Cryptocurrencies and future crime

Seven cryptocurrency-based crimes which could be achieved now or in the future are identified and ranked in relation to the level of harm they can or could cause.

Introduction

What are cryptocurrencies?

Cryptocurrencies are a form of digital or virtual currency that have become increasingly popular since Bitcoin, the first cryptocurrency, launched in 2009.[1] Cryptocurrencies use distributed ledger technology (DLT) to verify transactions, which are then added to a permanent digital record. The most familiar version of that record is the blockchain, as used by Bitcoin. On blockchains, transactions occurring in the same timeframe are compiled into a virtual list of transaction data on the ledger (i.e. a 'block') and validated through consensus by other users. The system was set up to be a cross-border payment platform that is peer-to-peer, with no third-party involvement or centralised legal oversight (such as a bank). Users can store their cryptocurrency in 'wallets' which consist of a public key (similar to an account number) and a private key (like a PIN code) that can be stored, such as on a user's hard drive, external storage media or online. In general, the identities of account-holders are said to be 'pseudo-anonymous'.[2] Whilst Bitcoin is the most widely known cryptocurrency, there are currently around 2700 actively traded different coins, although estimates vary between sources.[3]

How can they be used for crime?

In the first five months of 2020, crypto thefts, hacks, and frauds totalled $1.36 billion.[4] Cryptocurrencies have a number of features which make them an attractive target for criminal activity, including the following:

- **Technical complexity and market volatility:** Consumers may have limited understanding of the concepts involved and be tempted to invest to 'get rich quick' leaving them vulnerable to scams.
- **Decentralised nature:** Cryptocurrency exchanges (businesses which allow users to convert coins into other cryptocurrencies or fiat – "traditional" – currencies) are largely centralised and required to register with the Financial Conduct Authority through UK regulation. However, the cryptocurrency industry is, still a decentralised network with no central administrator, so accountability for law enforcement is not always clear.[5]
- **Anonymity:** The public blockchain records transfers, but they are linked to pseudonymous users. However, law enforcement agencies are able to use a variety of new forensic techniques and tools to analyse illicit flows of Bitcoin.
- **Ability to facilitate cross-border payments:** this could present an attractive opportunity for globalised criminal groups requiring borderless financial channels.[1,5]

Current regulation

Most cryptocurrency exchanges are now subject to anti-money laundering and counter terrorist financing (AML/CTF) regulation. The Financial Action Task Force (FATF) – the global watchdog for AML/CTF regulations – stipulated that from June 2020, virtual asset service providers (VASPs) must comply with the same financial crime standards that already apply to traditional financial institutions (such as banks).[4] However,

[1]House of Commons Library, 2020. Cryptocurrencies. Briefing paper 8780. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-8780/

[2]Financial Action Taskforce, 2014. Virtual Currencies. Key definitions and potential AML/CFT risks. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[3]Estimate from Nomics crypto data. https://nomics.com/

[4]Financial Action Taskforce, 2020.Virtual Assets. Available at: https://www.fatf-gafi.org/

[5]RUSI, 2017. Virtual Currencies and Financial Crime. Available at: https://rusi.org/publication/occasional-papers/virtual-currencies-and-financial-crime-challenges-and-opportunities

domestic regulators for National Governments must implement the requirements individually, which is not a matter of simply copying them.[6] In January 2020, changes to the UK's Money Laundering regulations came into force to include businesses carrying out crypto asset activities, to meet the FATF standards and the UK's obligation to transpose the EU's Fifth Money Laundering Directive into UK Law.[7] The 'Cryptoassets Taskforce' was set up in 2018 by the Chancellor of the Exchequer, consisting of HM Treasury, the Financial Conduct Authority (FCA) and the Bank of England. The Taskforce concluded that, while the use of crypto-assets for illicit activity remains low, these risks are increasing and the use of crypto-assets for money laundering is growing.[8]

Sandpit activity

Through a systematic review of the literature, this scoping study identified seven categories[9] of crime that could be facilitated by cryptocurrencies. At a two day 'sandpit' event, these were then ranked by 27 experts including representatives from academia, the police, the defence sector, the fintech industry and government in terms of:

- **Harm:** to individual victims or society.
- **Criminal profit:** for an individual or crime group.
- **Feasibility:** The readiness of the technology, its availability and the practicalities of achieving the crime.
- **Difficulty of defeat:** The difficulty of preventing, detecting or rendering the crime unprofitable. Consideration was given to whether measures would be obvious, simple or complex, and whether or not it required behaviour change.

The results of the cryptocurrency 'problem scenario' identification and ranking exercise are shown on the next two pages.

The future of cryptocurrency-based crime

This study found that extortion (ransomware), pump-and-dump schemes and money laundering using Bitcoin ATMs were perceived as the most profitable and feasible cryptocurrency-based crimes from the scenarios selected. Extortion (ransomware) was also seen as the most harmful crime. At the time of the sandpit, participants highlighted the need for regulation and international cooperation as countries responded to cryptocurrencies in different ways. The work of the FATF has begun to lead to wider coordination.

Sandpit participants did not have a shared view on how widespread the future uptake of cryptocurrencies is likely to be. However, it is clear that a number of crimes could be, and in some cases already are, enabled and accelerated by cryptocurrencies and there are opportunities for fraud based on its unique features.

This report exclusively focuses on the crimes identified at the sandpit event. A full report will be published later this year with a comprehensive overview of the field.

Future work

The scoping review of cryptocurrency crime highlighted that most work in this emerging field of research looks at only one type of cryptocurrency (Bitcoin). As a result of this study, The Dawes Centre has funded two new PhD projects which will look at the following to address key gaps in current understanding:

- Computational approaches to understanding cryptocurrency crime on a large scale; and
- Assessing the evidential requirements for cryptocurrency-related criminal prosecution and facilitating these using automated information extraction methods.

About the authors

Eray Arda Akartuna eray.akartuna.17@ucl.ac.uk
Florian Hetzel florian.hetzel.14@ucl.ac.uk
Dr Bennett Kleinberg bennett.kleinberg@ucl.ac.uk

Funders

This research was funded by the Dawes Centre for Future Crime at UCL. The Centre was established to identify how technological, social or environmental change might create new opportunities for crime and to conduct research to address them. The Dawes Centre is funded by the Dawes Trust and UCL.

Find out more

To find out more about the research reported here, see Dawes Centre at: www.ucl.ac.uk/jill-dando-institute/research/dawes-centre-future-crime or email vaseem.khan@ucl.ac.uk

This briefing was developed with the Policy Impact Unit. Find out more at: http://www.ucl.ac.uk/steapp/PIU or email PolicyImpactUnit@ucl.ac.uk

[6] RUSI, 2019. From Intention to Action. Next Steps in Preventing Criminal Abuse of Cryptocurrency. Available at: https://rusi.org/sites/default/files/20190911_intention_to_action_web.pdf

[7] FCA, 2020. Money Laundering Regulations. Available at: https://www.fca.org.uk/firms/financial-crime/money-laundering-regulations

[8] Cryptoassets Taskforce final report, 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf

[9] An eighth scenario, 'cryptocurrency owners as targets for extortion', was discussed at the sandpit. It was removed here given its close relation to the extortion (ransomware) scenario which is included.

Crime **Crime dimension ranking key:** ● Low ●● Medium ●●● High	Harm	Criminal Profit	Feasibility	Difficulty of defeat
Extortion (ransomware) Cryptocurrencies have helped to enable ransomware as a form of extortion. The most typical crime involves the use of malware to encrypt files on a victim's hard drive, making it impossible for them to decrypt and access them. To regain access, the victim has to pay the criminals, typically with cryptocurrency. While there is always the risk that the criminals will not decrypt the files after payment, they often do, which incentivises payment. This malware can have devastating effects on institutions (especially those relying on older technology, such as hospitals). Cryptocurrencies provide a means for offenders to receive payment from anyone with internet access, and in a way that can be more difficult to trace than a regular bank account. This crime rated highly for all four crime dimensions – they can be most harmful in denying access to essential IT systems and their prevention depends on humans' alertness of not becoming victim of standard cyber crime methods (such as phishing) which are often used to initiate these attacks.	●●●	●●●	●●●	●●●
Pump-and-dump schemes A common form of market manipulation where criminals purchase quantities of low-cost stock, and then artificially inflate the price (often through misinformation) before selling off their holdings. This also happens in the cryptocurrency space: bad actors purchase low market-capitalisation cryptocurrencies (meaning they are a lower price and have a smaller circulation supply) and then attempt to inflate the price by spreading misinformation and orchestrating a group buy of the coin to give the impression outsiders are buying it. This scam preys on people's fear of missing out. Pump-and-dump schemes ranked highly for profitability, feasibility and difficulty to defeat, but were seen to be the least harmful issue, perhaps because there is no particular victim and those involved are aware of the risk of speculative trading activities. However, such schemes could be harmful to the confidence and integrity of the market in question.	●	●●●	●●●	●●●
Money laundering: Bitcoin ATMs Bitcoin ATMs allow users to purchase cryptocurrencies in a physical location, with potentially illicitly acquired cash. The ATM will either scan a QR code on the user's phone or print out a receipt with a QR code that users can scan in order to transfer the cryptocurrencies into their own wallet. Bitcoin ATMs are not intrinsically criminal, but the worry is that they can facilitate money laundering (as in the case of money mules - see below). Most Bitcoin ATMs can require that a user identify themselves with some form of government ID, but whether this is required is up to the owner of the machine. In some jurisdictions, there is a legal requirement that ID is mandatory for these types of transactions, so machine owners would be expected to comply with this. This still makes machines susceptible to criminal use if offenders are engaging with identity fraud. Bitcoin ATMs were rated highly for all dimensions except 'difficulty of defeat', perhaps because control could be imposed through stricter ID checks or by placing maximum withdrawal limits on bitcoin. To launder large amounts, other steps need to be taken by criminals (such as hiring money mules), which might lower the profitability of the crime.	●●●	●●●	●●●	●

Crime **Crime dimension ranking key:** ● Low ●● Medium ●●● High	Harm	Criminal Profit	Feasibility	Difficulty of defeat
Cryptojacking Cryptocurrencies are generated through 'mining', which rewards 'miners' with cryptocurrency in exchange for the computing power necessary to verify transactions (which involves solving complex mathematical problems). By using cryptojacking malware, criminals can hack into a computer (usually many, using a network of infected devices) and then use that machine's computing power to mine cryptocurrency, providing them with coins at no electricity cost to themselves. Victims are often unaware that this is even happening, making it a hard crime to detect. The amount (and hence costs) of computing power and electricity consumed in crypto mining make this a profitable crime. It was rated as difficult to defeat, given its difficulty to detect and the inherent challenge to make humans more "cyber aware".	●	●●	●●	●●●
Cryptocurrency theft: fake crypto wallets A custodial wallet provider simplifies the use of cryptocurrencies by managing the private and public keys for the user, making sending and receiving cryptocurrency a straightforward task. Wallet providers help to manage the private keys. Genuine wallets will leave the keys under the user's control and verify the user's identity before use. Fake wallets can be set up (in some cases they are even downloadable from app stores),[10] which can then steal the user's coins. Users must check the reputation of a cryptocurrency wallet to avoid these types of scams. This was rated lowest for feasibility relative to other crimes because criminals need detailed knowledge of the working mechanisms of cryptocurrencies. It rated higher for harm, because users could lose all of their crypto-assets.	●●	●●	●	●●
Crypto money mules A money mule transfers money on behalf of a criminal, often unwittingly. They are directed to take a cut and send the remaining money to different accounts under the criminal's control. It is usually a method that money launderers use to distance themselves from their illicit funds. This form of money laundering has existed outside of cryptocurrencies, but increasingly, mules are being asked to purchase cryptocurrencies (often from Bitcoin ATMs) and ordered to send cryptocurrencies back. Even if unwitting, mules are complicit in the crime. Participants were less certain about their potential to harm and the difficulty of defeat than with other crimes but the crime is arguably closely connected to the problems around Bitcoin ATMs.	●	●	●●	●●
Investment scams Investment scams are not new, but cryptocurrencies offer a new type of investment scenario that scammers can use, which take various forms and levels of sophistication. For example, scammers use social media and images of celebrities to convince potential victims to buy into some new 'initial coin offering', or other crypto investment. Images are presented along with fake quotes recommending that people make investments with the fraudulent company in cryptocurrencies such as Bitcoin. Alternatively, a link in the advert might take the victim to a page where they are required to input contact details so that they can be called back (and persuaded to invest). Some scammers offer high returns to tempt people into investing, but, they may offer realistic returns to make it appear more legitimate.[11,12]	●●	●●	●	●

[10] Coin Telegraph, 2019. Fake Crypto Wallet app imitating Trezor found on google play store. https://cointelegraph.com/news/fake-crypto-wallet-app-imitating-trezor-found-on-google-play-store

[11] FCA, 2018. Cryptoasset investment scams. Available at: https://www.fca.org.uk/scamsmart/cryptoasset-investment-scams

[12] Action Fraud, 2018. Well-known names being used in cryptocurrency scams. https://www.actionfraud.police.uk/news/well-known-names-being-used-in-cryptocurrency-scams