EDISON

Edison Explains

Bitcoin's investment thesis

Part three: Durability and transferability

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.

Wealth accessible from anywhere in the world

BTC is a purely digital asset, which means it cannot be destroyed as long as the blockchain network remains intact. Moreover, someone who keeps its BTC in self-custody can access its wealth from anywhere in the world without any financial intermediaries – as long as they have an internet connection and access to the software or hardware wallet used to store the private key (an alphanumeric string used to sign transactions on the blockchain network). Finally, it can be easily transferred to any other address on the global Bitcoin network, normally within c 10 minutes. This represents a clear advantage over gold, which is more difficult to store and move quickly and securely.

Having said that, its holder needs to safeguard their private key, as losing it means losing the BTC holdings forever without any recourse. The story of a German programmer who forgot the password to his hard drive containing more than US$200m worth of BTC made the headlines earlier this year.

Edison Insight

BTC and other cryptocurrencies exist exclusively in a digital form on the blockchain and thus cannot be destroyed as long as the network continues to operate. Having said that, it is vital to safeguard the private keys used to sign transactions on the network. There are already multiple professional custody solutions available to both retail and institutional investors.

Multiple solutions to protect private keys are available

However, we note that the storage solutions currently available for digital assets eliminate this risk (the programmer received his BTC back in 2011, according to The New York Times, when these solutions were not widely available). Retail investors who decide to use self-custody for their digital assets can choose from a range of dedicated online and software wallets which, on set-up, ask the user to create a so-called 'recovery seed' or 'recovery phrase'. This is basically a list of 12, 18 or 24 words (preferably kept offline, eg written down and stored in multiple physical locations) that contain all the information required to recover a wallet if the user forgets their password, or their computer or any other device on which a software wallet is installed is damaged or lost/stolen. Another back-up solution is a Shamir Secret Sharing Scheme, which divides the private key into several parts which are distributed to other people or devices. In order to recover a wallet, all parts but one need to be recombined.

Investors who hold their BTC in self-custody may enhance the security level by using a hardware wallet, a dedicated device for storing private keys in cold storage (ie offline) and used to validate all digital asset transactions. Importantly, private keys never leave the hardware wallet, which protects the user from potential computer hacks. Users of hardware wallets also create a recovery seed. There are several providers of hardware wallets, with the two of the most recognised being Ledger and Trezor.

An example of a Ledger hardware wallet

Source: Unsplash

Third-party custodians for institutional investors

Furthermore, there are currently more than 100 companies providing professional digital assets custody services, which are particularly used by high-net-worth individuals and institutional investors. These companies normally offer a combination of secure hot (ie online) storage and cold storage on hardware security modules (HSM), ie physical computing devices that safeguard and manage digital keys. HSMs are usually certified (eg to Federal Information Processing Standard (FIPS) 140-2 Level 2 or 3) and stored in much the same way as high-value physical assets such as artwork or gold bullion, with high levels of security (eg biometric ID, armed guards, CCTV) and protection against fire, flood or power outages. In addition, custodians are putting in place insurance with companies active in the space, such as Aon, Lloyd's of London and Munich Re.

Some custody providers have attracted the attention of top tier banks and other financial institutions. For instance, Deutsche Börse recently acquired a controlling stake in Crypto Finance for US$108.6m, while BNY Mellon participated in the US$133m Series C funding round of Fireblocks. Moreover, several of the larger exchanges have acquired specialist crypto custodians, for example Coinbase acquired Xapo's institutional business in August 2019 for US$55m.

Assets kept on exchanges are more exposed

It is worth bearing in mind that digital assets kept in hot storage on centralised exchanges are more vulnerable to theft via hacking. In 2020, close to US$300m was stolen from cryptocurrency exchanges, according to the 2021 Crypto Crime report by Chainalysis. The vast majority of this represents the KuCoin hack in September 2020 (carried out by the North Korea-aligned cybercriminal syndicate Lazarus Group according to Chainalysis) when c US$275m was stolen. However, the exchange was able to recover roughly US$240m and covered the remaining amount from its insurance fund. Consequently, there was no permanent loss for KuCoin's customers. We note that top tier exchanges keep the majority of their customers' digital assets in cold storage (which is safer), with the remainder held in hot storage to maintain liquidity for withdrawals.

Some crypto exchanges have turned out to be scams, with some of the most infamous examples being Mt. Gox (2014) and Quadriga (2019). The most recent case, which seems to be an exit scam, is the largest South African crypto exchange Africrypt, whose founders have gone missing with US$3.6bn worth of BTC. Moreover, it is important to choose an exchange that has secure and efficient withdrawal protocols. Last year, the OKEx exchange temporarily froze any withdrawals after being 'out of touch' with one of its keyholders (who was part of a multi-signature approval process for withdrawals) as he was 'cooperating with a public security bureau in investigations', according to an announcement from OKEx. This suggests that investors should select their crypto service providers (including exchanges and brokers) carefully, focusing on well-established and reputable players with solid internal procedures.

Beyond Bitcoin – altcoins share BTC's features

Much like BTC, altcoins are easily accessible and transferable, and involve similar custody solutions associated with safeguarding the private keys attached to a given network address (ie public key). Having said that, each of the above-mentioned custody solutions supports a finite set of most popular altcoins, although the list can be quite extensive (as an example, see here for a list of coins supported by Trezor's hardware wallets).

Apart from hot storage on crypto exchanges, cryptocurrencies can also be more exposed to theft when locked in decentralised finance (DeFi) applications. DeFi stands for a global, open alternative to the existing financial system, granting all users free access to financial products such as borrowing, lending, saving, trading and payments (including those utilising fiat-linked cryptocurrencies called stablecoins such as Tether or USDC) without the need for traditional intermediaries and in a 24/7 set-up. It is being developed on blockchains which host so-called 'smart contracts' (which we discussed in detail in our previous report, Blockchain adoption: Implications for the financial services sector), most notably the Ethereum network, but also others such as Solana, Binance Smart Chain, Tezos, EOS, Tron or Stellar.

While truly revolutionary, it is still a nascent industry with the respective DeFi projects varying in terms of security. As the DeFi boom gathered pace starting last year, the attention of hackers increasingly turned towards these projects. Of the US$523.3m worth of cryptocurrency stolen in 2020 (including the above-mentioned exchange hacks), more than US$170m was stolen from DeFi platforms, according to Chainalysis. One of the key weaknesses exploited was vulnerability to price manipulation attacks, that is manipulation of external sources of asset pricing data (called 'oracles') on which DeFi platforms rely, especially with the use of so-called 'flash loans'. One of the main solutions to this vulnerability is the use of a network of decentralised oracles, such as Chainlink's.