In the ten years since the Bitcoin whitepaper was published in October 2008, the value and overall number of digital currencies has increased dramatically. There have been vast technical improvements made by a community of developers dedicated to making currencies like Bitcoin as secure and scalable as possible. The rapid growth of Bitcoin and other cryptocurrencies have also led to the spread of financial crime in new and innovative forms.

In August 2005, FBI agents raided the house of Louisiana Congressman William Jefferson, also known as “Dollar Bill” Jefferson. They were looking for bribe money given to him by the FBI. Hidden in his freezer in boxes of Pillsbury pie crusts were bundles of cash in US$10,000 increments. The serial numbers matched the US dollars given by the undercover agent. “Dollar Bill” received 13 years in jail – one of the longest prison sentences ever given to a congressman.

One year before Jefferson’s sentence, a person or group of people using the pseudonym Satoshi Nakamoto published a whitepaper for a new digital currency called Bitcoin. The whitepaper’s title, “Bitcoin: A Peer to Peer Electronic Cash System” promised a new form of digital payments that used peer to peer networks for transaction verification instead of relying on financial institutions as trusted intermediaries.

If “Dollar Bill” had waited a few more years before beginning to take his bribes, he might have been able to use cryptocurrencies to hide his cash on a flash drive, instead of wads of dollar bills in a pie crust box.

Anonymizing funds are not the only innovation of cryptocurrencies. Its pioneering use of a decentralized ecosystem for making financial payments has a wide variety of uses for criminals looking to hide illicit profits. Political corruption, decentralized illicit markets, and elaborate scams are a few areas where digital currencies and decentralized environments help criminals hide illicit profits and activity.
Decentralized Illicit Markets

The use of centralized Dark Net Marketplaces and the incorporation of cryptocurrencies by criminals seeking to cover their illegal activities are well documented. Infamous Dark Net Markets like Silk Road, Hansa, and Alphabay have all been brought down by coordinated worldwide law enforcement actions. This is because they were centralized markets vulnerable to discovery, but decentralized online illicit marketplaces present more complex challenges. Decentralized markets are broader than a simple centralized market that can be shut down with the seizure of a server. These networks, with the incorporation of cryptocurrencies, have the potential to create a marketplace impervious to current law enforcement approaches. Projects such as “Open Bazaar” have proven that a decentralized marketplace can thrive when communities of dedicated supporters work as nodes to sustain the network, and cryptocurrencies are incorporated as a means to transact.

Parts of the open source community are developing a collection of decentralized tools to serve a growing community of users – including criminals - emboldened by the cryptographic security that decentralized systems and private cryptocurrencies offer. One example of this transition from centralized markets to decentralized ones is the case of Backpage.com, which was taken down by the U.S. government. Backpage was a common marketplace used by human traffickers and pimps to promote prostitution and sell sexual services anonymously. Not long after the website was taken down, a decentralized version of the website was posted on GitHub that allowed users to download a version of the new site on a peer to peer network and host a node on their personal computer.

A decentralized online marketplace like Backpage.com will present substantial challenges to law enforcement armed with outdated laws and regulations. It cannot be taken down by seizing a server because there is no single server unlike most websites. Once the code is published, the community can continue to develop it and patch any flaws. No single administrator can be arrested because the administration of the site can be run by thousands of individuals globally. The creation of an illicit marketplace impervious to government takedown and utilizing private cryptocurrencies for transactions is one where its users can operate with little enforcement risk for their criminal behavior. Technology and the innovation of those seeking anonymity in dark net markets are quickly making this a reality, and right now it appears there is very little governments worldwide can do about it. Increased government investment in understanding the new technology can help find solutions to these emerging challenges.

Fraud

The rise of Bitcoin and other cryptocurrencies has enriched a small number of committed investors. These gains have been well publicized and created an environment where others sought to duplicate their success. Cryptocurrencies also opened the door to thousands of scammers looking to take advantage of potential investors. Fake Initial Coin Offerings (ICO), Ponzi schemes, pump and dump schemes and thousands of Twitter scammers are using the perceived promise of virtual currencies and crypto assets to defraud victims.

Fake ICOs are often the most complex scams, and involve many layers of false statements to get people to invest. Fake websites, Twitter, LinkedIn accounts accompanied by a whitepaper often plagiarized from other projects create the appearance of legitimacy, convincing the investor that their currency is the next Bitcoin or Ethereum. One example of this was an ICO marketing the coin “Benebit.” Its purpose was to unify customer loyalty programs under one currency. The creators of the scam provided fake passport details, a telegram channel with 9,000 members, and a whitepaper explaining the concept of the coin and its purported value. After it was revealed that the photos of the founders were stolen from a UK school for boys, the team behind the scam began to remove all social media accounts related to the project. It is estimated that the scammers stole between US$2-4 million.

Federal Regulators, led predominantly by the SEC, are cracking down on fraudulent ICOs by educating the public about these scams and by prosecuting violators of key U.S. financial regulations, such as the Securities Exchange Act. However, the scale of the problem is larger than the government can adequately tackle at the moment, which has caused the relevant regulatory authorities to scramble to bring in talent tackle the issue. A recent study by the ICO advisory firm, Statis Group, revealed that in 2017 80% of the ICOs conducted were scams. With the development of the Ethereum network, creating a currency has become something the average programmer can complete in an afternoon. This rise in fraudulent investment scams degrades the potential of cryptocurrencies as a whole, and is an issue the U.S. government can crack down on with increased regulation and attention.
Corruption

As cryptocurrencies make their way into the mainstream, they could be used in areas like campaign financing, government procurement, and lobbying. The current policies on government or campaign financing have not evolved to incorporate the complexities of cryptocurrencies. The reporting of income and expenditures for these activities rely on traditional banking infrastructure to track funds. Some cryptocurrencies have privacy features that would make tracking those finances difficult. Privacy coins like Monero mix in valid previous transactions in order to obfuscate the details of the current transaction, something known as mixing, which has been shown through studies on cryptocurrencies to be almost entirely used for criminal purposes.

One of the largest holders of cryptocurrencies in the past ten years was Ross Ulbricht, founder of the Silk Road. Silk Road was an online illicit marketplace where users placed orders in Bitcoin and received drugs or other illicit items through the U.S. postal system. In 2013, the Silk Road was shut down, Ross was given a life sentence, and the U.S. government instantly became one of the largest holders of Bitcoin when they seized the Silk Road’s official Bitcoin wallet. The total amount of Bitcoin at the time was $33 million.

In 2015, two federal agents investigating the Silk Road case diverted some of its Bitcoin into personal wallets. They were able to do this because they had access to Silk Road’s digital wallet/private keys, allowing them to move the coins. Both agents were caught and sentenced to six years in prison. However, as privacy features of cryptocurrencies continue to improve, the ability to track the movement of these coins will become increasingly difficult, if not impossible. Privacy-centric coins such as Monero and Zcash have the sending address, receiving address, and amounts of the transaction obscured, which is key information to any investigation. Retaining the transparency of transactions is important in order to ensure an ethical transition in the use of cryptocurrencies, which extends into political campaigns and by government agencies.

Conclusion

Cryptocurrencies and decentralized ecosystems can provide value for societies looking to create transparency and accountability in their financial system. However, the advantages these new technologies give to criminals must not be overlooked. Decentralized illicit markets can provide drug dealers, arms dealers, terrorists and human traffickers a safe haven to conduct their transactions under the security and anonymity of a service that cannot be taken down.

The public must be educated about common cryptocurrency fraud schemes, and violators of U.S. financial regulations should be held accountable. Cryptocurrencies can be a valuable tool for creating accountability in politics, but it can also be used to conceal corruption. As corrupt politicians like Dollar Bill Jefferson move from storing their bribes in pie crust boxes to cryptographically sealing them onto a USB drive, the U.S. government must promote the use of currencies that creates transparency rather than concealment in order to safeguard the financial system.

Cryptocurrency trading organizations operate in what is arguably the highest risk regulatory space in the world – Refinitiv (formerly the Financial and Risk business of Thomson Reuters) is well recognized by regulators, financial institutions, and corporations as a best-in-class service provider able to navigate complex regulatory requirements, screen for customer and third-party risk, and help companies to minimize reputational risk and, ultimately, fight financial crime.

Visit refinitiv.com

About the author
Jack Burrus is a Research Analyst at Refinitiv. He covers emerging risk for the Washington D.C. research team, and focuses on topics such as cryptocurrencies, blockchain, human trafficking, and wildlife trafficking.