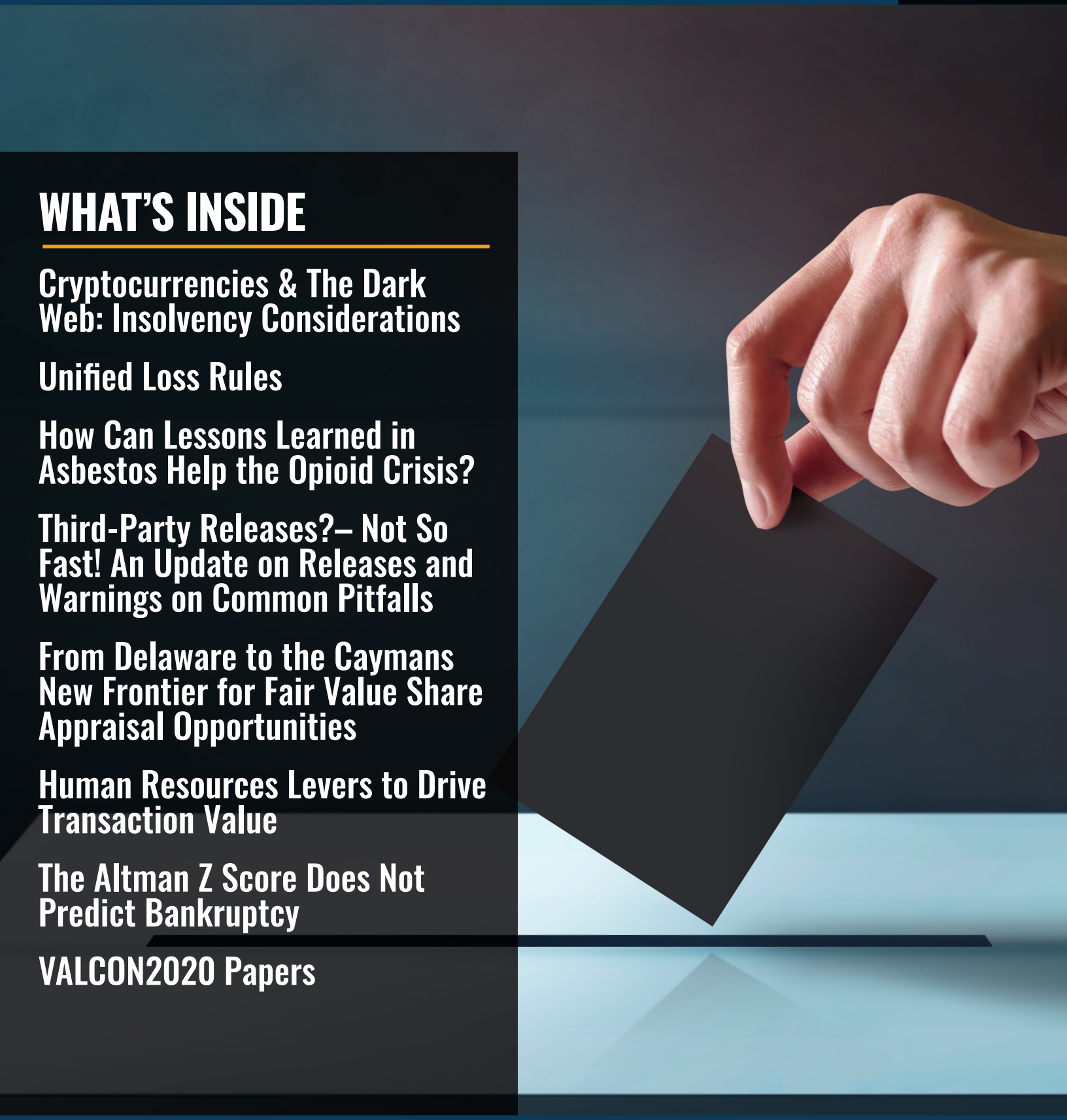
AIRA Journal

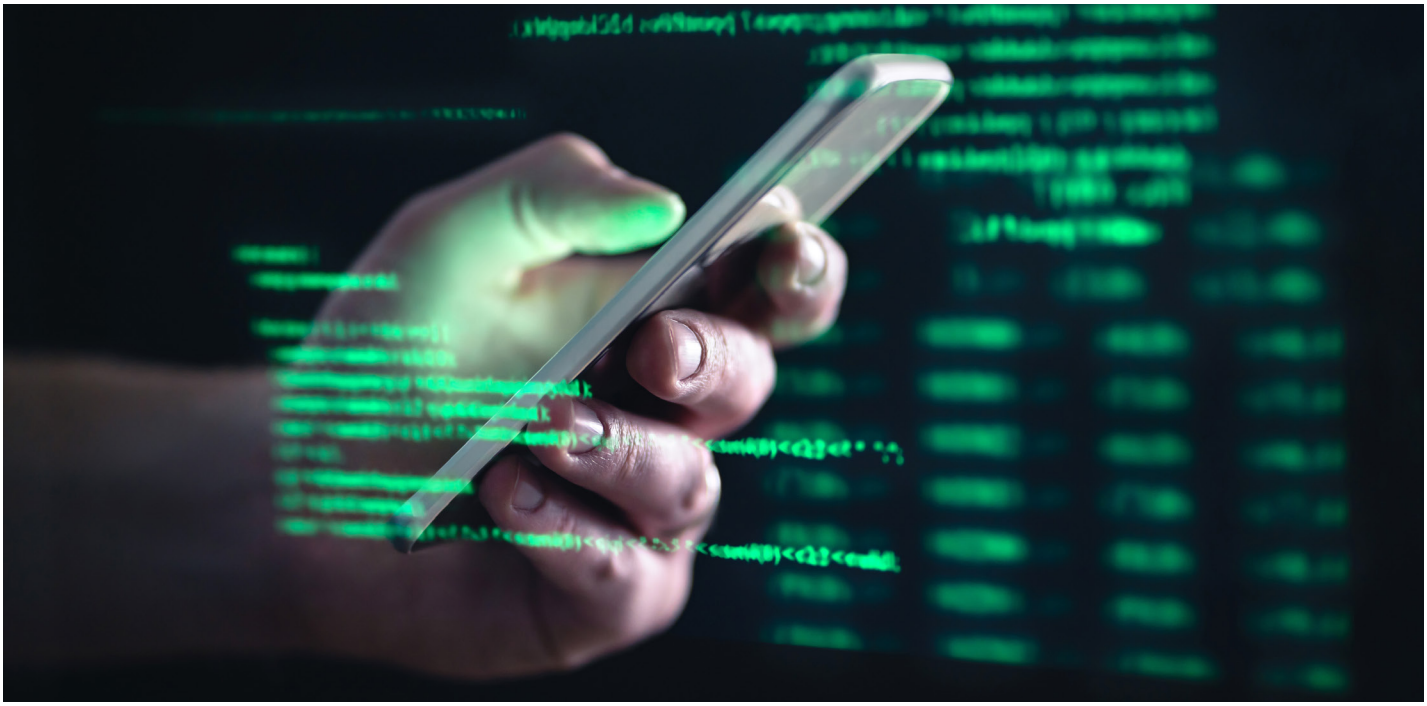
Volume 33
No. 3



WHAT'S INSIDE

CRYPTOCURRENCIES & THE DARK WEB: INSOLVENCY CONSIDERATIONS

REGINA LEE, CIRA, and DAVID WHITE
AlixPartners, LLP



Current Market Conditions

COVID-19 has created economic uncertainty in global financial markets. As a consequence of this volatility, cryptocurrency has become a more common potential source of liquidity and investor safe haven.[1] On October 8, 2020, US Attorney General William P. Barr stated "cryptocurrency is a technology that could fundamentally transform how human beings interact, and how we organize society."[2] On the same day, FBI Director Christopher Wray stated that the FBI sees "first-hand the dangers posed when criminals bend the important technological promise of cryptocurrency to illicit ends."[3] Criminals are always at the ready to exploit the fast-moving pace of technological advancement. The use of custodians to conduct cryptocurrency transactions creates additional risk to investors as opposed to direct transactions. As cryptocurrency custodians fail because of business reasons, fraud, or theft, it is important for investors to understand the risks associated with asserting claims against a bankrupt crypto custodian.

Crypto as Currency

Criminals are always looking for ways to exploit weary investors. Cryptocurrencies are no exception. As these new financial transaction payment methods rapidly gain acceptance worldwide, so too have they become a prime target for hackers and fraudsters. Advances in chip and pin technology, better security protocols and better fraud detection by banks have all made credit card fraud and identity theft far less lucrative than they used to be, turning criminals toward more fertile grounds. Another driver is the rapid deployment of new and often ill-tested cryptocurrency technologies in the race to go to market, often with major vulnerabilities. Cryptocurrency is also being far more widely adopted, further opening up the field of opportunities for fraudsters. Surveys indicate that 36.5 million Americans, or 14.4% of the population, owned cryptocurrency in 2019.[4] The reported reasons for respondents' purchase of cryptocurrency are presented in Exhibit 1.[5]

[1] Haentjens, Matthias, et. Al. (2020). *Disintermediation: Crypto-custodian Insolvency, Legal Risks, and How to Avoid Them*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589381.

[2] US Department of Justice, Office of Public Affairs. Justice News Press Release. *Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework*, October 8, 2020. Retrieved from https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-publication-cryptocurrency-enforcement-framework

[3] Id.

[4] Partz, Helen (2019). *Number of Americans Owning Crypto Doubled in 2019: Finder*. Retrieved from https://cointelegraph.com/news/number-of-americans-owning-crypto-doubled-in-2019-finder.

[5] Id.

Exhibit 1: Survey Respondents' Reasons for Owning Cryptocurrency

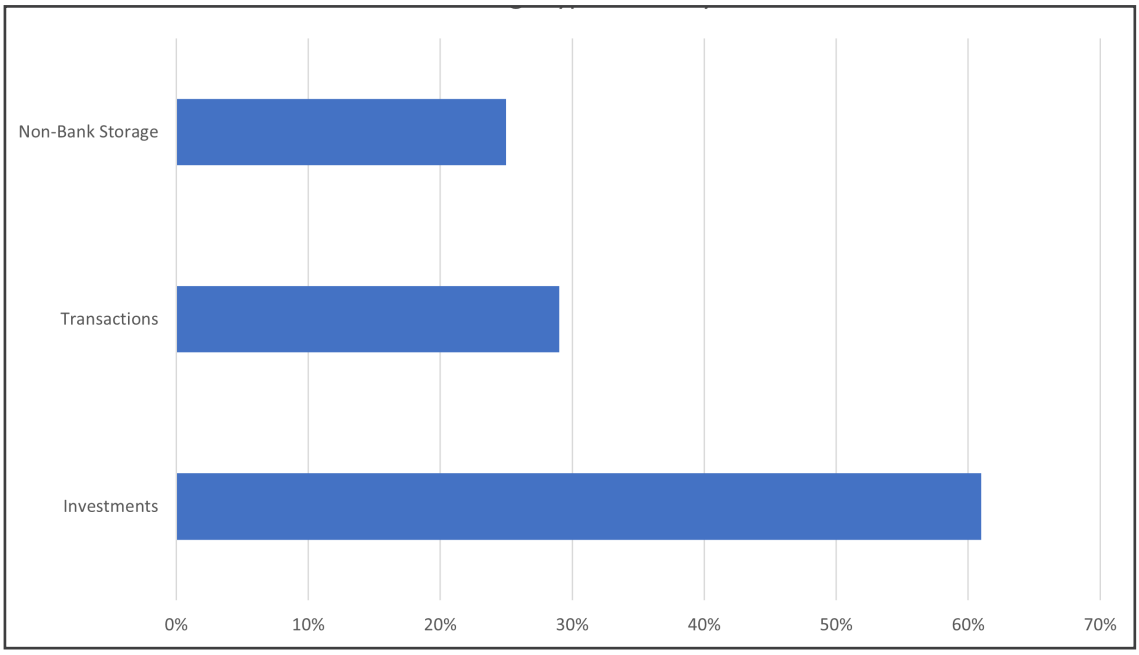
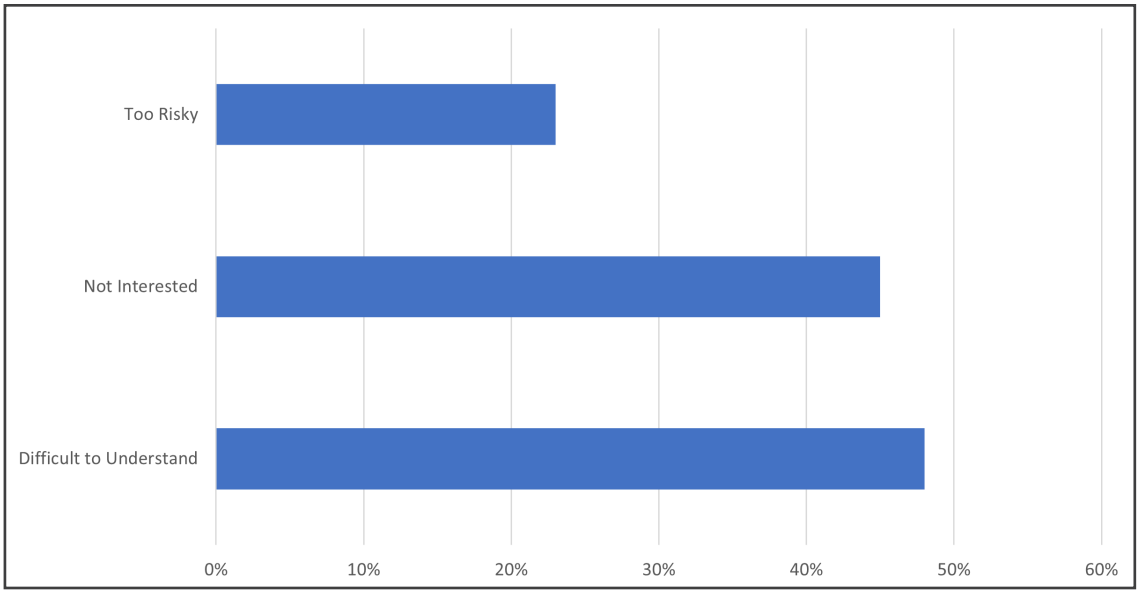


Exhibit 2: Survey Respondents' Reasons for Not Owning Cryptocurrency



Source: Partz, Helen (2019)

In contrast, survey respondents who reported not purchasing cryptocurrency detailed their rationale as shown in Exhibit 2.[6]

Initial Coin Offering Scams

One prime area ripe for exploitation is Initial Coin Offering (ICO) exit scams. Criminals find these very attractive as they can yield very large direct cash payments. Two key targets are cryptocurrency exchanges – where the actual cryptocurrency coins are deposited by investors and then stolen and liquidated for cash, and Ponzi fraud schemes built into many initial coin offerings – where the operators of the ICO entice direct investments in a new crypto-technology and then siphon off investor funds for their own enrichment. Typically, many of these scams are built on wholly non-viable technology disguised to be the next best thing. Some have even been allegedly backed by commodities such as gold bullion or fiat currencies. Through the end of 2019, more than 5,600 ICOs raised over $27 billion as shown in Exhibit 3 on p.8.[7]

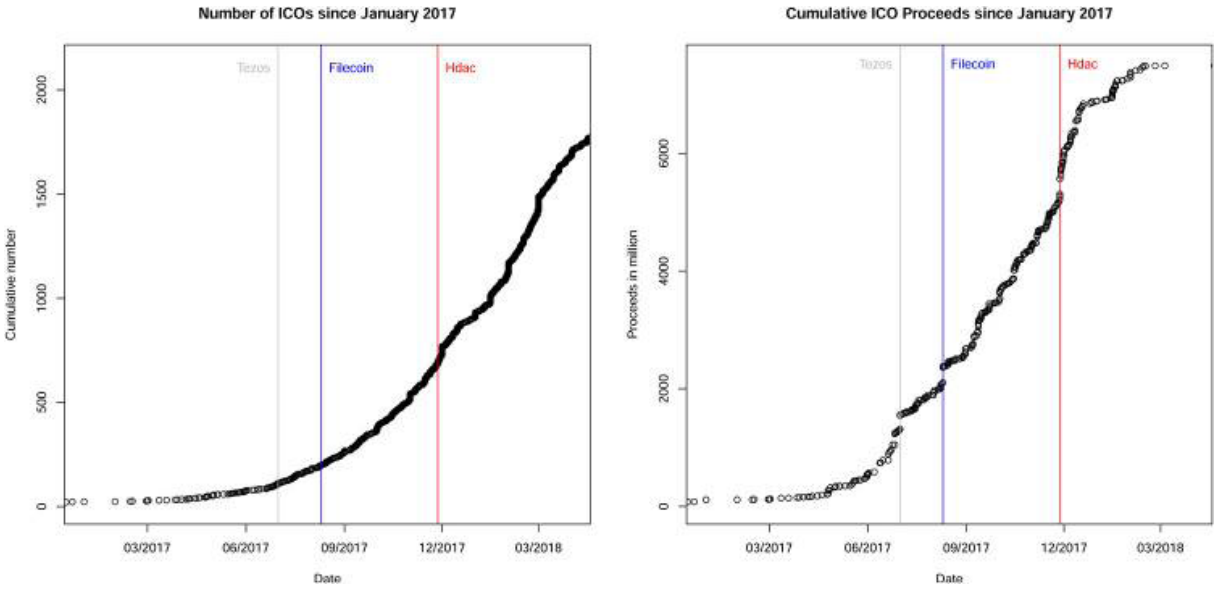
Together, cryptocurrency exchange theft and ICO scams have yielded losses totaling billions of dollars.

[6] Id.

[7] Momtaz PP (2020) Initial Coin Offerings. PLoS ONE 15(5): e0233018. https://doi.org/10.1371/journal.pone.0233018

Continued from p.7

Exhibit 3: Survey Respondents' Reasons for Not Owning Cryptocurrency



Source: Momtaz, PP (2020).

More than 40 ICO scams have been identified,[8] with ten of the most high-profile ICO scams having swindled a staggering $687.4 million from unsuspecting investors.[9] A study prepared by ICO advisory firm Statis Group revealed that more than 80 percent of ICOs conducted in 2017 by number were identified as scams.[10] According to the study, total funding of coins and tokens in 2017 amounted to $11.9 billion, and over $1.5 billion of this funding went to scams.[11] The vast majority went to three large Ponzi scams: Pincoin ($660 million), AriseBank ($600 million) and Savedroid ($50 million), which together equal $1.31 billion.[12] In 2019, scams totaled $8.6 billion in transactions, with three large Ponzi schemes accounting for the majority of the crypto crime.[13] One large Ponzi scheme in China, PlusToken, defrauded more than three million people and totaled more than $2 billion.[14] A correlation between price drops of Bitcoin and the timing of PlusToken cash outs exists, so even those not directly impacted by the PlusToken Ponzi scheme may have been indirectly impacted through devaluation of their Bitcoin holdings.[15]

Cryptocurrency Hacking

Cryptocurrency hacking is equally as lucrative. Last September, hackers reportedly stole $59 million worth of cryptocurrencies from Japanese exchange Zaif, while in Korea there have been at least seven hacks reported in 2019 totaling over $250 million in losses and leading to the bankruptcy of the largest exchange in that country.[16] Another $200 million was stolen from cryptocurrency exchanges through phishing email schemes in 2020 by the CryptoCore Group.[17] Globally, $4.5 billion worth of cryptocurrencies were reported stolen from crypto exchanges in 2019, a Exhibit that is nearly three times the 2018 annual total.[18] Of the $4.5 billion stolen, $4.1 billion related to fraud or misappropriation of funds, and $371 million was lost from exchange thefts and hacks.[19] The cyberfirm Carbon Black reports that roughly $1.1 billion worth of digital currency was stolen across all sources in the first half of this year, with exchanges accounting for 27 percent of these hacks. Even countries that have banned cryptocurrency exchanges and ICOs

[8] Schwienbacher, A. and Hornuf, L. (2018) *Initial coin offerings and fraud cases*. Conference Presentation. Max Planck Institute for Competition and Innovation.

[9] Finance Monthly (2018) *The 10 Biggest ICO Scams Swindled $687.4 Million*. Retrieved from https://www.finance-monthly.com/2018/10/the-10-biggest-ico-scams-swindled-687-4-million/

[10] Cryptocurrency News (2018). *Statis Group Finds That Nearly 80% of ICOs in 2017 Were Scams*. Retrieved from https://cryptocurrencynews.com/statis-group-ico-scams/#:~:text=2018%20Chelsea%20Roh-,Statis%20Group%20Finds%20That%20Nearly%2080%25%20of%20ICOs%20in%202017,held%20in%202017%20were%20scams.

[11] Id.

[12] Id.

[13] Chainalysis (2020). *The 2020 State of Crypto Crime*. Retrieved from https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf

[14] Orcutt, Mike (2020), MIT Technology Review. *Millions of people fell for crypto-Ponzi schemes in 2019*. Retrieved from https://www.technologyreview.com/2020/01/30/275964/cryptocurrency-ponzi-scams-chainalysis/#:~:text=Cryptocurrency%20scammers%20raked%20in%20%244.3,more%20than%20triple%202018's%20haul.&text=Predation%20by%20Ponzi%3A%20But%20according,the%20elephant%20in%20the%20room.

[15] Chainalysis (2020). *The 2020 State of Crypto Crime.*

[16] Bitcoin.com (2020). *US Charges North Korea-Linked Chinese Nationals for Laundering Over $100 Million in Stolen Cryptocurrency*. Retrieved from https://news.bitcoin.com/north-korea-chinese-cryptocurrency/

[17] Palli, Ishita (2020). *Hacker Group Stole $200 Million from Cryptocurrency Exchanges*. Retrieved from https://www.bankinfosecurity.com/hacker-group-stole-200-million-from-cryptocurrency-exchanges-a-14506

[18] Q42019 Cryptocurrency Anti-Money Laundering Report. Retrieved from https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/#:~:text=Total%20of%20cryptocurrency%2Drelated%20frauds,fraud%20and%20misappropriation%20of%20funds.

[19] Id.

outright have still seen large losses. The Financial Action Task Force (FATF) now requires all member countries to "regulate and supervise cryptocurrency service providers, including exchanges,"[20] and the U.S. Homeland Security department launched a cryptocurrency intelligence program specifically focused on darknet markets.[21]

Mt. Gox Hack Leads to Bankruptcy

The Mt. Gox exchange hack in 2014 was one of the earliest, and still the largest, of the cyberheists. While it is still unclear if this was an inside or outside job, the result was the loss of over 750,000 Bitcoins (BTC) from the company coffers, which brought the exchange into bankruptcy. The proceedings, which were consolidated in Japan, are still ongoing and very few creditor claims have been paid out to date. The case, however, calls out many of the unique legal issues relating to asset recovery in the world of digital currencies. Determination of the applicable law is critical because no standard international rules exist to define the relationship between cryptocurrency customers and custodians.

One of the primary questions in discussion has been whether successful claimants can expect a proprietary remedy in tokens, or merely an unsecured creditor claim for the cash value of the tokens at the time of insolvency. That is, does a token holder have a creditor claim or a property claim in the estate? This question, which is common to any insolvency proceeding involving cryptocurrency tokens, is important as it can have serious financial repercussions for the claimants. The answer, as Mt. Gox demonstrated, turns on the legal classification of the tokens, which differs widely around the globe, as well as on the structure of the relationship between the user and the platform and how the courts choose to characterize that relationship.[22]

Cryptocurrency Under U.S. Law

U.S. securities law does not include cryptocurrency tokens in the definition of "money," but rather treats them as intangibles, a classification that severely restricts their utility as a mainstream payment medium and as an asset that can easily be made the subject of a security interest. Intangibles are also treated as the least negotiable of all UCC forms of property. In Japan, however, the Mt. Gox court held that, under the local Civil Code, tokens are not capable of personal ownership at all.[23] This meant that those with recoverable claims would not be able to recover their tokens back. Instead, they would only be able to recover the pre-filing cash value of those tokens. At the time of the bankruptcy filing in 2014, the Bitcoins had a total value of about $473 million.[24] Since then the value of Bitcoin has increased considerably, putting the present-day value at over seven billion U.S. dollars. The Mt. Gox collapse affected 24,000 creditors, and the company was put into liquidation two months after the filing.[25] This creates a large residual in the estate that could lead to a potential windfall recovery for the owner of Mt. Gox, the very person who was likely instrumental in its failure

[20] Bitcoin.com (2020). *US Charges North Korea.*

[21] Helms, Kevin (2020). *US Develops Cryptocurrency Intelligence Program Targeting P2P Sites, Forums, Darknet Markets.* Retrieved from https://news.bitcoin.com/us-p2p-darknet-markets/

[22] Haentjens, Matthias, et. al. (2020). *The Failed Hopes of Disintermediation: Crypto-custodian Insolvency, Legal Risks, and How to Avoid Them.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589381

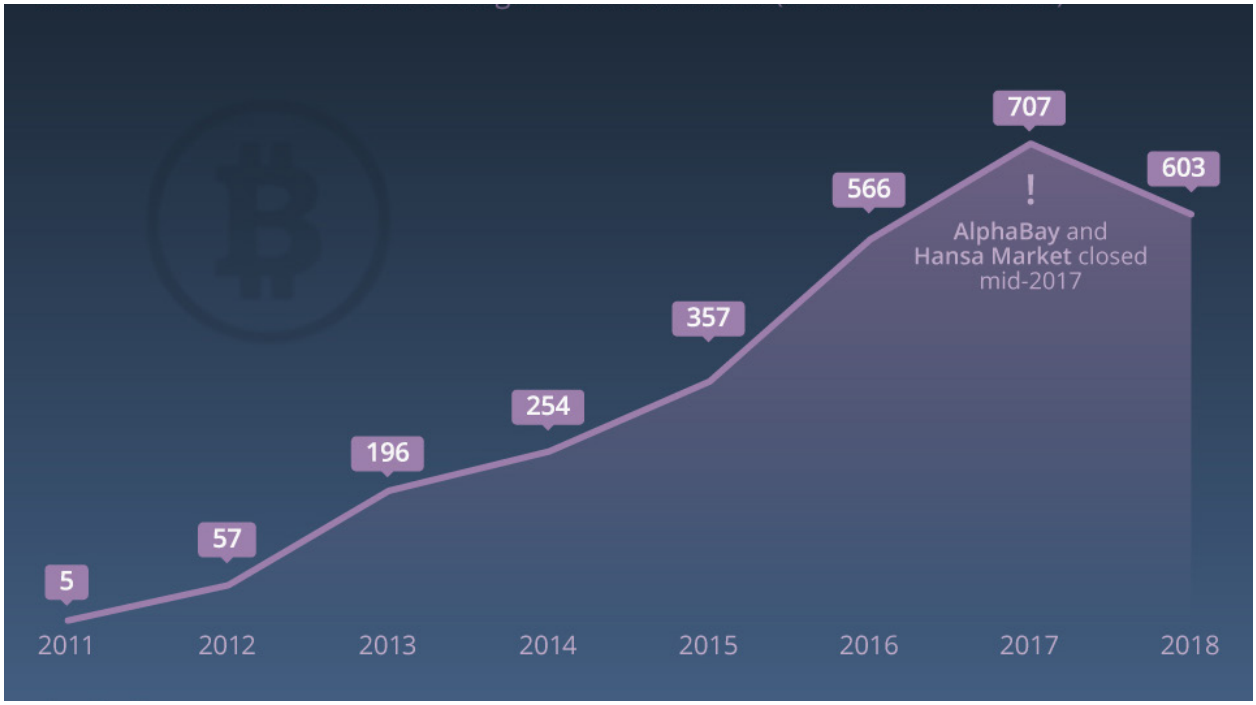
[23] Id.

[24] Castor, Amy (2018). *Mt. Gox Trustee Confirms He Sold Off $230 Million in Cryptocurrency.* Retrieved from https://finance.yahoo.com/news/mt-gox-trustee-confirms-sold-165413471.html

[25] Bybit Insight (2020). *How Mt. Gox's "Happily Never After" Could Reach a Fairy Tale Conclusion.* Retrieved from https://blog.bybit.com/insights/how-mt-goxs-happily-never-after-could-reach-a-fairytale-conclusion/

Continued from p.9

Exhibit 4: Darknet Bitcoin Use is Persistent Despite Busts
Estimated amount of Bitcoin flowing to darknet markets (in million U.S. dollars)



Source: Chainalysis

and who is imprisoned in connection with the event. Fortress created an investment vehicle to purchase Mt. Gox creditor claims at approximately 25% of the market value of Bitcoin, but creditors who preserve valid claims until the trustee makes distributions could end up with a hefty return if they are paid in Bitcoin shares as opposed to the cash value of their investments.[26]

Insolvency Considerations

In addition to novel legal issues around asset classification, there are also a whole host of new technical and logistical issues that arise when an exchange, ICO or wallet holder goes into insolvency. These primarily stem from the digital nature of cryptocurrencies, which raises complex problems that simply are not seen with tangible or secured assets and fiat currencies. One area where this is most evident is bringing assets under the control of the receiver or trustee. This task can always be a challenge. AlixPartners has served as claims agent in the liquidation of assets for the Bernie Madoff Trust since his Ponzi scheme collapsed more than 10 years ago; and bringing all of Madoff's assets under control has been no small task. However, it pales in comparison to gaining control of digital assets that are not only encrypted but may also be scattered around the globe with no associated financial institutions attached to them.

Many investors choose cryptocurrency to bypass governmental oversight and enjoy anonymity; however, this creates significant risk considering insolvency of crypto exchanges. The ownership of cryptocurrency in bankruptcy depends on the applicable laws. The agreement between the investor and the cryptocurrency brokers or agents should be carefully reviewed by the customer as it may govern ownership in bankruptcy. Investors engaging with cryptocurrency brokers who pool crypto assets should realize the higher inherent risk of the pooling. Using segregated blockchain addresses for each investor or investment mitigates some of this risk but does not eliminate the possibility that cryptocurrency assets are commingled among customers and their keys controlled by the broker

Cryptsy Exchange Liquidation

One of the first U.S. cases to bring these issues forward was the Cryptsy exchange liquidation. Cryptsy, a U.S.-based cryptocurrency trading platform, claimed to be hacked in January of 2016 for 13,000 BTC and 300,000 LTC.[27] Since then the founder of the exchange, Paul Vernon, left his residency in Miami, Florida, and is now allegedly hiding out somewhere near Liaoning, China. The exchange was placed into receivership after its customers filed a class action lawsuit for recovery of their losses. After a default judgment of $8.2 million was issued against him for failing to appear, the

[26] Id.

[27] Redman, Jamie (2017). *Vanished Cryptsy CEO "Big Vern" Ordered to Pay $8M in Class Action Lawsuit.* Retrieved from https://news.bitcoin.com/vanished-cryptsy-ceo-big-vern-ordered-to-pay-8m-in-class-action-lawsuit/#:~:text=5-,Vanished%20Cryptsy%20CEO%20'Big%20Vern'%20Ordered%20to%20Pay%-20%248M,company%20Project%20Investors%20(Cryptsy).

defendant confessed through a blog posting that the exchange had been insolvent after $5 million disappeared in June 2014 and that he concealed this fact from customers and regulators.[28] He also admitted to having operated a fraudulent scheme for nearly 18 months while withdrawals were made from profits in its business operating account rather than being funded from safeguarded assets. Unfortunately, this scenario is becoming all too common across hundreds of failed exchanges and fraudulent ICOs.

This case study serves as a good example of the many novel technological challenges faced by the asset recovery and liquidation teams. During its heyday, Cryptsy had a small IT team who ran a full stack of servers needed to manage a vast array of digital wallets. The deposits were comprised of billions of tokens from over 1,000 different cryptocurrencies, each running on its own blockchain software that the receiver had to take control over and manage. The whole environment had to be recreated and assembled in a functional environment. This involved not only engaging a team of IT experts, but also computer forensic experts with blockchain experience to both operate and investigate the hardware and software. Each wallet contained hundreds of thousands of transactions that had to be uncovered, analyzed and assessed for claims settlements. For each account, the entire blockchain history must be analyzed in order to validate its balance. To this end, both the creditors' and the debtors' anonymous public encryption keys first had to be discerned from forensic evidence and records. But these encryption keys only allow for analysis of the blockchain.

Receiver Accessibility

Going one step further, in order to take control of the assets of the debtors, the receiver also had to uncover and take control of the debtors' own private encryption keys as well. Some token holders store these keys on their computers or mobile devices. In such a case, they may be able to be forensically recovered in the absence of cooperation if you have physical access to the devices and they themselves aren't further encrypted or locked. However, many token holders wisely opt to store their digital credentials offline and in secure areas such as in cold USB or even paper wallets. In extreme cases, token holders with significant holdings are reportedly storing their private keys on offline computers locked underground in decommissioned Swiss military bunkers to avoid hacking. In the absence of cooperation, it may be impossible to gain control of keys and their associated assets if they are stored in such unknown or inaccessible places. In the Cryptsy case, some wallets were also corrupt or damaged, and some maliciously destroyed by the debtor.

Recovery of this data, where possible, required an even deeper level of digital forensic expertise. Further, the debtor sought to obfuscate or dissipate assets by destroying computer servers, destroying a database of books and records and their backups, starting a new exchange in China so he could transfer cryptocurrencies to it, and by converting tokens to jewelry and real estate. Unlike traditional funds tracing, tying these tangible assets back to token sales required careful and detailed analysis of digital transactions spread across the many crypto wallets and their associated blockchains. This could only be completed once all the data was safely secured and recompiled.

Liquidating Cryptocurrencies

Other hurdles still abound. Beyond recovery and control, assets may also need to be liquidated before claims can be paid out. Despite what headlines say about the fungibility and demand of popular coins like Bitcoin and Ethereum, not all tokens are created equal. There are a great many alternative cryptocurrencies that have low to medium liquidity and very little demand, making liquidation difficult.

As the Mt. Gox trustee found out—but denied publicly—liquidating large amounts of coin can have significant negative impacts on their market values and require strategic timing. Blockchains, the ledgers that record cryptocurrency transactions, are by design also immutable. Therefore, once you have agreed on a transaction and recorded it, it can never be changed. Doing so corrupts and invalidates the entire ledger. You can subsequently record another transaction about that asset to change its state, but you can never alter or remove the original transaction. This is great for preserving the provenance of assets. For any asset, you can tell where it is, where it's been and what has happened throughout its life.

Unwinding fraudulent conveyances and other reviewable cryptocurrency transactions is technically impossible. Recording a subsequent transaction may be the only viable option, which means that receivers and trustees are being forced to find or produce creative new ways of unwinding needed transactions within the law. This is often akin to fitting a square peg in a round hole with today's jurisprudence, however.

Cryptocurrencies and the Dark Web

In October 2020, the US Attorney General announced the publication of a Cryptocurrency Enforcement Framework. In connection with the release of the framework, FBI Director Christopher Wray stated:

> as this Enforcement Framework describes, we see criminals using cryptocurrency to try to prevent us from 'following the money' across a wide range of investigations, as well as to trade in illicit goods like criminal tools on the dark

[28] Id.

Continued from p.11

> web. For example, the cyber criminals behind ransomware attacks often use cryptocurrency to try to hide their true identities when acquiring malware and infrastructure and receiving ransom payments. The men and women of the FBI are constantly innovating to keep pace with the evolution of criminals' use of cryptocurrency.[29]

One place the criminals often hide and seek to monetize their exploits is on the Dark Web. This is a term that has been getting a lot of attention in corporate boardrooms and media outlets as of late. The general preconception of the Dark Web is that it's a seedy underground digital hiding place for drug dealers, assassins, cybercriminals and pedophiles, which isn't far from the truth. For this reason, security researchers and law enforcement agencies have been surveying the Dark Web for years and keep close eyes on what goes on there. Sales through the Dark Web approached $800 million in 2019, representing 0.08%of all cryptocurrency transactions.[30] Exhibit 4 on p.10 details the estimated value of Bitcoin flowing to Dark Web markets.[31]

The Dark Web contains digital markets that aren't necessarily illegal; however, most Dark Web marketplaces are structured to sell drugs, identities, counterfeit goods, weapons, or other illicit products. The Dark Web's digital marketplaces offer the exchange of goods or services for money, often in the form of cryptocurrency. Cryptocurrency for payment offers anonymity to both buyers and sellers. In many instances, as with public cryptocurrency exchanges Dark Web exchanges have resulted in the theft of millions of customer dollars held in escrow by the marketplace administrator.

Dark Web Intelligence

Quite often the Dark Web is the first place that people learn of a data breach or cryptocurrency theft. This has also made it a place of interest for corporate legal, IT security teams and risk managers in the face of fraudulent or suspicious events. According to the rumor mill in cybersecurity circles, stolen data from the Target and Sony breaches potentially sat on the Dark Web for months before making public headlines. However, while Dark Web intelligence may be helpful in defending your organization from cybercriminals, one must have a full understanding of these underground regions of the Internet and an understanding of how malicious actors use it to commit their crimes in order to avoid running afoul of unnecessary risks.

What is the Dark Web?

The Internet is composed of three primary layers: the World Wide Web (or Surface Web), the Deep Web and the Dark Web. The top layer, which is the area that most users are familiar with, represents only a very small fraction of the Internet. It is the roughly 4 percent of the Internet that is easily accessible via any common search engine.

Underneath the Surface Web is the Deep Web, a much larger pool of information that is largely untouched by search engines. No one knows the exact size of the Deep Web, because it is hard to quantify without search engines. Typically, the Deep Web consists of corporate and academic environments that can only be accessed through direct queries. In other words, you need to know precisely what information you're looking for and you often need to have some kind of authorization to obtain the information. Legal research databases and subscription services are common examples, as are corporate intranets.

The third layer is the Dark Web. It's referred to as "dark" because it can only be accessed with special browsers, routers and encryption tools that render all traffic to its sites anonymous. The sites also use tools to hide their IP addresses, which make tracking their location and ownership especially difficult. These two aspects of anonymity are what make the Dark Web suitable as a digital underground. However, they are also what enables anonymous whistleblowing and protects users from surveillance and censorship in authoritarian regimes.

Risks of Dark Web Access

Given the wealth of intelligence that can be gleaned from the Dark Web, it is understandable that corporate security and risk teams are attracted to it. However, counsel must ensure that these teams proceed with due caution in order to avoid what can be very significant risks. Most importantly, impromptu Dark Web reconnaissance can inadvertently expose an organization to greater security risks because of unknown malicious files that can infiltrate the corporate network. Just like other underground black markets, the Dark Web is full of unscrupulous actors who enjoy taking advantage of the unacquainted. If IT staff isn't properly trained nor has the right resources and equipment, they could easily bring that malware and its controllers back home without even knowing it. In fact, connecting to the Dark Web from any corporate network is always ill-advised. It's important to use air-gapped assets that have no way to transfer malicious data into the corporate environment, as well as to use multiple layers of encryption.

Further, gaining access is not for the faint of heart. Not

[29] US Department of Justice, Office of Public Affairs. Justice News Press Release *Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework*, October 8, 2020. Retrieved from https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-publication-cryptocurrency-enforcement-framework

[30] Chainalysis (2020). *The 2020 State of Crypto Crime.*

[31] Feldman, Sarah (2019). *Darknet Bitcoin use is Persistent Despite Busts.* Retrieved from https://www.statista.com/chart/17128/darknet-use-of-bitcoin/#:~:text=Between%202017%20and%202018%2C%20bitcoin's,14%20percnet%20after%20the%20closures.

all content on the Dark Web is immediately accessible. It can take considerable time, expertise and manual effort to glean useful information. It may take a researcher years to establish trust in certain communities and sales forums. Additionally, several criminal forums on the Dark Web utilize a "vouching" system, similar to a private members club, which might require an investigator to associate with criminals or stray into significantly gray ethical territory to gain access to the content. The average systems administrator probably doesn't have the operational skills necessary to pass himself off as a hacker on the Dark Web. Without the requisite skills, reconnaissance is likely to prove fruitless and will open the company up to further danger.

Even if your team was successful in safely gaining access, their activities must be closely monitored to ensure they do not run afoul of any laws. For example, you certainly wouldn't want your employees accidentally viewing child pornography or bringing it onto the corporate network. Also, while it can be tempting to download files pertaining to purported breaches, taking receipt of stolen goods is a felony in the United States (18 U.S.C. § 2315) that can cause legal issues for your team. Beyond that, such activities may disrupt the legitimate work of law enforcement agencies engaged in their own actions. Also, keep in mind that there is no way to confirm who the seller actually is. Purchasing data in such places can subject the company to risks of violating the Patriot Act if it turns out the data is being sold by a terrorist organization and you transfer funds to them.

As tempting as it may be for in-house IT experts to access the Dark Web for legitimate purposes, a better strategy is to engage a reputable security firm to assist with these services. Many firms now offer some level of Dark Web reconnaissance, ranging from manual intelligence gathering to more automated approaches using Web scraping and analytics tools. Further, by integrating and organizing social media, Deep Web public records and peer-to-peer domains, skilled researchers are able to provide a more unified view of their external threats than internal teams can. The use of artificial intelligence and deep learning enables a more valuable exploration and indexing of large unstructured data sources, while enriching the analysis. The result is real-time finished intelligence, safe from the risks of self-gathering.

Conclusion

Cryptocurrency and Dark Web issues have negatively impacted many investors, and every company should be aware of the risks associated with these activities. While the regulatory environment is improving with respect to cryptocurrency, the opaque nature of the investments causes uncertainty about jurisdiction in the event of an insolvency, governing law for fraud events, transparency with transactions, and the counterparties involved, and the Dark Web can make it more difficult to uncover the actors. Both these technologies will undoubtedly continue to disrupt financial payment systems, and criminals will continue to find more and more lucrative ways to exploit these technologies and those who use them. This means that the number of insolvent exchanges and ICOs is only going to grow. In the face of this, it is imperative that our profession continues to evolve both legally and technically at an equal pace. It also means finding the right technical partners with the computer forensic skills and forensic accounting skills needed to resolve the many unique issues raised by digital currencies. Similarly, understanding the potential bankruptcy implications of your investment decisions prior to selecting an investment vehicle is critical for asset protection. Great care must be taken to ensure that qualified professionals are involved when making these decisions.

ABOUT THE AUTHORS

Regina Lee, CIRA, CPA, CFE

Regina is a Managing Director at AlixPartners in Houston, who has focused on bankruptcy case management and litigation consulting since 1995. She regularly assists clients (debtors, creditors, trustees) in resolving complex bankruptcy-related claims and litigation matters. She also conducts forensic accounting investigations and provides expert testimony on findings. Regina was named to LawDragon's 2020 list of Top Global Restructuring Advisors & Consultants and was honored in 2019 as one of Consulting Magazine's Top 25 Global Consultants, with an additional endorsement for Excellence in Energy. Regina is a CPA (TX and NY), a CIRA, CFE, and a Forensic CPA.

David White

David White is a Director at AlixPartners' New York office. David assists clients in dealing with technically complex regulatory and legal issues and in coordinating internal investigations and fact-finding missions. David has more than 25 years of professional legal, consulting, and technological acumen to help clients manage data breaches, complex legal disputes, and regulatory inquiries. He also has deep knowledge of the technical arts of computer information systems, database technology, computer forensics, artificial intelligence, and machine learning. He has overseen hundreds of digital investigations and provided expert-witness testimony on privacy, data security, and computer forensic matters, and he has led data compliance assessments, security audits, and privacy program development and improvement projects at some of the world's largest companies.