EDISON

Edison Explains

Bitcoin's investment thesis

Part seven: A tool used in illicit activity

Negative **Positive**

Cryptocurrencies: Irrational hype or financial revolution?

Bitcoin (BTC) and other digital assets have been making 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.

Darknet: An early Bitcoin network adopter

Every human innovation has some unwanted/illicit use cases. As the worldwide web is being misused by criminals active on the dark web, BTC is also being misused as a currency for illicit activity. One of the Bitcoin network's (Bitcoin's) early adoption drivers, which provided it with the initial visibility to take off, was the Silk Road. The Silk Road was an online black market (founded in February 2011 and shut down in October 2013 by the FBI) where users were allowed to buy and sell any goods for BTC (as long as these were not causing any harm to a third party) and was primarily used for trading drugs. As a result, BTC earned a reputation as a currency used primarily for illicit activity.

Edison Insight

While the darknet was one of Bitcoin's early adopters, the current share of illicit activity in total cryptocurrency transaction volumes seems minor according to the data from major blockchain analytics companies. Nevertheless, BTC is appealing for some criminals due to its fungibility, ease and speed of use, as well as perceived anonymity (although Bitcoin in fact is not anonymous, but pseudonymous).

Illicit activity now a fraction of all BTC transactions

BTC has evolved since its early days and in 2020, illicit transactions made up less than 0.5% of Bitcoin's yearly volume, according to the 2020 Cryptocurrency Crime and Anti-Money Laundering Report of CipherTrace (which was recently acquired by MasterCard). Similarly, Chainalysis (a blockchain analytics company regularly working with law enforcement including the FBI) estimated in its 2021 Crypto Crime Report that the value of BTC and other cryptocurrencies sent by illicit entities represented a mere 0.34% of total cryptocurrency transaction volume. This compares with the amount of money laundered globally per annum worth c 2–5% of global GDP, according to the United Nations Office on Drugs and Crime. Still, it is worth examining the types of criminal activity involving BTC, which can be divided into: 1) scams, 2) darknet markets 3) ransomware, 4) stolen funds, 5) evading sanctions and 6) terrorism and extremism financing. We exclude scams and stolen funds from the analysis as we do not consider it an illicit use case of BTC and other cryptocurrencies, but rather an exploitation of the system itself (the same way a bank robbery is not considered the use of the banking system for illicit activity).

Bitcoin is used for criminal activities mainly because of its three features: **1) fungibility** – it represents a universal means of payment globally, which can be used for example to demand ransom from a victim but also pay all the providers across the criminal's supply chain, **2) ease and speed of use**, including transferring value across borders and jurisdictions, and **3) perceived anonymity** (we discuss this in detail below).

BTC in darknet markets today

Similar to the Silk Road in 2011–13, cryptocurrencies are a convenient means of payment on today's darknet markets, whose aggregate revenues have grown from below US$0.5bn in 2015 to US$1.7bn in 2020, according to Chainalysis. Interestingly, growth over the last three to four years was largely attributable to one particular marketplace: Hydra. Hydra is by far the largest darknet market globally with cryptocurrency volumes of c US$1.37bn in 2020 (representing over 75% of global darknet revenue), according to a joint study by Flashpoint Intel and Chainalysis. It serves exclusively Russian-speaking users and is a marketplace for drugs (utilising an Uber-like delivery service), stolen credit cards, SIM cards and counterfeit documents and IDs, among others. Hydra's high darknet market share is a combination of its 'organic' revenue growth and the shutdown of a number of other darknet marketplaces in recent years, such as AlphaBay Market (2017), Wall Street Market (2019) and Flugsvamp Market 2.0 (2020).

Ransomware attacks making the headlines

A ransomware attack occurs when an individual or group of individuals use technology to enter the victim's IT system and hold its data hostage (encrypt or steal it), demanding a ransom for unlocking/returning the data. In some cases, the attacker threatens to release a set of sensitive data to the public. According to an FBI release from February 2021, at least US$144.35m in BTC was paid out as ransomware ransom between 2013 and 2019. But in 2020, the total value of cryptocurrency received by ransomware addresses surged to US$350m (up 311% y-o-y), according to the above-mentioned 2021 Crypto Crime Report by Chainalysis (which the company admits may be understated given the level of underreporting by victims). This trend continued into 2021 with a number of high-profile attacks, such as the hack of the software vendor Kaseya in July (affecting between 800 and 1,500 businesses around the world, according to Reuters) with US$70m demanded in BTC. Further examples include the attacks on CNA Financial (which reportedly paid a US$40m ransom), Colonial Pipeline with 75 BTC (worth c US$4m at that time) paid by the company and JBS, one of the largest meat processing plants in the United States with c US$11m ransom paid in BTC.

Interestingly, a new business model called 'ransomware-as-a-service' emerged recently, opening the industry to entities that do not have the technical capability to create malware, but are willing and able to infiltrate a target organisation. In this model, the malware is created by the ransomware developer and then used by the so-called 'ransomware affiliate' to infect a system and demand/negotiate ransom. Following a successful attack, the ransomware developer gets their cut. While not being the sole factor driving an increase in ransomware attacks, cryptocurrencies (BTC in particular) have become a convenient means of ransom payment because of the features discussed above. A ransomware attacker is able to receive ransom in BTC and then use it to conveniently pay its service providers, including money laundering services, penetration testing services, exploit sellers or hosting providers.

Terrorist/local extremism and evading sanctions

Terrorist groups are soliciting donations in cryptocurrencies to purchase various services and goods, including weapons, training for its members, paying for international transportation costs, etc., though the extent of these activities seems to be limited at present. In August 2020, the US Department of Justice seized US$2.0m in cryptocurrency from terrorist groups such as al-Qaeda, ISIS and Hamas, the largest seizure from terrorist groups so far. Moreover, BTC donations are also used to finance local extremism. For instance, alt-right groups and individuals (such as Nick Fuentes) involved in the January 2021 Capitol riot received over US$500k in BTC from French donors one month prior, according to Chainalysis.

Finally, according to Elliptic, Iran is utilising its oil and gas resources to power domestic BTC mining operations and earn BTC, which can then be used to purchase imported goods and services to bypass sanctions. Elliptic estimated Iran's share in global BTC mining at 4.5% in a May 2021 publication.

Is Bitcoin really anonymous?

Bitcoin is not really anonymous – every transaction on the blockchain involving a given address is recorded and easily traceable. According to an analysis prepared by Michael Morell (who is a former acting director, deputy director and director of intelligence at the Central Intelligence Agency) and his team from Beacon Global Strategies, a CFTC official he consulted said that it is easier for law enforcement to trace illicit activity using Bitcoin than it is to trace cross-border illegal activity using traditional banking transactions, and far easier than cash transactions.

Having said that, without a proper know your customer (KYC) process, it is difficult to associate a blockchain address with a given person or organisation. For this reason, Bitcoin can be described as pseudonymous. Consequently, the attractiveness of being paid in BTC for criminal activities is dependent on the illicit actor's ability to launder the money before it is used in services imposing KYC procedures (both on-chain and upon converting crypto into fiat). Moreover, there are a number of further threats to Bitcoin users' anonymity, such as off-network information (eg email addresses, credit card and bank account details etc kept by organisations and services accepting BTC), temporal data, internet protocol (IP) address data and other side channels (see the research paper from F. Reid and M. Harrigan for details).

Most cryptocurrency exchanges have KYC/AML procedures in place and use blockchain analytics tools to find potential links of customer deposits to illicit activity. Still, there are certain jurisdictions that do not enforce these

regulations and exchanges in these locations can be used by the illicit actors. According to CipherTrace, a third of cross-border BTC volume is sent to exchanges with demonstrably weak KYC (which however does not mean that these funds necessarily originate from illicit activities). Criminals also use services called 'mixers' or 'tumblers' that help disguise the path of the illicit funds on the blockchain, primarily by pooling funds from different users in a series of addresses and then recombining these funds by sending them to addresses specified by the users (after deducting a fee). Other money laundering methods include peer-to-peer networks, cryptocurrency ATMs, prepaid cards, darknet services (eg the above-mentioned Hydra) as well as gambling and gaming sites (see Elliptic's blog here and here for details). Consequently, disrupting money laundering services is one possible way to derail illicit crypto activities. Interestingly, Chainalysis pointed out in its 2021 Crypto Crime Report that the number of relevant players across the ransomware supply chain is surprisingly limited, ie several key ransomware groups use the same money laundering services.

Beyond BTC: Privacy coins provide more anonymity

There are several cryptocurrencies providing greater anonymity than BTC, which are often referred to as 'anonymity-enhanced cryptocurrencies' (AECs) or 'privacy coins'. Some of the major coins by market cap that are considered to fall under this category include Monero, zcash and dash. According to the above-mentioned analysis from Beacon Global Strategies, the share of illicit transactions using privacy coins is visibly higher compared to BTC (although the latter is still dominant in terms of absolute volumes). Some darknet services and ransomware groups decided to abandon BTC and exclusively accept Monero (eg the White House Market and the ransomware group Sodinokibi). In an alleged ransomware attack on Acer in March 2021, hackers demanded US$50m in Monero.

However, we note that last year, a number of major exchanges decided to delist several privacy coins (eg the South Korea-based Bithumb and the Dutch LiteBit). There is also increased regulatory and banking pressure to limit their use and create barriers for privacy coins. Finally, in the case of particularly large-scale illicit activities, the attacker may still prefer BTC due to its superior liquidity (as it currently represents c 41% of total crypto market cap, compared to Monero for example at just 0.2%).