BUT [INSERT NEW TECHNOLOGY] IS USED BY CRIMINALS

Benjamin Dean – Director, Digital Assets
16 Mar 2022

The digital asset ecosystem is not the wild west that it once was. It is getting safer and more regulated.

The past month saw the release of the Biden Administration's Executive Order on ensuring responsible development of digital assets[1] in the United States. This is one very clear example of a government in the process of assimilating this new technology into the existing legal and regulatory system.

In terms of law enforcement, we saw the arrest of two people accused of having perpetrated a hack of the Bitfinex exchange in 2016[2]. The equivalent of around USD$3.6bn in bitcoin was seized by authorities. The perpetrator of the hack of the decentralized autonomous organization (DAO), an early smart contract failure on Ethereum in 2016, was also allegedly identified via deanonymisation of transactions[3].

In the past, when the topic of cryptocurrencies was raised, many flatly responded, 'but cryptocurrencies are used by criminals'. The implied argument behind this statement is that cryptocurrencies are mostly used by criminals to perpetrate crimes – and/or cryptocurrencies are associated with criminal acts (e.g. hacking of exchanges). A cursory look at history suggests that the word 'cryptocurrencies' could be replaced with many technologies that (at the time) were new.

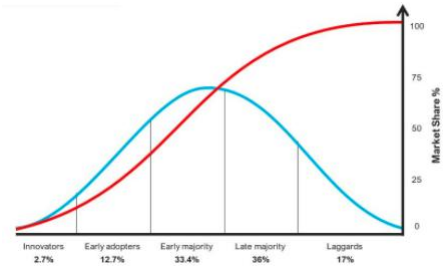
Spies, criminals and new technologies

Fears around new technologies are common – and can manifest in several ways. One way is to associate the new technologies with criminal activity. Indeed, this is the consequence of criminals being some of the first 'innovators' to use new technologies. In a constant cat-and-mouse game with law enforcement, criminals have to be innovative to stay ahead. This pushes them to use whatever newer, less well-known technologies and methods. Moreover, legacy or incumbent systems typically have measures in place to prevent criminal activity – pushing these people into alternatives as a consequence.

In the 19th century, the Telegraph (aka the Victorian Internet) was greeted with some fears. Writing on the parallels between the emergence of the telegraph and the internet, Tom Standage articulated the history of the use of the telegraph: "spies and criminals are invariably among the first to take advantage of new modes of communication. [then] the information supplied by the telegraph to businessmen was like a drug to businessmen [and finally the telegraph became] the handmaiden of commerce[4]". This is the adoption curve in three phrases – and is mirrored with the internet as well.

The history of the first railways in the United Kingdom was also greeted with some fears. One commonly held fear was that people from outside major cities could quickly travel to the city, commit crimes then quickly whisk themselves away. One of the stories that seriously raised public awareness of the railways was a crime committed by John Tawell (he put prussic acid in the stout of his mistress) after which he made a swift get-away aboard the next train to London. He was promptly arrested upon arrival, the authorities of his transit using the telegraph[6].
The recurrent pattern is as follows: As more and more people used new technologies, they came to see the benefits for themselves – thus their fears subsided. At the same time, governments take action(s) to mitigate the risks posed by the use of these technologies at scale. Privacy laws were enacted around telegraphs, safety laws passed for railways and so on. The same thing is happening with cryptocurrencies and digital assets.

The technology adoption curve



Source: https://www.slideteam.net/two-technology-adoption-curve-by-percentage-of-market-share.html

The point is that it is not uncommon for new technologies to be used for criminal purposes in their nascent phases. As new technologies move along the adoption curve – from discovery, commercialisation to eventual saturation – these concerns tend to subside. The benefits from new technologies manifest as new use cases and consequent diffusion throughout society render these technologies part 'of the furniture in the room[7]'. Confronted with the more visible risks at scale, governments take action in the form of greater law enforcement activity, regulation or legislation. Understanding this recurrent process is key when identifying the opportunities and risks that are created by new waves of technological change.

A short history of crypto crime – and government responses

The early association between cryptocurrencies and criminal activity has a lot to do with one of the ways in which it was proved that the technology worked. The silk road, an online market for illegal goods (especially drugs), became infamous in the years following its launch in 2011. At its peak buyers and sellers were exchanging Bitcoin for illegal goods at levels estimated to be between USD$15 million[8] to 45USD$ million[9] annually – until a series of FBI operations took the site down in 2013[10]. Many offshoots from silk road arose over the subsequent years – and were eventually stamped out by law enforcement[11,12].

Another type of criminal activity commonly associated with cryptocurrencies was hacking and theft. There have been many high-profile hacks of major cryptocurrency exchanges over the years – two of them have already been mentioned in the introduction to this article. Indeed there have been many instances of the owners of these exchanges walking away with users' funds – but the frequency and

severity of these incidents have reduced in recent years[13]. This reduction can be attributed to a consolidation of the sector, which has led to better cybersecurity through the increased scale of larger exchanges, increased regulatory scrutiny[14] and more recent efforts to disable the infrastructure of the groups that perpetrate these acts[15].

Fraud associated with so-called 'initial coin offerings' (ICOs) was rife in the years 2016-2018. This fraud involved issuing tokens, in the place of regulated securities, then misappropriating the money raised through these schemes. By some estimates up to 80% of ICOs were scams[16]. Again, regulators began applying pressure on particularly egregious examples[18,19], warned investors of these risks[19,20], and this kind of activity has now largely subsided[21].

Many other examples could be explored in depth: for example, tax evasion, ransomware, money laundering and evading capital controls. The list goes on. The point is that each of these problems is progressively dealt with by reactive government authorities as their costs become too big to ignore. This has been the case for centuries of technological progression and change.

Maximising benefits, minimising costs

The objection to cryptocurrencies as something 'used by criminals' has had some grounding in recent years – though this isn't unusual with new technologies.

The good news is that the digital asset ecosystem continues to grow and diversify, which means more use cases that benefit more people.

The other good news is that governments have been more active in addressing criminal acts associated with this technology. The Biden Administration's executive order on ensuring responsible development of digital assets[22] in the United States is just another example of a government in the process of assimilating this new technology into the existing legal and regulatory system.

To focus only on the negative side of the ledger would be to ignore many of the opportunities – and concomitant benefits that these technologies can bring. To dismiss digital assets as 'only used by criminals' would be tantamount to dismissing the railways – or telegraphs – based solely on similar early fears.

Sources

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[2] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[3] https://www.theblockcrypto.com/post/135017/new-research-claims-to-identify-the-man-who-hacked-the-dao

[4] Standage T. (1998), 'The Victorian Internet: the remarkable story of the telegraph and the nineteenth century's online pioneers'.

[6] Hylton S. (2015), 'What the railways did for us: the making of modern Britain', p69.

[7] https://www.collinsdictionary.com/dictionary/english/part-of-the-furniture

[8] https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf

[9] http://www.dailydot.com/business/silk-road-monthly-sales-black-market-drugs-study/

[10] https://web.archive.org/web/20140220003018/https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf

[11] https://portswigger.net/daily-swig/cast-no-shadow-history-of-darknet-market-takedowns-is-littered-with-opsec-fails

[12] https://en.wikipedia.org/wiki/Category:Defunct_darknet_markets

[13] https://selfkey.org/list-of-cryptocurrency-exchange-hacks/

[14] https://cointelegraph.com/news/compliance-is-a-journey-says-binance-ceo-amid-regulatory-scrutiny

[15] https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html

[16] https://www.frontiersin.org/articles/10.3389/frai.2021.718450/full#:~:text=According%20to%20Satis%20Group%20(Delisle,%24687.4%20million%

[17] https://techcrunch.com/2017/09/29/the-sec-has-charged-two-initial-coin-offerings-with-defrauding-investors/

[18] http://fortune.com/2017/08/29/sec-blockchain-ico-scam/

[19] https://www.fca.org.uk/news/statements/initial-coin-offerings

[20] https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf

[21] See table under 'Regulation': https://en.wikipedia.org/wiki/Initial_coin_offering

[22] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

Related blogs

+ What lies around the corner for digital assets
+ Digital asset networks are like train lines
+ Welcome to the metaverse

Related products

+ WisdomTree Crypto Mega Cap Equal Weight (MEGA / WMEG)
+ WisdomTree Crypto Market (BLOC / WBLC)
+ WisdomTree Crypto Altcoins (WALT / ALTC)
+ WisdomTree Bitcoin (BTCW / WBIT)
+ WisdomTree Ethereum (ETHW / WETH)

View the online version of this article here.

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

The application of regulations and tax laws can often lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.