closing the respective state channel.

The open-source tech stack of the Bitcoin Lightning Network allows it to handle a much greater number of transactions per second than is possible on the main chain. The exact figure is difficult to quantify, but in terms of the technological set-up, the throughput seems to be limited only by the speed of internet connection between parties. The main non-technological scaling limitation is the level of overall liquidity and its distribution throughout the network. This is because in order to send a certain amount of BTC on the Bitcoin Lightning Network, each of the peer-to-peer channels involved in the transfer needs to have sufficient liquidity to process it.

At present, the network is still at quite an early stage of adoption, with around 2,247 BTC (currently worth c US$104m) locked in the channels, according to bitcoinvisuals.com (representing only c 0.02% of the aggregate BTC free float market cap estimated by Coin Metrics). Some recent technological advancements, such as wumbo channels (which can be larger than the originally implemented cap of 0.1677 BTC, ie c US$7,759 per channel currently) and multi-path payments (which allow payments to be split into smaller amounts routed through different paths), should reduce the likelihood of a transfer failure due to insufficient liquidity. We also note that a small amount of BTC locked in the state channels can process a much larger transaction volume if it has a high circulation velocity. Nevertheless, we believe the amount of BTC locked on the Bitcoin Lightning Network needs to increase significantly for it to become a more widely accepted alternative payment system.

Nevertheless, the current state of the network allows for live commercial implementations, with some recent examples being Moon, Zap's Strike, Lastbit and Teslacoil (the latter is being developed by the listed company Arcane Crypto, an Edison client). Interestingly, Strike forms the basis for the roll-out of the BTC-based payment system in El Salvador, which recently adopted bitcoin as legal tender (ie its official currency) alongside the US dollar. Strike currently supports the remittance of money between users and is in the process of launching a Visa debit card for online shopping. Importantly, users do not have to keep a BTC balance to be able to use Strike – they keep their balance in fiat (ie in traditional currencies) and on remittance/payment, Strike converts the fiat money into BTC and transfers it over the Bitcoin Lightning Network. It then converts it back into fiat to credit the recipient's account.

We note that the Bitcoin Lightning Network is a nascent technology and not fully battle-tested yet. Because single transactions are not subject to the standard validation process carried out by network nodes on the main chain, the security level of the Bitcoin Lightning Network may be somewhat lower than the layer 1 network. Having said that, the Bitcoin Lightning Network has its own security features, with transactions in a given channel secured by so-called Hash Timelock Contracts (explained by the Binance Academy). However, given that the network remains at the development stage, it may contain vulnerabilities that could potentially be exploited by a malicious actor (using tactics such as 'griefing', 'flood and loot', 'time-dilation eclipse' or 'pinning'). Consequently, the technology is yet to be tested during mass deployment. As the first large-scale implementation of the Bitcoin Lightning Network, investors will be keen to follow the progress of El Salvador.

It is also worth noting that BTC's high price volatility somewhat limits its appeal as a means of payment on a standalone basis. However, at least some of the currently developed platforms utilising the Bitcoin Lightning Network have an embedded instant hedging solution to mitigate this problem. Meanwhile, merchants accepting BTC payments on the base layer normally indicate a time window for the user to complete a payment (which needs to be confirmed by the network to be accepted by the merchant). This may cause issues if the user finalises the BTC transfer after the time window closes.

Beyond Bitcoin: A race for scalability

Several other blockchains offer (or promise to offer) higher throughput in terms of TPS versus Bitcoin's base layer. However, before we discuss some examples of competing solutions, we need to flag that each blockchain's design is determined by a trade-off between scalability at the base layer in terms of transaction throughout and the level of the network's decentralization and security. While Bitcoin's base layer has limited scalability, it is at the same time highly decentralized in terms of the number of nodes (which are relatively inexpensive to operate, see Part 2 of this Edison Explains series for details).

Litecoin (one of the oldest altcoins) has an estimated capacity of 56 TPS and an average block confirmation time of 2.5 minutes (versus c 10 minutes for Bitcoin). Ripple has a throughout of more than 1,500 TPS, although this is at least partly due to the greater centralisation associated with its system of trusted nodes. Ethereum is currently undergoing a multi-phase upgrade (called Serenity) involving, among other things, a change in the consensus mechanism (from 'proof-of-work' to 'proof-of-stake') and the introduction of so-called 'sharding' (see our report, Blockchain adoption: Implications for the financial services sector, for details), as well as roll-ups (a layer 2 solution for the off-chain aggregation of transactions inside an Ethereum smart contract). The update is aimed at

increasing the scalability of the network from c 10–30 TPS at present to potentially 100,000 TPS. Solana, one of the major Ethereum challengers, allegedly has a theoretical peak capacity of 65,000 TPS without any layer 2 solutions (although this is based on Testnet results rather than live implementation).

The above is just a selection of the plethora of competing projects seeking to improve the scalability of blockchain-based transactions to be able to compete with traditional payment systems. An alternative means of payment utilising these blockchains can either be their native cryptocurrencies or so-called stablecoins, that is cryptocurrencies whose value is pegged to a fiat currency (eg the US dollar). Firstly, the price volatility of stablecoins is much lower than BTC and major altcoins (and comes almost entirely from the volatility of the underlying fiat currency), which means no additional hedging solutions are required. Secondly, while the main stablecoins backed by commercial players such as Tether and USDC were originally implemented on the Ethereum network only, they have since been expanding to other blockchains as well, providing the flexibility to utilise more efficient networks as they emerge.

A distinct subgroup of stablecoins is Central Bank Digital Currencies (CBDCs), which are being considered or already developed by several countries, although we believe that, except for China, their implementation process is at a very early stage and could take several years, hence representing a long-term rather than near-term threat for BTC as a means of payment. Importantly, as already discussed in Part one of this Edison Explains series, Bitcoin is not merely a payment processing system, but an independent, alternative monetary system.