Published on Alvarez & Marsal | Management Consulting | Professional Services
(https://www.alvarezandmarsal.com)

March 28, 2018

Introduction

The historic rise in the price of bitcoin has led many to wonder how a virtual or crypto currency popularized by its use on Silk Road (commonly referred to as the "eBay of drug sales") may also be considered a store of value that others view as digital gold. To those scratching their heads, cryptocurrencies resemble the late 90's dot-com era, where success stories of early adopters making large gains have attracted a flurry of experienced venture capitalists and inexperienced retail investors alike. Yet, comparisons to the Internet don't stop there. Blockchain technology, the innovation behind cryptocurrency, has been compared to the next phase of the Internet itself. Whereas current Internet-based technology companies like Uber serves as one of the largest taxi companies while owning no vehicles, the blockchain promises to allow for trusted peer-to-peer transactions for anything of value *without* the need for any central authority.

As with any emerging technology, cryptocurrency offers potential benefits such as lower transaction fees, transparency and enhanced efficiency, but also presents new risks to consumers, governments and other institutions. As regulators continue to build their knowledge base around cryptocurrency, leverage analytical tools and enforce the law, it will become increasingly clear whether cryptocurrency and the blockchain will reach its full potential as Internet 2.0.

What are the Benefits of Cryptocurrency and Blockchain?

Blockchain represents the intersection of three technologies applied to create a new type of decentralized database: the Internet, cryptography and an incentivization protocol[1]. This mix of connectivity, security and incentives is facilitated by a cryptocurrency, with the result being a system for tamper-proof digital transactions where no trusted third party is necessary. The key benefits of cryptocurrency over government-issued currency are:

- Immediate settlement of transactions;
- Global access to anyone with an Internet connection or a mobile phone; and
- Greater protection from centralized hacking or misuse.

Thus, users can generate immutable transactions in seconds with anyone in the world while also protecting personal data from being revealed to third parties. Currently, the two top cryptocurrencies in terms of market capitalization are bitcoin and Ethereum, and they serve different purposes. Bitcoin, the first cryptocurrency to gain in popularity, was created in 2008 with the goal of becoming a digital currency with lower fees by being completely decentralized and independent of any government issued currency. Ethereum was created in 2015 as a platform to enable the creation of decentralized applications (DApps) built using "smart contracts," which is program logic committed to the blockchain to facilitate automatic and foolproof transactions between parties. Network participants are incentivized to power DApps based upon a cryptocurrency reward system within each respective

ecosystem.

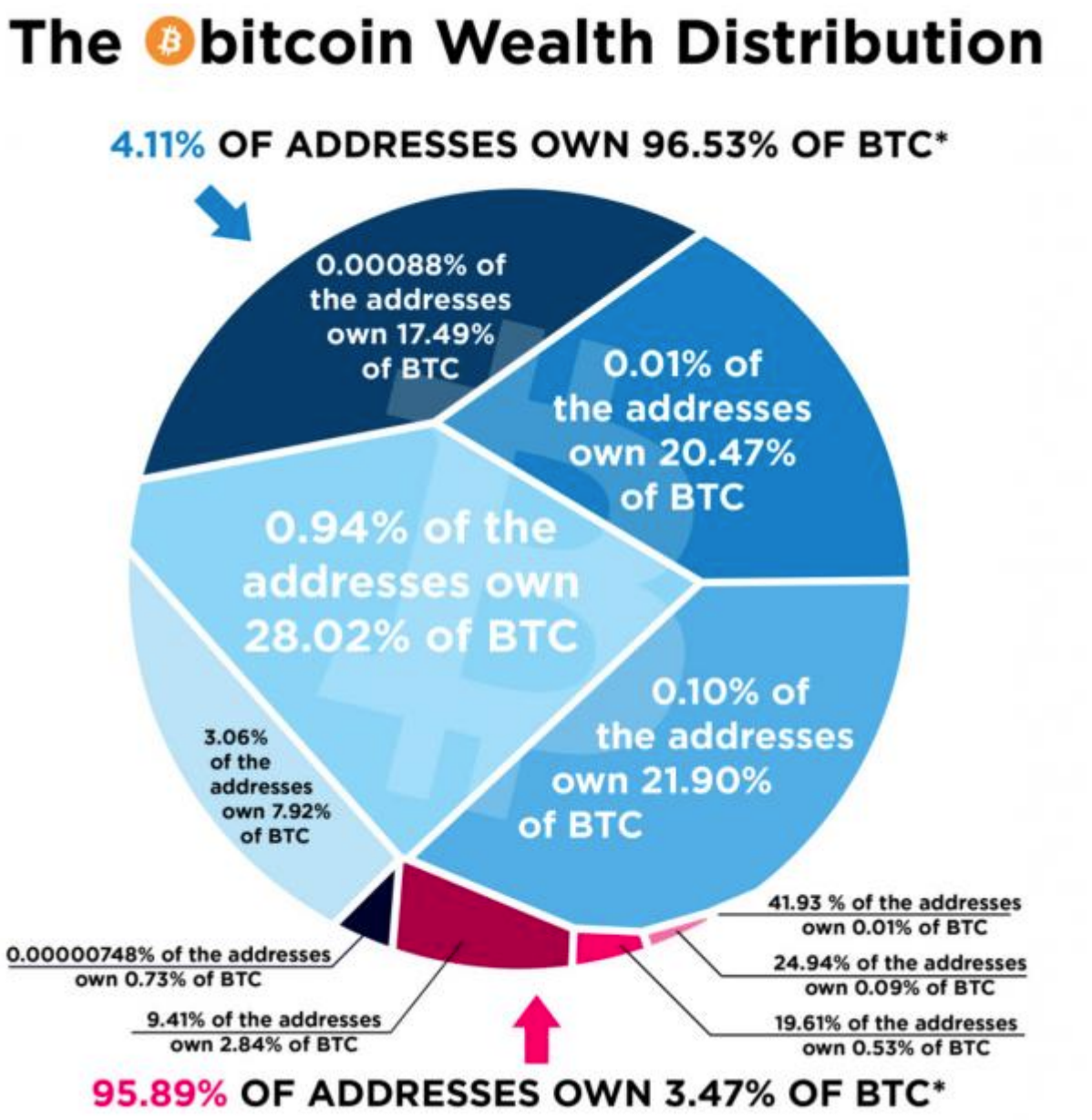
Key Risks of Cryptocurrency

While the transformational nature of cryptocurrency has attracted technology enthusiasts and investors alike, it also opens the door to criminal behavior, and thus many risks. Primarily, these fall into two categories:

- Fraud that exploits knowledge gaps and features of cryptocurrencies
- Criminal behavior perpetrated with cryptocurrency payments

Cryptocurrency Fraud

One reason that cryptocurrency is so susceptible to market manipulation and fraud is that its ownership is very highly concentrated.



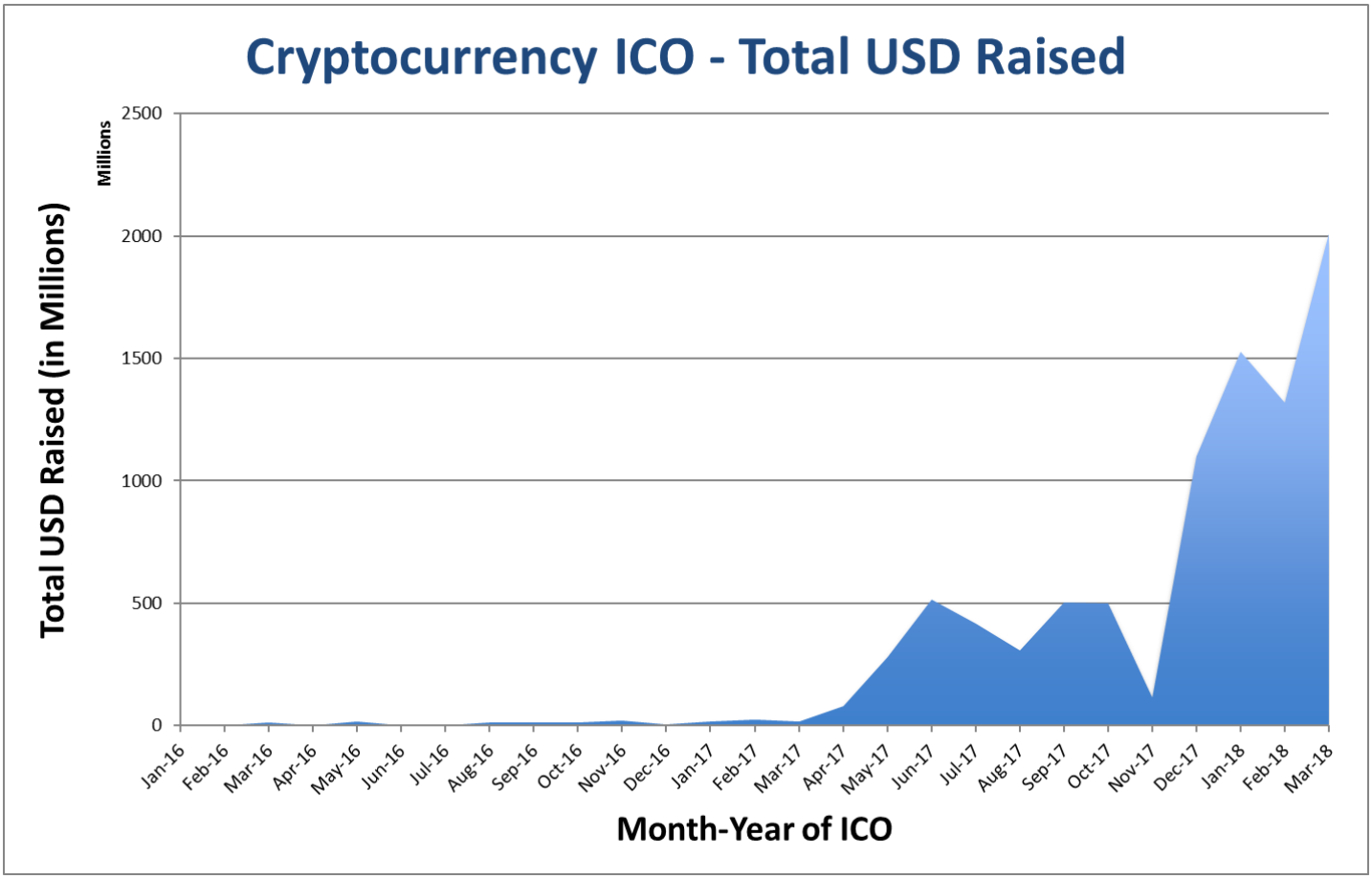
https://howmuch.net/articles/bitcoin-wealth-distribution

As per the chart above, since only about 4 percent of wallet addresses own over 95 percent of bitcoin, “large holders can collude to manipulate the price”[2] which raises red flags about the integrity of the market. As an example, an academic paper published by

the *Journal of Monetary Economics* found that one single bot was responsible for the rise in the price of bitcoin from $150 to $1,200 over a two-month period in 2013 on the Mt. Gox exchange[3]. Automated bots make coordinated purchases of low-priced coins to pump the price. Once new investors buy the pump, bots dump the asset.

Additionally, the rapid rise of fundraising for cryptocurrencies known as an Initial Coin Offering (ICO), has become an increasing concern for the Securities Exchange Commission (SEC), which seeks to protect investors from fraudulent coins and scams. ICOs have enabled start-up companies to quickly raise funding, but the quick-cash success stories have attracted both entrepreneurs and investors resembling the gold rush. However, unlike angel or venture capital investing which has clearly defined requirements for accepting accredited investors only, the easy access to ICOs has enabled virtually anyone with a computer or mobile device to invest in high risk companies. The month of March 2018 looks to be on pace for the largest amount raised, with almost $1.5 billion raised in only the first week.

ICO Fundraising January 2016 - March 6, 2018:



https://www.coinschedule.com/stats.html

The sharp rise in funding has opened the door to over a thousand cryptocurrencies, and regulators are still playing catch-up with new laws and regulations, inter-regulatory collaboration and increased enforcement actions.

Criminal Behavior Perpetrated with Cryptocurrency Payments

Cryptocurrency has become a popular mode of payment for malicious activity given its features by design; bitcoin is portable, easily transferrable, secure and seemingly anonymous. As a result, it has become a popular tool for money laundering, where the purpose is to separate a perpetrator's identity from financial transactions. For example, the recent "WannaCry" ransomware cyberattack in which compromised computers were frozen until payment was made in bitcoin is an example where bitcoin's anonymity promoted its use for criminal behavior. The malicious use of cryptocurrency is expected to continue not only to perpetrate cybercrime, but also as money laundering and malicious payment vehicles for white collar crime.

Combating Cryptocurrency Risks

While the market composition and features of cryptocurrency present major risks that may be exploited by criminals, the regulatory and investigative community are responding tactically to establish stronger governance and examination measures. These include:

- Increased focus by banking and securities regulators, law enforcement and the blockchain community
- Analytical platforms that marry digital artifacts, blockchain records and data from exchanges and other sources
- More stringent Bank Secrecy Act (BSA)/anti-money laundering (AML) and Know Your Customer (KYC) compliance programs to identify wallet owners and minimize risk of financial crime

Increased Focus by Regulators, Law Enforcement and the Blockchain Community

Cryptocurrency's main features are also its greatest risks. Early adopters and enthusiasts are typically tech-forward retail investors attracted to its global reach, quick and irreversible nature and anonymity. Alongside a rapidly growing universe, regulators and law enforcement are constantly playing catch-up, creating a perfect storm for criminals seeking to exploit new opportunities. To prevent such behavior, the regulator community is looking to create a federal framework for protecting investors from volatility, fraud and cyber risks present in potential exchange hacks, while also balancing the desire for innovation.

Regulating cryptocurrency falls into a gray area with necessary cross-regulator collaboration amongst the Commodity Futures Trading Commission (CFTC), SEC, the Treasury Department, Financial Crimes Enforcement Network (FinCEN), Internal Revenue Service (IRS) and state banking supervisors. For example, on March 7, 2018, a U.S. district judge backed the CFTC in defining cryptocurrencies as commodities noting, "Virtual currencies are 'goods' exchanged in a market for a uniform quality and value. They fall well within the common definition of 'commodity'"[4]. Also, the SEC has declared that digital tokens issued as part of ICOs represent securities, and that the "Howey test" should be used to determine whether certain transactions qualify as "investment contracts"[5]. Additionally, 20+ state, federal and international law enforcement agencies along with blockchain community have formed a public-private partnership known as the Blockchain Alliance to help make the blockchain ecosystem more secure and promote further development of the technology[6].

The SEC and CFTC are taking the lead in acting against criminals perpetrating fraud using cryptocurrencies. As an example, in December 2017, the SEC obtained an emergency asset freeze against PlexCoin, which promised investors more than a 13x return within a month[7]. Similarly, the CFTC filed civil charges in January 2018 against two alleged cryptocurrency fraudsters, one who took money to conduct trades and impart market tips, but instead took the bitcoin without providing anything in return, and another for creating a bitcoin Ponzi scheme masked as an investment vehicle for trading commodities[8].

Analytical Platforms That Marry Digital Artifacts, Blockchain Records and Data from Exchanges and Other Sources

Contrary to common belief, bitcoin is not fully anonymous since activities are available publicly on the blockchain. Examining the public blockchain with monitoring tools provides investigative insights into who is transacting and how much, such that one can trace movement of value through cryptocurrency. In addition, system artifacts such as system logs, web browsing history, emails and phone application usage can help identify potentially fraudulent transactions. Further, scraping structured and unstructured data sources for key identifiers and obtaining information from exchanges through subpoenas may provide additional insights on the use of cryptocurrency. Using the methods previously mentioned, cryptocurrency and the blockchain may instead enable visibility into an entirely new universe of transactions. As an example, the IRS is using software which deploys millions of tags to help track and identify transactions. Only 802 people declared a capital gain or loss related to bitcoin in 2015, while the price of bitcoin soared from around $13 to over $1100 between 2013 and 2015[9]. The software uses clustering methods to determine how bitcoins are typically aggregated or split up among wallets, and thus help to identify owners of bitcoin addresses.

More Stringent BSA/AML and KYC Programs to Identify Wallet Owners and Minimize Risk of Financial Crime

Lastly, since cryptocurrency exchanges are required to register as Money Service Businesses (MSBs), compliance with BSA/AML laws are critical for identifying wallet owners, as it serves as a key on-ramp for new investors[10]. Law enforcement may then identify the people involved in a potential crime, but need to gather evidence to determine what happened. In the case of cryptocurrency, the reverse is true where the crime is known, but law enforcement needs to identify the people. Thus, compliance with BSA/AML laws helps provide visibility into most bitcoin transactions. Developing a compliance program which is commensurate to the risk presented by the cryptocurrency, whether security token or utility token, with robust KYC compliance to meet the increasingly stringent regulatory requirements is critical for long-term success.

Conclusion

Cryptocurrency and the blockchain may revolutionize the Internet as we know it by removing middlemen from transactions. While market manipulation, fraud, money laundering and malicious payments may exist in the cryptocurrency world, these are people problems, and not design features of the technology itself. As with any widespread new technology that is changing constantly, gaps in knowledge and resources may be exploited by criminals, and a significant amount of education needs to occur for law enforcement, regulators and investors to catch up and stay current. However, stakeholders will continue to build the tools, skills and practice necessary to adjust to a constantly changing environment, and protect the public from criminal activity. To the extent that they're successful, cryptocurrency and the blockchain may be on its way to becoming Internet 2.0.

Read More Raising the Bar Articles

---

[1] https://www.coindesk.com/information/what-is-blockchain-technology/

[2] https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market

[3] https://www.cbsnews.com/news/bitcoin-cryptocurrencies-fear-of-market-manipulation/

[4] https://www.coindesk.com/us-judge-rules-cryptocurrencies-are-commodities-in-cftc-case/

[5] https://www.coinbase.com/legal/securities-law-framework.pdf

[6] http://blockchainalliance.org/

[7] https://www.forbes.com/sites/rogeraitken/2018/01/30/u-s-sec-halts-alleged-crypto-ico-scam-from-decentralized-bank-seeking-1-billion/#7759ebc394b0

[8] http://money.cnn.com/2018/01/19/technology/cftc-feds-bitcoin-fraud/index.html?iid=EL

[9] https://cointelegraph.com/news/only-802-people-paid-taxes-on-bitcoin-profits-irs-says

[10] https://www.trulioo.com/blog/bitcoin-regulation/

Source URL:https://www.alvarezandmarsal.com/insights/cryptocurrency-blockchain

Authors:
Steven Lee