POLICY ALERT // APRIL 23, 2018

Virtual Currencies: Momentum Building For Regulation and Enforcement

Summary

Regulators around the world are paying more attention to the risks associated with virtual currencies amid increasing trading volumes and a flood of new coins being offered for sale. Virtual currencies[1] (VCs), which are nominally digital representations of value that function as a medium of exchange despite lacking legal tender status in any jurisdiction, have captured popular attention recently as prices have soared and crashed. Regulatory treatment on a global scale is neither set nor harmonized. Governments are exploring ways to cultivate innovation in financial and regulatory technologies and are considering the official use of digital currencies. Still, facilitating virtual currency transactions presents high risks for virtual currency exchanges and banks that provide financial services to those exchanges.

- The White House on March 19 issued an executive order banning U.S. persons from trading in digital currencies issued by the Venezuelan government. That same day, OFAC issued guidance laying out compliance expectations for transactions involving digital currencies.
- U.S. authorities, which regulate virtual currency exchangers as money services businesses (MSBs), also have signaled increased enforcement focus related to drug trafficking and online opioid sales, so new actions may target those facilitating associated VC payments.
- Globally, regulatory efforts have varied, with some jurisdictions seeking transparency and others attempting to implement bans on VC trading.
- VC exchanges and other VC-related businesses are high risk because of the inherent challenges such companies face in applying appropriate controls against money laundering, terrorist financing, sanctions evasion, and other crimes. Banks, in turn, are not well equipped to assess the controls in place at VC-related businesses.
- Risks are especially high for businesses connected to anonymity-friendly VCs such as Monero. Despite the availability of more opaque alternatives, recent studies indicate that bitcoin, the most established virtual currency, is continuing to play a substantial role in illicit transactions.

Risk assessment and mitigation measures are necessary both for VC exchanges and for financial institutions with exposure to virtual currencies. Banks may be

exposed to VCs beyond direct relationships with VC exchanges.

- As is the case for all MSBs, VC exchanges must implement anti-money laundering controls. Exchanges should take advantage of VC ledgers to understand the transactional histories of customers and counterparties. They should also be monitoring for certain types of transactions that present high risk in the virtual currency space.
- Financial institutions banking VC exchanges need to follow core customer due diligence measures. However, enhanced due diligence measures for intermediated relationships should also be applied to VC exchanges given the risks involved.
- Assessing a VC exchange's risks and risk management poses special challenges for banks.

Initial coin offerings (ICOs) have been plagued by fraud and theft, making them particularly risky. Criminal activity related to ICOs has triggered new enforcement efforts, and some countries have banned ICOs altogether.

- Some ICOs promise unrealistic returns or claim falsely to be backed by investments in real estate, diamonds, or other goods.
- Ernst & Young estimates that more than ten percent of $3.7 billion raised in initial coin offerings has been lost or stolen.[2]
- Banks with ICO exposure should apply due diligence measures to all parties involved in the ICO, including exchanges, coin developers, and those who stand to benefit most from the offering.

Financial Institutions in the VC Ecosystem

VC exchanges link virtual currencies to the rest of the international financial system. VC exchanges are MSBs. Such exchanges present varying risk profiles, but their baseline illicit finance risk is high because VCs have traits that are very attractive to criminals.

- VC exchanges' risk profiles are shaped primarily by their regulatory environments, the profiles of their customers, and the types of cash-out services offered, with the sophistication of their counter-illicit finance function mitigating their inherent risks. As a starting point, risk mitigation measures should be based on the risks associated with MSBs.
- VC exchanges' risks grow with the real and perceived risks tied to VCs

themselves. A January 2018 study by academics in Australia and Latvia estimates that approximately "one quarter of bitcoin users and one half of bitcoin transactions are associated with illegal activity" and that "around $72 billion of illegal activity per year involves bitcoin, close to the scale of the U.S. and European markets for illegal drugs."[3]

VC users can take additional steps to mask their identities and transactions. Businesses that help individuals hide their tracks pose clear and prohibitive risks to financial institutions.

- Because some VCs such as bitcoin are associated with public blockchains—ledgers or databases which capture the entire transactional history of a VC—users involved in illicit activity often take advantage of "mixers," gambling sites, and other conversion services to obscure payments.
- Exchanges dealing in Monero, Dash, and other anonymity-friendly VCs also present high risk because users transacting in such VCs may not require mixers and similar services to conceal activity.

On March 19, the White House issued an executive order banning U.S. persons from conducting any transactions related to virtual currencies issued by the Venezuelan government after January 9, 2018.[4] OFAC also amended its guidance with five frequently asked questions on virtual currency.[5]

- The guidance defined virtual currency, digital currency, digital currency wallet, and digital currency address and said that OFAC will use its authorities against criminals and other malicious actors who abuse virtual currencies.[6]
- It also clarified that U.S. persons' obligations are the same whether transactions are denominated in virtual currency or fiat currency.[7]
- OFAC said that it may start adding digital currency addresses to the SDN list to alert the public to digital currency addresses associated with sanctioned persons.[8]

U.S. authorities have already penalized VC-related businesses and may be poised to ramp up enforcement efforts against them.

- In 2015, Ripple Labs, Inc. paid a $700,000 penalty to the Financial Crimes Enforcement Network (FinCEN) at the U.S. Treasury Department for violating Bank Secrecy Act (BSA) requirements. The company sold VCs without registering with FinCEN, and it did not have an appropriate anti-money laundering program.

- FinCEN also fined the BTC-e exchange for facilitating ransomware and drug sales. That July 2017 action was FinCEN's first against a foreign-located MSB. Such MSBs are subject to the Bank Secrecy Act (BSA) when they provide financial services to people located in the United States.[9]

- In its proposed budget, the White House has requested a $3 million increase for FinCEN, in part to target organizations that are fueling the opioid crisis in the United States. A report recently published by the U.S. Senate Permanent Subcommittee on Investigations found that online sellers of synthetic opioids operate openly, and that such online sellers prefer bitcoin.[10]

- New York Attorney General Eric Schneiderman launched a Virtual Markets Integrity Initiative this month to better understand the policies and practices, including money laundering controls, of platforms that consumers use to trade VCs. His office also sent letters to 13 VC exchanges requesting disclosures on their operations, use of bots, conflicts of interest, outages, and other issues.[11]

Globally, authorities and regulators have taken steps to curb illicit activity linked to virtual currency exchanges.

- China, the most stringent VC regulator among major economies thus far, banned VC exchanges in 2017, and then instituted a nationwide ban on online platforms and mobile apps that offer exchange-like services.[12]

- The European Union has agreed to change its Fourth Anti-Money Laundering Directive to "end anonymous transactions on virtual currency platforms and with pre-paid payment cards, which investigators said could have been used to fund attacks by militants." Once the rules are implemented, "Bitcoin exchange platforms and 'wallet' providers that hold the [currency] for clients will be required to identify their users."[13]

- The Australian Transaction Reports and Analysis Centre has announced that, as of April 3, VC exchanges are required to meet obligations including adopting and maintaining a program to manage money laundering and terrorism financing risks; identifying and verifying customer identities; reporting suspicious activity and transactions involving physical currency of $10,000 or more; and keeping certain records for seven years.[14]

- In Japan, VC exchanges are now allowed, but only under certain conditions: mandatory registration with the government, minimum capital of 10 million yen, a secure IT system to prevent theft, and mandatory annual auditing.[15] In

March, following a $530 million theft from an exchange called Coincheck, a group of Japanese VC exchanges announced plans to "set up a self-regulatory body to bolster trust" in the industry.[16]

- The South Korean government's position is in flux, but "authorities are taking measures to prevent money laundering and other illegal activities. … The country outlawed deposits into anonymous virtual accounts at banks and told lenders to report suspicious traders, including those who deposit or withdraw 10 million won or more a day from cryptocurrency venues."[17]

- Other authorities have signaled future action. The Governor of the Bank of England stated on March 1 that "the time has come to hold the crypto-asset ecosystem to the same standards as the rest of the financial system," pointing to money laundering and terrorist financing risks.[18]

As a result of real and regulatory risks, some major banks do not allow their correspondent banks to deal with VC exchanges.[19] Bank of America's February 2018 filing with the U.S. Securities and Exchange Commission (SEC) states that VCs and other emerging technologies "could limit our ability to track the movement of funds," limiting the bank's ability to comply with sanctions and anti-money laundering laws.[20] Like several other banks, Bank of America has prohibited customer VC purchases through credit cards, and it has restricted clients of its Merrill Lynch brokerage unit from making bitcoin-related investments.[21] Some mortgage lenders, concerned about sources of funds, are turning away potential clients who are attempting to turn their VC windfalls into real estate investments.[22]

Risk Mitigation for Money Services Businesses, Including VC Exchanges

For VC exchanges, as with any other MSB or financial institution, risk assessment is the necessary first step before risk mitigation. Every exchange has different product/service risks, customer risks, geographic risks, and operational risks. An understanding of these risks should inform controls related to sanctions, money laundering, terrorist financing, bribery, corruption, and proliferation financing.

In the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual for Money Services Businesses, FinCEN provides guidance regarding risk assessment and risk mitigation.[23] The manual is centered on four pillars of a risk-based AML program:

- Policies, procedures, and internal controls designed to ensure ongoing compliance;

- Designation of individual(s) responsible for coordinating and monitoring day-to-day compliance;
- Training for appropriate personnel; and
- Independent review to monitor an adequate program.

Regarding the first pillar above, VC exchanges require controls focused on:

- Users exchanging VC for fiat currency, in either direction;
- Users transferring VC to other addresses on the same ledger (since many exchanges also function as wallet providers, allowing users to send VC to and receive VC from addresses external to the exchange); and
- To the extent that detection is possible, users transferring VC for the purpose of exchanging that VC for a higher-risk VC more amenable to anonymous, illicit activity (and the reverse pathway).

Compliance personnel should be alerted to any user transactions involving addresses known to be associated with, for instance, mixers, gambling sites, illicit markets, or sanctioned jurisdictions (geographic information may be especially difficult to obtain for private entities, but exchanges should be aware of the growing risk of sanctions enforcement). In addition, compliance personnel should be able to check the transactions of the user's counterparties. An exchange's compliance policy should explain how many "hops" are checked for connections to illicit activity. In addition to screening for known red-flag addresses, exchanges should be checking user transaction patterns against anti-money laundering and countering the financing of terrorism (AML/CFT) typologies. Commercial tools that simplify analysis of public blockchains are useful in establishing these controls.

Risk Mitigation for Banks

It is understood that financial institutions banking VC exchanges will need to follow core customer due diligence (CDD) measures:

- Identifying the customer and verifying the customer's identity;
- Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
- Conducting ongoing due diligence on the business relationship and scrutiny

of transactions undertaken throughout the course of that relationship.

However, enhanced due diligence measures for correspondent banking relationships should also be applied to VC exchanges because VC exchanges present intermediated risks similar to those associated with correspondent banking. These measures include:

- Obtaining senior management approval for opening an account;
- Gathering information from the applicant consistent with global CDD standards;
- Assessing the applicant's financial crimes compliance (FCC) risks, including through an independent audit of the compliance function;
- Assessing the applicant's FCC risk management programs;
- Maintaining records on each applicant for the purpose of answering inquiries; and
- Clearly understanding the respective responsibilities of each institution.

Assessing an exchange's risks and risk management poses special challenges for banks because banks are not accustomed to dealing with customers who trade in VCs. To assess an applicant's FCC risks, bank personnel will need to understand the unique nature of the services that the VC exchange provides and the nature of the illicit finance vulnerabilities and threats that arise from the nature of the services provided. Independent audit of the exchange's AML/CFT and sanctions compliance functions will be necessary. Furthermore, banking such exchanges may require a hands-on approach by the financial institution (e.g., seconding personnel in the exchange to better understand risks and mitigation measures).

Banks should also have risk management policies in place regarding customers who transact in significant amounts or frequencies with known VC-related businesses, including exchanges. In addition, banks may be exposed to virtual currency risks through customers who participate in peer-to-peer services such as Paxful which match buyers and sellers to facilitate exchange. Through Paxful, an individual who wants to purchase bitcoin can be matched to a potential seller. The bitcoin buyer then deposits cash in person and into an account held by the seller. After the bitcoin seller confirms that the cash has been deposited, he or she then transfers bitcoin to the bitcoin buyer's virtual address. Those who are selling bitcoin through Paxful are effectively operating as unlicensed MSBs. Yet an informal poll of compliance officers suggests that a large majority of financial institutions are not monitoring transactions for cryptocurrency activity, so the unlicensed MSB activity is likely to go undetected.[24]

Initial Coin Offerings

An ICO is a fundraising mechanism in which a new virtual currency is created on a protocol such as Counterparty, Ethereum, or Openledger, with the coin's initial value arbitrarily determined by the startup team before the value is allowed to fluctuate.[25] Relative to traditional fundraising, "investors can see gains more quickly, and can pull profits out more easily, via ICOs."[26]

The Swiss Financial Market Supervisory Authority categorizes ICOs as follows:[27]

- *Payment tokens* (cryptocurrencies) are tokens intended to be used as a means of payment for acquiring goods or services or as a means of money or value transfer. They give rise to no claims on their issuer.
- *Utility tokens* are tokens intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.
- *Asset tokens* represent assets such as a debt or equity claim on the issuer. They promise, for example, a share in future company earnings or future capital flows. These are analogous to equities, bonds, or derivatives. (Tokens which enable physical assets to be traded on the blockchain also fall into this category.)

ICO successes in 2016 and 2017 have spurred fraud concerns, with some ICOs promising unrealistic returns or purporting to be backed by investments in real estate or diamonds.[28] Theft has also been an issue: Ernst & Young estimates that more than ten percent of $3.7 billion raised in initial coin offerings has been lost or stolen by hackers who obtain personal information to access VC.[29] Hacked exchanges averaged $2 billion in hacking losses as of November 2017, and blockchain technology prevents transactions from being reversed.[30]

The SEC created a new Cyber Unit in September 2017, to focus the Enforcement Division's cyber-related expertise on misconduct involving distributed ledger technology, initial coin offerings, and other related issues. Its first charges came in December 2017, when it halted a coin offered by a recidivist securities law violator from Canada.[31] The SEC and the Commodity Futures Trading Commission have taken other actions against ICO fraud as well.[32] Overseas, China and South Korea have banned ICOs.[33]

Banks with ICO exposure (e.g., through a VC exchange client) should apply the CDD measures noted above to all parties involved in an ICO, including exchanges, coin developers, and those who stand to benefit most from the ICO, because these parties will be among the ultimate beneficiaries of transactions conducted through a bank, if

not direct counterparties of a client who is a VC exchange.

In addition, banks and exchanges should conduct assessments of coins themselves. The SEC's December 2017 statement on VCs and ICOs included questions that investors should ask to assess an ICO's vulnerability to fraud and market manipulation, and these questions also are useful for banks and exchanges considering whether they should service an ICO:[34]

- Who exactly are investors contracting with? Specifically, who is issuing and sponsoring the product, what are their backgrounds, and have they provided a full and complete description of the product? Do they have a clear written business plan?
- Who is promoting or marketing the product, what are their backgrounds, and are they licensed to sell the product? Have they been paid to promote the product?
- Where is the enterprise located?
- Where is investor money going and what will it be used for? Is investor money going to be used to "cash out" others?
- What specific rights come with investment?
- Are there financial statements? If so, are they audited, and by whom?
- Is there trading data? If so, is there some way to verify it?
- How, when, and at what cost can investors sell? For example, do they have a right to give the token or coin back to the company or to receive a refund? Can they resell the coin or token, and if so, are there any limitations on the ability to resell?
- If a digital wallet is involved, what happens if an investor loses the key?
- If a blockchain is used, is the blockchain open and public? Has the code been published, and has there been an independent cybersecurity audit?
- Has the offering been structured to comply with the securities laws and, if not, what implications will that have for the stability of the enterprise and the value of users' investments?
- What legal protections may or may not be available in the event of fraud, a hack, malware, or a downturn in business prospects? Who will be responsible for refunding investments if something goes wrong?

- If investors do have legal rights, can investors effectively enforce them, and will there be adequate funds to compensate investors if their rights are violated?

Government-Run Virtual Currencies?

Some speculate that the next frontier for virtual currencies may be state-issued virtual currencies. Several governments have expressed interest, but it is unclear exactly how these projects would work. For instance, unlike digital fiat currencies, virtual currencies are decentralized in nature, so the idea of government control is difficult to reconcile with VC.

The presale for Venezuela's "petro" token began February 20. The Government of Venezuela has released contradictory details[35] about the ICO. For example, the official petro "white paper" had stated that the petro would be hosted on the Ethereum platform. Yet, as the presale was beginning, the government announced that the token would be hosted on the lesser-known NEM blockchain.[36] On March 19, as noted above, the White House issued an executive order banning U.S. persons from conducting any transactions related to virtual currencies issued by the Venezuelan government after January 9, 2018.[37]

Russia is reportedly considering the development of a "cryptoruble" to evade sanctions and perhaps to hedge against payment system cutoff, even as Russia's central bank has warned that other virtual token offerings "have all the signs of a financial pyramid."[38] Details remain unclear, since it is unknown who would issue the cryptoruble and who would be able to open an account.[39]

Other governments, along with banks, may continue to experiment with digital representations of fiat currency. Projects in this space would likely avoid the volatility associated with bitcoin and other virtual currencies, and governments would look to design a preferred level of transparency into each initiative. In Japan, for instance, a consortium of banks plans to launch the J Coin by 2020. Intended as a mobile-phone based cash replacement, the project aims to establish a digital currency convertible to the yen on a one-to-one basis, with central bank support.[40]

Endnotes

1 According to the U.S. Treasury Department, virtual currency is a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; is neither issued nor guaranteed by any jurisdiction; and does not have legal tender status in any jurisdiction. Digital currency, a broader category, includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency. In common usage, "cryptocurrency," "digital tokens," and "digital currency" are often used interchangeably with "virtual currency."

2 Evelyn Cheng, "Nearly $400 million lost, stolen from sales of new digital coins, Ernst & Young says," CNBC, January 22, 2018, https://www.cnbc.com/2018/01/22/nearly-400-million-lost-stolen-from-sales-of-new-digital-coins.html.

3 Sean Foley, Jonathan R. Karlsen, and Talis J. Putnins, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?" SSRN, January 30, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645.

4 "Executive Order: Taking Additional Steps to Address the Situation in Venezuela," March 19, 2018, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/vz_eo_petro.pdf.

5 "Frequently Asked Questions," 559-563, OFAC, March 19, 2018, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.

6 "Frequently Asked Questions," 559 and 561, OFAC, March 19, 2018, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.

7 "Frequently Asked Questions," 560, OFAC, March 19, 2018, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.

8 "Frequently Asked Questions," 562, OFAC, March 19, 2018, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.

9 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(a)(2). See generally FIN-2012-A001, "Foreign-Located Money Services Businesses," February 15, 2012.

10 "Combatting the Opioid Crisis: Exploiting Vulnerabilities in International Mail," Staff Report, Permanent Subcommittee on Investigations, U.S. Senate, https://www.portman.senate.gov/public/index.cfm/files/serve?File_id=12F93202-C8EC-4AF1-8A66-181EE6716F37.

11 "A.G. Schneiderman Launches Inquiry Into Cryptocurrency 'Exchanges,'" New York State Office of the Attorney General, April 17, 2018, https://ag.ny.gov/press-release/ag-schneiderman-launches-inquiry-cryptocurrency-exchanges.

12 "China Escalates Crackdown on Cryptocurrency Trading," Bloomberg News, January 15, 2018, https://www.bloomberg.com/news/articles/2018-01-15/china-is-said-to-escalate-crackdown-on-cryptocurrency-trading.

13 Francesco Guarascio, "EU agrees clampdown on bitcoin platforms to tackle money laundering," Reuters, December 15, 2017, https://www.reuters.com/article/uk-eu-moneylaundering/eu-agrees-clampdown-on-bitcoin-platforms-to-tackle-money-laundering-idUSKBN1E928M.

14 "Digital currency exchange providers: register online with AUSTRAC," April 3, 2018, http://www.austrac.gov.au/news/digital-currency-exchange-providers-register-online-austrac.

15 John Boyd, "Japan Takes Lead in Legitimizing Digital Currencies," IEEE Spectrum, May 12, 2017, https://spectrum.ieee.org/tech-talk/computing/it/japan-takes-lead-in-legitimizing-digital-currencies.

16 Takahiko Wada and Thomas Wilson, "Japan's cryptocurrency exchanges to set up self-regulatory body," Reuters, March 1, 2018, https://www.reuters.com/article/us-crypto-currencies-japan/japans-cryptocurrency-exchanges-to-set-up-self-regulatory-body-idUSKCN1GE037.

17 Kyungji Cho, "Why the Cryptocurrency World Is Watching South Korea," Bloomberg News, February 4, 2018, https://www.bloomberg.com/news/articles/2018-02-04/why-the-cryptocurrency-world-is-watching-south-korea-quicktake.

18 Ben Chu, "Cryptocurrency exchanges to face regulatory clampdown, says Bank of England's Mark Carney," The Independent, March 2, 2018, http://www.independent.co.uk/news/business/news/url-cryptocurrency-bitcoin-regulation-trading-uk-mark-carney-bank-of-england-clampdown-a8236066.html.

19 Gregor Stuart Hunter and Julie Steinberg, "Risk-Wary Banks Chill Bitcoin Market," Wall Street Journal, April 26, 2017, https://www.wsj.com/articles/risk-wary-banks-chill-bitcoin-market-1493206300.

20 SEC Filings, Bank of America, http://investor.bankofamerica.com/phoenix.zhtml%3Fc%3D71595%26p%3Dirol-sec.

21 Alistair Gray, "Bank of America cautions on potential cryptocurrency threat," Financial Times, February 23, 2018, https://www.ft.com/content/99fdd3e4-1821-11e8-9e9c-25c814761640.

22 Kate Beioley and James Pickford, "Bitcoin investors struggle to cash out new fortunes," Financial Times, January 12, 2018, https://www.ft.com/content/40c64992-f606-11e7-88f7-5465a6ce1a00.

23 "Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses," FinCEN, 2008, https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf.

24 According to Manju Manglani, 78% of AML compliance officers at a recent compliance conference said their financial institution is not monitoring transactions for cryptocurrency activity. https://twitter.com/ManjuManglani/status/983695810104881154.

25 Richard Kastelein, "What Initial Coin Offerings Are, and Why VC Firms Care," Harvard Business Review, March 24, 2017, https://hbr.org/2017/03/what-initial-coin-offerings-are-and-why-vc-firms-care.

26 Richard Kastelein, "What Initial Coin Offerings Are, and Why VC Firms Care," Harvard Business Review, March 24, 2017, https://hbr.org/2017/03/what-initial-coin-offerings-are-and-why-vc-firms-care.

27 "FINMA publishes ICO guidelines," Swiss Financial Market Supervisory Authority, February 16, 2018, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.

28 "SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds," U.S. Securities and Exchange Commission, September 29, 2017, https://www.sec.gov/news/press-release/2017-185-0.

29 Evelyn Cheng, "Nearly $400 million lost, stolen from sales of new digital coins, Ernst & Young says," CNBC, January 22, 2018, https://www.cnbc.com/2018/01/22/nearly-400-million-lost-stolen-from-sales-of-new-digital-coins.html.

30 Evelyn Cheng, "Nearly $400 million lost, stolen from sales of new digital coins, Ernst & Young says," CNBC, January 22, 2018, https://www.cnbc.com/2018/01/22/nearly-400-million-lost-stolen-from-sales-of-new-digital-coins.html.

31 "SEC Emergency Action Halts ICO Scam," U.S. Securities and Exchange Commission," December 4, 2017, https://www.sec.gov/news/press-release/2017-219.

32 "CFTC Charges Randall Crater, Mark Gillespie, and My Big Coin Pay, Inc. with Fraud and Misappropriation in Ongoing Virtual Currency Scam," U.S. Commodity Futures Trading Commission, January 24, 2018, http://www.cftc.gov/PressRoom/PressReleases/pr7678-18#PrRoWMBL. See also Jean Eaglesham and Paul Vigna, "Cryptocurrency Firms Targeted in SEC Probe," Wall Street Journal, February 28, 2018, https://www.wsj.com/articles/sec-launches-cryptocurrency-probe-1519856266?tesla=y&mod=e2tw.

33 As noted above, South Korea's stance on VC issues remains in flux.

34 Jay Clayton, "Statement on Cryptocurrencies and Initial Coil Offerings," U.S. Securities and Exchange Commission, December 11, 2017, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

35 David Floyd, "Venezuela's Petro Isn't Oil-Backed. It's not Even A Cryptocurrency," Investopedia (opinion), February 22, 2018, https://www.investopedia.com/news/venezuela-petro-not-cryptocurrency/.

36 Timothy B. Lee, "Venezuela says its cryptocurrency raised $735 million—but it's a farce," Ars Technica, February 22, 2018, https://arstechnica.com/tech-policy/2018/02/venezuela-says-its-cryptocurrency-raised-735-million-but-its-a-farce/.

37 "Executive Order: Taking Additional Steps to Address the Situation in Venezuela," March 19, 2018, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/vz_eo_petro.pdf.

38 Max Seddon and Martin Arnold, "Putin considers 'cryptorouble' as Moscow seeks to evade sanctions," Financial Times, January 1, 2018, https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da.

39 Max Seddon and Martin Arnold, "Putin considers 'cryptorouble' as Moscow seeks to evade sanctions," Financial Times, January 1, 2018, https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da.

40 Martin Arnold and Leo Lewis, "Japan's big banks plan digital currency launch," Financial Times, September 25, 2017, https://www.ft.com/content/ca0b3892-a201-11e7-9e4f-7f5e6a7c98a2.