THOMSON REUTERS
Westlaw®

Risks and rewards: Blockchain, cryptocurrency and vulnerability to money laundering, terrorist financing and tax evasion

By Alma Angotti and Anne Marie Minogue, *Navigant Consulting Inc.*

NOVEMBER 26, 2018

While blockchain technology offers transactional advantages, not everyone welcomes the opportunity it offers to transact in cryptocurrency. In fact, Warren Buffett, CEO of Berkshire Hathaway, warns: "Stay away from it. It's a mirage, basically. In terms of cryptocurrencies, generally, I can say almost with certainty that they will come to a bad ending."[1]

Perhaps Buffett has misgivings about cryptocurrency because he knows that nefarious individuals can exploit blockchain's features and exchange cryptocurrencies to launder money, finance terrorist activity, evade taxes and make prohibited purchases. Law enforcement is pursuing prosecution of individuals who transact in cryptocurrency in concert with illegal activity.

Regulators recognize the need to create clear legislation to protect against the criminal use of cryptocurrency exchanged on the blockchain and to ensure it is used only for lawful activities. It is anticipated that regulators, law enforcement and the cryptocurrency industry itself will find ways to use the blockchain technology to prevent and detect illegal activity.

BLOCKCHAIN TECHNOLOGY

Blockchain is a colloquial term used to describe distributed ledger technology.[2] It is a type of DLT — essentially a shared, cryptographical secure ledger of transactions. When people talk about blockchain, they usually mean open public systems that anyone can access and interact with in the chain. In contrast, a closed or private blockchain requires users to have credentials to use the system.

Blockchain is groundbreaking for several reasons. First, it enables transactions between two unrelated parties without the need for a trusted intermediary.[3]

Second, through cryptography, the blockchain can provide confidence in the digital identity of the network participant as well as confidence in the integrity of the ledger itself.[4]

Finally, the distribution of a replicated ledger to all participants provides resilience[5] to the network and significant data management efficiencies.

CRYPTOCURRENCY

Cryptocurrency is "a math-based, decentralized convertible virtual currency that is protected by cryptography."[6] Bitcoin, launched in 2009, was the first cryptocurrency to capture the public's attention. It is estimated that as of May 2018, there were over 17 million bitcoins in circulation.[7]

Regulators recognize the need to create clear legislation to protect against the criminal use of cryptocurrency exchanged on the blockchain and to ensure it is used only for lawful activities.

For the purposes of this discussion, cryptocurrency describes a digital asset transacted on a blockchain, including those referred to as virtual currency, digital currency or cryptocurrency.

CURRENT REGULATORY LANDSCAPE

There is presently little regulation specifically governing the blockchain and cryptocurrency. Regulators, government agencies and law enforcement rely on existing laws and regulations to govern participants, such as administrators and exchanges, in the cryptocurrency ecosystem.

These laws and regulations were not constructed or amended to address the nuances of cryptocurrency exchanged on the blockchain. For that reason, it is difficult to apply them seamlessly. The rules are often applied inconsistently, adding additional regulatory uncertainty.

FinCEN's regulation of virtual currency and cryptocurrencies

The Bank Secrecy Act sets forth anti-money laundering and know-your-customer compliance obligations for money service businesses.[8] The current rules regarding the definitions of MSBs under the BSA were last amended in 1999, long before the existence of cryptocurrency and the blockchain.[9]

Historically, MSBs involved the transmission of cash from one brick and mortar location to another. Following the media

attention concerning bitcoin,[10] in March 2013 the Financial Crimes Enforcement Network issued guidance applicable to "convertible virtual currency." The guidance categorized administrators and exchangers of convertible virtual currency as money transmitters and therefore entities regulated under the BSA.[11]

At the same time, the guidance indicated that "users" of convertible virtual currency are not considered MSBs under the BSA regulations because, in contrast to administrators and exchangers, they are not engaged in the business of transmitting the value of funds to another person or location.

The Securities and Exchange Commission has stated that in some circumstances, cryptocurrency may be a security.

FinCEN explained that a person who creates units of convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter.

By contrast, a person who creates or exchanges units of convertible virtual currency to another person for real currency or its equivalent is a money transmitter.

Thus, FinCEN has reviewed different activities involving virtual currency and has made determinations regarding the appropriate regulatory treatment of administrators and exchangers.

In an address delivered on Aug. 10, FinCEN Director Kenneth Blanco reiterated the fact that cryptocurrency can be exploited for illegal purposes and stressed that exchanges classified as MSBs are subject to the BSA.[12]

Internal Revenue Service

The IRS issued guidance regarding the tax consequences on the use of virtual currencies in IRS Notice 2014-21. The notice provides that virtual currencies that can be converted into traditional currency are property for tax purposes.

It further advises that a taxpayer can have a gain or loss on the sale or exchange of a virtual currency, depending on the cost to purchase the virtual currency (that is, the taxpayer's tax basis).[13]

Securities and Exchange Commission

The Securities and Exchange Commission, however, has stated that in some circumstances, cryptocurrency may be a security.

SEC Chairman Jay Clayton has said, "On cryptocurrencies, I want to emphasize ... while there are cryptocurrencies that do not appear to be securities, simply calling something a 'currency' or a currency-based product does not mean that it is not a security."[14]

If a cryptocurrency is a security, then institutions that trade them may need to be registered as a broker-dealer or an alternative trading system under federal securities laws.

Commodity Futures Trading Commission

In *Commodity Futures Trading Commission v. McDonnell et al.*, the U.S. District Court for the Eastern District of New York ruled that virtual currencies are treated as commodities under the Commodity Exchange Act.[15]

While the CFTC primarily regulates commodity derivatives contracts that are based on underlying commodities, it also maintains general anti-fraud and manipulation authority over virtual currency cash markets as a commodity in interstate commerce.

Office of Foreign Assets Control

In March 2018 the Office of Foreign Assets Control posted on its website that its sanctions regulations would apply equally to both virtual and "fiat" currencies.[16] OFAC also may include digital currency addresses that are associated with blocked people on its Specially Designated Nationals and Blocked Persons list.

Regulation in New York state

The New York State Department of Financial Services has taken perhaps the most targeted approach to regulate virtual currency. DFS regulations require a license for most virtual currency business activity.[17] It specifies on its website that anyone engaging in any of the following activities must obtain a license:

- Virtual currency transmission.
- Storing, holding or maintaining custody or control of virtual currency on behalf of others.
- Buying and selling virtual currency as a customer business.
- Performing exchange services as a customer business.
- Controlling, administering, or issuing a virtual currency.[18]

Further, the DFS requires reporting and monitoring of suspicious activity, including filing of suspicious activity reports for transactions that might show indicia of money laundering, tax evasion or other illegal activity.

EFFECT OF REGULATORY UNCERTAINTY

Money launderers, tax evaders and terrorist financiers can take advantage of the definitional challenges associated with cryptocurrencies. This is because cryptocurrencies combine properties of currencies, commodities and payment systems, and their classification will determine how they are regulated.[19]

Furthermore, cryptocurrency classifications, even within the same jurisdiction, are not always consistent. Some jurisdictions have avoided a formal classification and focused instead on the nature or type of transaction being conducted. This disparity within and among jurisdictions may hamper coordination and lead to gaps in regulation and inconsistencies in enforcement.

ILLEGAL USES OF BLOCKCHAIN AND CRYPTOCURRENCIES

Due to limited regulation and the uncertainty of the regulatory environment, cryptocurrency may be attractive to criminals. Cryptocurrencies transacted on the blockchain are not intrinsically illegal. Nonetheless, they can be used to facilitate illegal activities such as money laundering, terrorist financing, tax evasion and fraud.

Financial crimes typically involve the need to move money in a concealed manner, and cryptocurrency transactions on the blockchain can provide a means to accomplish this goal.

Money laundering

Money laundering is the criminal practice of processing ill-gotten gains, or dirty money, through a series of financial transactions so the funds appear to be proceeds of legal activities.[20]

Cryptocurrency arguably provides more anonymity than cash because it can be used and exchanged through the internet, and the parties to the transaction may remain unknown or difficult to trace.

Terrorist financing and sanctions evasion

Terrorist financing is the criminal practice of using funds to sponsor or facilitate terrorist activity.[21] Terrorist financing is also known as reverse money laundering because it can involve the use of clean money or money from an unknown source to commit crime, thereby turning clean money bad.

Those who fund terrorist activity may use cryptocurrency's cross-border capabilities to send funds to terrorist organizations. The United States and other countries have issued sanctions against those who support terrorist activity.

Fraud and tax evasion

Cybercriminals may also exploit the anonymous and decentralized characteristics of cryptocurrency transacted on the blockchain to demand ransomware payments, create pyramid schemes and receive the proceeds of other types of fraud.

Additionally, tax evaders may use cryptocurrency exchanged on the blockchain as a mechanism to divert receipts or conceal sources of income.

CHARACTERISTICS CRIMINALS VALUE

The blockchain is described as immutable because there is an unchangeable record of the transaction's path. But cryptocurrency powered by blockchain technology can possess characteristics that attract illegal use.

The anonymity and ease of cryptocurrency's cross-border transaction capabilities are important to money launderers who want to disassociate the funds from criminal activity. Similarly, fraudsters and tax evaders want to prevent the government from linking them with their fraudulent activity and unreported income.

Terrorist financiers particularly find the transactions and lack of regulation in some jurisdictions to be useful in their quest to avoid detection by law enforcement.[22]

Because money launderers, terrorist financiers and tax evaders do not want the government to link them with their earnings and uses of funds, the anonymity afforded by cryptocurrency provides an advantage to these criminals.

Blockchain transactions are recorded only as digital addresses that are not necessarily tied to anyone's real identity. Also, because the payer initiates and executes the transaction, there is no exchange of sensitive personal information and the payer can remain anonymous, or, more often, pseudonymous.[23]

Cryptocurrency arguably provides more anonymity than cash because it can be used and exchanged through the internet and the parties to the transaction may remain unknown or difficult to trace.

In addition, the lack of clear regulatory requirements results in many unregulated exchanges whereby no information is collected and as such there are no means to prevent financial crime.

Furthermore, while it is possible to associate internet protocol addresses with the transactions, it may be difficult to associate such addresses with identification because there are additional ways that the parties to the transaction can obscure their identities or confuse the blockchain.

For example, those who wish to conceal or disguise the illicit origin or illegal destination of funds use anonymizers such as layers of encryption, the so-called onion router,[24] BitLaunder,[25] Dark Wallet[26] and fictitious identifiers to further obscure their identities.

Using these tools, the founders of Liberty Reserve[27] laundered hundreds of millions of dollars for criminal organizations for six years. Law enforcement is nevertheless finding ways to pierce the protective veil of anonymity, resulting in arrests and the dismantling of criminal organizations.

On July 20, 2017, the U.S. Attorney's Office for the Eastern District of California announced the seizure of Alpha Bay, the largest illicit marketplace on the internet.

Alpha Bay operated for over two years on the dark web. People used this marketplace to sell illegal drugs, stolen and fraudulent identification documents, counterfeit goods, malware and other computer hacking tools, firearms and toxic chemicals anonymously throughout the world.[28]

Velocity

The speed with which transactions can be executed is particularly important to those who want funds to reach their intended destination prior to detection by law enforcement agents.[29] For this reason, those involved in these criminal activities likely consider cryptocurrency an attractive option.

Cryptocurrency account holders can move funds internationally as quickly as they can move funds using money transfers or traditional wire transfers. In addition, because they conduct these transactions within seconds, sanctioned parties may avoid screening, interception and blocking by traditional financial institutions.

Lack of governance

Money launderers also may find cryptocurrency's lack of governance to be a big benefit. Because cryptocurrency transactions on a blockchain do not involve a central repository of information, there may be no central management. As a result, there may be no entity to conduct due diligence on participants or monitor transactions for indicia of criminal activity.

The lack of governance for cryptocurrency transactions conducted on the blockchain may also be an attractive characteristic to those who fund terrorist activities and seek to evade sanctions. This is because cryptocurrency transactions can avoid the monitoring and surveillance systems of virtually all regulators.

Cross-border capabilities and lack of regulation

The ease with which transactions can be executed across international borders through cryptocurrency on the blockchain may also be another attractive characteristic for money launderers, terrorist financiers and tax evaders. Since narcotics trafficking, human smuggling and other organized illegal enterprises often operate globally, money launderers frequently seek to send the proceeds across international boundaries.

Virtual currency can be transmitted through the internet without using traditional regulated intermediaries such as banks, broker-dealers and MSBs. Also, virtual currency exchanges may or may not be regulated, depending on the jurisdiction.

Furthermore, because payers can conduct cryptocurrency transactions through exchanges in any country, tax evaders and terrorist financiers may choose to deal with cryptocurrency companies in so-called secrecy jurisdictions, in countries supportive of terrorist activity or in countries with weak or nonexistent regulations.

CASE STUDIES

Silk Road and BITC-e

During the past five years, U.S. law enforcement agents have actively pursued and prosecuted money laundering schemes operating through bitcoin exchanges.[30] One of the most notable prosecutions is known as Silk Road.

The Silk Road operation illustrates how the anonymity, decentralization and lack of controls in regard to the use of cryptocurrency can be exploited to facilitate large-scale international money laundering.[31]

Launched in January 2011, Silk Road was an online black-market platform that brokered anonymous criminal transactions and was used to sell illegal drugs and to distribute illicit goods and services.

Silk Road allowed online users to transact anonymously, free of monitoring. It accepted only bitcoins, which further concealed the identities of senders and receivers because their transactions were identified only by an anonymous bitcoin address/account. Users were also able to use different addresses for each transaction, further obscuring their identities.

Silk Road employed a "tumbler" for every purchase, which, as the illicit site explained, "sent all payments through a complex, semi-random series of dummy transactions."[32]

> The encryption properties associated with blockchain make it an ideal application for enhancing an institution's know-your-customer procedures.

In another case, Alexander Vinnik and BITC-e were indicted on 21 charges in the U.S. District Court for the Northern District of California on July 16, 2017, for allegedly committing and facilitating several crimes.

The alleged crimes included identity fraud, drug trafficking and money laundering through the bitcoin exchange BITC-e, which Vinnick operated.[33] BITC-e was also noted for its role in several ransomware attacks.

In this scheme, criminals stole, extorted or otherwise criminally derived bitcoin, which they would transfer to BITC-e. The exchange would then convert the virtual currency into traditional currency using a host of bank accounts registered under the names of shell companies.[34]

The indictment in this case illustrates how the anonymity provided by bitcoin, a lack of anti-money laundering controls and governance, and cross-border exchanges can facilitate criminal activity.

IRS goes after tax evaders

The IRS is aggressively pursuing those who use cryptocurrency as a way to evade paying taxes.[35] The

Coinbase matter illustrates how tax evaders can use the purchase of cryptocurrency transactions to falsify expenses.

The IRS issued a "John Doe" summons after it found instances of tax evasion involving customers of Coinbase, a company that facilitates cryptocurrency transactions.[36]

In a declaration to the court in support of the summons, an IRS revenue agent noted that his investigations included probes into two taxpayers with annual revenues in the millions who "admitted disguising the amount they spent purchasing the bitcoins as deductions for technology expenses on their tax returns."[37] Those corporate taxpayers had wallet accounts at Coinbase.

Terrorist financing and sanctions circumvention

On Dec. 13, 2017, a woman named Zoobia Shahnaz was indicted on charges of money laundering stemming from her alleged defrauding of several financial institutions.

According to the indictment and prosecutors, Shahnaz generated over $85,000 in illicit proceeds, which she converted to bitcoin and other cryptocurrencies. The indictment further indicates that Shahnaz then laundered the funds, moving them out of the country to support the Islamic State of Iraq and al-Sham.[38]

Furthermore, a study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs indicated that a small number of cases suggest some jihadist and right-wing extremists are using cryptocurrencies because of the anonymity they provide.[39]

Moreover, Iran recently announced plans to develop its own national cryptocurrency in order to circumvent U.S. sanctions. This announcement further substantiates the concern that cryptocurrency can be exchanged on the blockchain to support terrorist financing and evade sanctions.[40]

According to a recent news report, Iranian MP Mohammad-Reza Pourebrahimi discussed, at a meeting in Moscow, the possibility of using cryptocurrencies for international payments, stating that Iran and Russia could use digital currencies to avoid U.S. dollar transactions and potentially even replace the use of the SWIFT interbank payment system,[41] which banks use to send money transfer instructions.

POTENTIAL SOLUTIONS

As regulations evolve to better govern cryptocurrency transactions on the blockchain and enforcement actions relating to cryptocurrency-related financial crimes increase, organizations may want to perform additional due diligence to protect themselves from exploitation by illegal enterprises.

Transaction monitoring

Exchanges that plan to facilitate transactions on the blockchain may want to consider leveraging blockchain's qualities to enhance their transaction-monitoring capabilities. The blockchain contains an immutable and traceable record of transactions. With access to the set of transactions across the entire network, detection protocols may be able to better identify behavioral anomalies.[42] Furthermore, advanced transaction monitoring may become a regulatory expectation, particularly for administrators and exchanges classified as MSBs.

Know-your-customer procedures

The encryption properties associated with blockchain make it an ideal application for enhancing an institution's know-your-customer procedures.[43] With proper identification of the customer, and their subsequent association with a single cryptographic key, institutions can be confident in that customer's digital identity.

A blockchain ledger may also be used to establish a universal KYC repository. Institutions that participate in the blockchain would be able to share KYC data. In addition, as information on a customer is amended, the entire network would have the up-to-date information.

Additional regulation and governance

Regardless of the approach various governments take in further regulating the industry, legislation on cryptocurrency is likely to be specific and targeted. First, regulators may want to consider defining cryptocurrency with consistency and appropriately regulating its use, taking into account any potential legal differences between types of offerings and exchanges.

Second, a statute on cryptocurrency will likely provide for centralized monitoring and reporting mechanisms.

Third, regulations should define and distinguish domestic versus international transactions to ensure the collection of taxes, duties and reporting when appropriate.

Industry self-regulation

Self-regulation may play a big part in improving governance in the cryptocurrency industry. In fact, exchanges themselves likely have more insight and are in a better position to govern and monitor their activities across jurisdictional borders.

The Wall Street Journal[44] reports that Cameron and Tyler Winklevoss founded the Virtual Commodity Association with a mission to establish industry guidelines to improve transparency and stability. Exchanges such as Bittrex Inc., bitFlyer USA Inc. (a unit of Japan's bitFlyer Inc.), Bitstamp Inc. and Gemini have already joined the association.

CONCLUSION

Money launderers, terrorist financiers, fraudsters and tax evaders may use the blockchain to exchange cryptocurrency in a manner that conceals the identities of the counterparties because this technology facilitates cross-border transactions

without scrutiny and allows large-dollar transactions to be executed swiftly and frequently.

With the proper legislation, industry self-governance and government oversight, however, the very features that make blockchain vulnerable can be used to develop more sophisticated prevention and detection ability.

Specifically, the transactional transparency offered by blockchain can be used to conduct sophisticated monitoring by blockchain operators and regulators to identify suspicious activity in real time or soon after the transaction. Investigators who follow the money may be afforded international visibility to view the complete paper trail with little restriction or bureaucracy.

Additional regulation is necessary, however, to bring this enhanced monitoring capability to fruition. In particular, government regulators need to affix responsibility with blockchain administrators and/or cryptocurrency operators to identify individuals operating on the blockchain and require that these identities be associated with transactional activity. When this is accomplished, blockchain transactions may afford a more robust control environment than that offered by traditional financial institutions.

NOTES

[1] Berkeley Lovelace Jr., *Buffett on Cryptocurrencies,* CNBC, Jan. 10, 2018, https://cnb.cx/2EsDFUm.

[2] A distributed ledger is an asset database that can be shared across a network of multiple sites, geographies, or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically using "keys" and signatures to control who can do what within the shared ledger.

[3] Karl Wuest, Security of Blockchain Technologies, 2016, https://bit.ly/2S2BVYW.

[4] Christian Cachin et al., Blockchain, Cryptography, and Consensus, 2016, https://bit.ly/2DwGWVC.

[5] David Mills et al., *Distributed Ledger Technology in Payments, Clearing, and Settlement,* J. OF FIN. MKT. INFRASTRUCTURES, Feb. 16, 2018, 207.

[6] Financial Action Task Force, FATF Report: Virtual Currencies: Key definitions and Potential AML/CFT Risks, June 2014, https://bit.ly/1iQmaS2.

[7] The Statistics Portal, Number of Bitcoins in circulation worldwide from 1st quarter 2011 to 2nd quarter 2018 (in millions), https://bit.ly/2DN2I3R.

[8] Department of the Treasury, Guidance FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, 2013, https://bit.ly/2D33N7W.

[9] Department of the Treasury, "Am I an MSB?," https://bit.ly/2RZ7zqb.

[10] Stephen T. Middlebrook & Sarah J. Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions,* WILLIAM MITCHELL L. REV., 2014, 813-48, https://bit.ly/2DZsAcZ.

[11] Sidley Austin LLP, *FinCEN Issues Guidance on Application of Bank Secrecy Act Regulations to Virtual Currencies* (Mar. 26, 2013), https://bit.ly/2Dxq2WY.

[12] Kenneth A. Blanco, FinCEN Director, Prepared Remarks Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), https://bit.ly/2vWI6nJ.

[13] Internal Revenue Bulletin 2014-16, April 14, 2014, https://bit.ly/2Qa1iug.

[14] Jay Clayton, SEC Chairman, Public Statement on Cryptocurrencies and Initial Coin Offerings, https://bit.ly/2C7emqG.

[15] *CFTC v. McDonnell,* No. 18-cv-361 (E.D.N.Y. Mar. 6, 2018), https://bit.ly/2A6BNjP.

[16] U.S. Department of the Treasury OFAC Frequently Asked Questions: Sanctions Compliance, https://bit.ly/2Ts8PU5.

[17] Regulations of the Superintendent of Financial Services, New York. Codes, Rules and Regulations, Title 23, Part 200 (proposed), https://on.ny.gov/2TsitpK.

[18] New York State Department of Financial Services, BitLicense Frequently Asked Questions, https://on.ny.gov/2Bh2fZN.

[19] Dong He et al., *Virtual Currencies and Beyond: Initial Considerations,* 16/03 IMF Staff Discussion Note 24, 2016, https://bit.ly/1PlWVez.

[20] Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2015, https://bit.ly/2A46zcV.

[21] International Monetary Fund, Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT), https://bit.ly/1M7MEsz.

[22] Internal Revenue Manual Pt. 25 ch. 1 sec. 1, Jan. 23, 2014, https://bit.ly/2KfCPhP.

[23] "Pseudonymous" means bearing or using a fictitious name.

[24] The onion routing network is used to protect internet initiators and responders against both eavesdropping and traffic analysis from other users of the internet. In the onion routing of the invention, instead of making connections directly to a responding machine, users make connections through onion routers. The onion routing network allows the connection between the initiator and responder to remain anonymous. Anonymous connections hide who is connected to whom and for what purpose from outside eavesdroppers, see Google Patents at https://www.google.com/patents/US6266704.

[25] BitLaunder advertises that it tumbles a client's bitcoins with thousands of other users to render the client's transactions untraceable in the blockchain. Tainted bitcoins go in and clean bitcoins come out, see forum at https://bit.ly/2OSi5xr.

[26] An open source bitcoin platform designed for the sole purpose of protecting users' privacy. Dark Wallet is a digital wallet that enables data anonymization by obfuscating bitcoin transactions carried out in the online market space. Dark Wallet was created by Cody Wilson and Amir Taaki. Investopedia, https://bit.ly/2DJMeOg.

[27] To date, it is the largest online money-laundering case in history. In May 2013 the U.S. Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than $6 billion in illicit proceeds.

[28] U.S. Dep't of Justice, https://bit.ly/1U2Up4y.

[29] Office of the Comptroller of the Currency, Money Laundering: A Banker's Guide to Avoiding Problems, 2002, https://bit.ly/2A4xg0Z.

[30] Press Release, U.S. Dep't of Justice, Former Federal Agents Charged with Bitcoin Money Laundering and Wire Fraud (Mar. 30, 2015), https://bit.ly/2QWLbxE; Financial Action Task Force, FATF Guidance for a Risk-Based Approach: Virtual Currencies, June 2015, https://bit.ly/1elZfMz.

[31] *Beyond the Silk Road, Hearing Before the S. Comm. On Homeland Sec. & Governmental Affairs* (Nov. 18, 2013) (statement of Mythili Raman, acting Ass't Atty. Gen., U.S. Justice Dep't, Crim. Div.), https://bit.ly/2QVrDtc.

[32] *Law Enforcement and Virtual Currencies, Hearing Before N.Y. State Dep't of Fin. Servs.* (Jan. 29, 2014) (statement of Richard B. Zabel, Deputy U.S. Att'y), https://bit.ly/2DNeEXY.

[33] Press Release, U.S. Dep't of Justice, Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox (July 26, 2017), https://bit.ly/2v9ns5R.

[34] Nathaniel Popper, *Bitcoin Exchange Was a Nexus of Crime, Indictment Says,* N.Y. Times, July 27, 2017, https://nyti.ms/2v9SrPa.

[35] Nathaniel Popper, *Bitcoin Users Who Evade Taxes Are Sought by the I.R.S.,* N.Y. Times, Nov. 18, 2016, https://nyti.ms/2OSlVqa.

[36] United States' Memorandum in Support of Ex Parte Petition for Leave to Serve John Doe Summons, Nov. 17, 2016, https://bit.ly/2KgvK0D.

[37] Kelly Phillips Erb, *IRS Wants Court Authority to Identify Bitcoin Users & Transactions at Coinbase,* Forbes, Nov. 21, 2016, https://bit.ly/2Q9E086.

[38] Grand Jury Indictment in *United States v. Zoobia Shahnaz,* December 13, 2017, https://bit.ly/2BinZEG.

[39] Study for the TERR committee, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, May 2018, https://bit.ly/2JCNYs5.

[40] Yaya Fanusie, *Blockchain Authoritarianism: The Regime In Iran Goes Crypto,* Forbes, Aug. 15, 2018, https://bit.ly/2DwxLV9.

[41] Ashour Iesho, *Russia and Iran may Use Cryptocurrency to Bypass International Sanctions,* Bitcoinist, May 21, 2018, https://bit.ly/2BhMuBW.

[42] Elliptic, The Bitcoin Big Bang, https://bit.ly/2zgDU4U.

[43] David Shrier, Weige Wu & Alex Pentland, *Blockchain & Infrastructure (Identity, Data Security),* Mass. Inst. of Tech. (2016.)

[44] Paul Vigna, *Winklevoss Effort to Self-Regulate Cryptocurrency Gets Members,* Wall St. J., Aug. 20, 2018, available at https://on.wsj.com/2OSR0tV.

This article appeared November 26, 2018, in Westlaw Journal Bank & Lender Liability.

ABOUT THE AUTHORS

Alma Angotti (L) is a managing director and co-head of the global investigations and compliance practice at **Navigant Consulting Inc.** in Washington. She is a widely recognized expert on financial crime, anti-money laundering, terrorist financing and economic sanctions issues. She has worked with financial institutions, governments and regulators globally to strengthen regulatory compliance and to help prevent abuse by terrorists and criminals. She can be reached at alma.angotti@navigant.com. A senior director in Navigant Consulting's global investigations and compliance practice in New York, **Anne Marie Minogue** (R) is a veteran in financial investigations and compliance. Expert in indications of fraud, corruption and money laundering, she conducts investigations, assesses fraud, anti-bribery and corruption and anti-money laundering risk management capabilities, and reviews regulatory compliance activities. She can be reached at anne.minogue@navigant.com. The authors gratefully acknowledge the assistance of Gene Bolton, Brandy Schindler, Elizabeth Sisul and Mariya Stetsyna in preparing this article.