



# ICLG

The International Comparative Legal Guide to:

## Fintech 2018

### 2nd Edition

A practical cross-border insight into Fintech law

Published by Global Legal Group, with contributions from:

A&L Goodbody

Advokatfirmaet BAHR AS

Anderson Mōri & Tomotsune

Anjarwalla & Khanna

Appleby

ATZ Law Chambers

Bär & Karrer Ltd.

BBA

BonelliErede

Bonn Steichen & Partners

Bredin Prat

De Brauw Blackstone Westbroek

ENSafrica

Erciyas Law Office

Etah-Nan & Co, Attorneys

Evris Law Firm

Galicia Abogados, S.C.

Gilbert + Tobin

Gleiss Lutz

Goldfarb Seligman & Co.

Gorrissen Federspiel

GVZH Advocates

Haiwen & Partners

ISOLAS LLP

Kim & Chang

Lee and Li, Attorneys-at-Law

Mannheimer Swartling

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

McMillan LLP

MinterEllisonRuddWatts

QUORUS GmbH

Rahayu and Partners Law Offices  
in Association with HFW

Romulo

Roschier, Attorneys Ltd.

Shearman & Sterling LLP

Shearn Delamore & Co.

Shook Lin & Bok LLP

Slaughter and May

Trilegal

Udo Udoma & Belo-Osagie

Uría Menéndez

Uría Menéndez – Proença de Carvalho

Wilmer Cutler Pickering Hale and Dorr LLP

WKB Wierciński, Kwiecieński, Baehr

Yale Law School



global legal group

**Contributing Editors**  
Rob Sumroy and Ben Kingsley, Slaughter and May

**Sales Director**  
Florjan Osmani

**Account Director**  
Oliver Smith

**Sales Support Manager**  
Toni Hayward

**Sub Editor**  
Jane Simmons

**Senior Editors**  
Suzie Levy  
Caroline Collingwood

**CEO**  
Dror Levy

**Group Consulting Editor**  
Alan Falach

**Publisher**  
Rory Smith

**Published by**  
Global Legal Group Ltd.  
59 Tanner Street  
London SE1 3PL, UK  
Tel: +44 20 7367 0720  
Fax: +44 20 7407 5255  
Email: info@glgroup.co.uk  
URL: www.glgroup.co.uk

**GLG Cover Design**  
F&F Studio Design

**GLG Cover Image Source**  
iStockphoto

**Printed by**  
Stephens & George  
Print Group  
May 2018

Copyright © 2018  
Global Legal Group Ltd.  
All rights reserved  
No photocopying

ISBN 978-1-912509-08-9  
ISSN 2399-9578

**Strategic Partners**



**General Chapters:**

1	<b>Artificial Intelligence in Fintech</b> – Rob Sumroy & Ben Kingsley, Slaughter and May	1
2	<b>U.S. Regulation of Cryptocurrency as a Type of Financial Technology</b> – Franca Harris Gutierrez & Sharon Cohen Levin, Wilmer Cutler Pickering Hale and Dorr LLP	7
3	<b>Fintech and Private Equity: Blockchain Technology Use Cases</b> – Jonathan Cardenas, Yale Law School	12

**Country Question and Answer Chapters:**

4	<b>Australia</b>	Gilbert + Tobin: Peter Reeves	16
5	<b>Brazil</b>	Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados: Renato Schermann Ximenes de Melo & Fabio Ferreira Kujawski	23
6	<b>Cameroon</b>	Etah-Nan & Co, Attorneys: Brice Tcheuffa & Hervé Feudjougou	28
7	<b>Canada</b>	McMillan LLP: Pat Forgione & Jeffrey Nagashima	33
8	<b>China</b>	Haiwen & Partners: Jinen Zhang & Xixiang Lin	39
9	<b>Denmark</b>	Gorrissen Federspiel: Morten Nybom Bethe & Tue Goldschmieding	45
10	<b>Finland</b>	Roschier, Attorneys Ltd.: Niklas Östman & Sonja Heiskala	51
11	<b>France</b>	Bredin Prat: Bena Mara & Vincent Langenbach	57
12	<b>Germany</b>	Gleiss Lutz: Dr. Stefan Weidert & Dr. Martin Viciano Gofferje	63
13	<b>Gibraltar</b>	ISOLAS LLP: Joey Garcia & Jonathan Garcia	69
14	<b>Hong Kong</b>	Slaughter and May: Benita Yu & Jason Webber	75
15	<b>Iceland</b>	BBA: Baldvin Björn Haraldsson & Stefán Reykjalín	83
16	<b>India</b>	Trilegal: Kosturi Ghosh & Preethi Srinivas	89
17	<b>Indonesia</b>	Rahayu and Partners Law Offices in Association with HFW: Sri Hartati Rahayu & Indriana Pramesti	95
18	<b>Ireland</b>	A&L Goodbody: Claire Morrissey & Peter Walker	101
19	<b>Isle of Man</b>	Appleby: Claire Milne & Mark Emery	109
20	<b>Israel</b>	Goldfarb Seligman & Co.: Ariel Rosenberg & Sharon Gazit	115
21	<b>Italy</b>	BonelliErede: Federico Vezzani & Tommaso Faelli	121
22	<b>Japan</b>	Anderson Mōri & Tomotsune: Taro Awataguchi & Ken Kawai	127
23	<b>Kenya</b>	Anjarwalla & Khanna: Sonal Sejpal & Dominic Rebelo	133
24	<b>Korea</b>	Kim & Chang: Jung Min Lee & Samuel Yim	138
25	<b>Luxembourg</b>	Bonn Steichen & Partners: Pierre-Alexandre Degehet & Marie Casanova	144
26	<b>Malaysia</b>	Shearn Delamore & Co.: Christina Kow & Timothy Siaw	149
27	<b>Malta</b>	GVZH Advocates: Dr. Andrew J. Zammit & Dr. Kurt Hyzler	156
28	<b>Mexico</b>	Galicia Abogados, S.C.: Mariana Islas & Claudio Kure	161
29	<b>Netherlands</b>	De Brauw Blackstone Westbroek: Richard van Staden ten Brink & Björn Schep	166
30	<b>New Zealand</b>	MinterEllisonRuddWatts: Jeremy Muir & Lloyd Kavanagh	173
31	<b>Nigeria</b>	Udo Udoma & Belo-Osagie: Yinka Edu & Tolulope Osindero	179
32	<b>Norway</b>	Advokatfirmaet BAHR AS: Markus Nilssen & Sondre Graasvoll	185
33	<b>Philippines</b>	Romulo: Claudia Squillantini & Agustin Montilla	191
34	<b>Poland</b>	WKB Wierciński, Kwiecieński, Baehr: Marcin Smolarek & Agnieszka Wiercińska-Krużewska	196

Continued Overleaf →

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

**Disclaimer**

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication. This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

35	<b>Portugal</b>	Uría Menéndez – Proença de Carvalho: Pedro Ferreira Malaquias & Hélder Frias	203
36	<b>Russia</b>	QUORUS GmbH: Maxim Mezentsev & Nikita Iovenko	211
37	<b>Singapore</b>	Shook Lin & Bok LLP: Andrea Chee & Agnes Lim	219
38	<b>South Africa</b>	ENSafrica: Prof. Angela Itzikowitz & Era Gunning	227
39	<b>Spain</b>	Uría Menéndez: Leticia López-Lapuente & Livia Solans	233
40	<b>Sweden</b>	Mannheimer Swartling: Martin Pekkari & Anders Bergsten	241
41	<b>Switzerland</b>	Bär & Karrer Ltd.: Dr. Daniel Flühmann & Dr. Peter Hsu	247
42	<b>Taiwan</b>	Lee and Li, Attorneys-at-Law: Robin Chang & Benjamin K. J. Li	254
43	<b>Tanzania</b>	ATZ Law Chambers: Shamiza Ratansi & Aggrey Ernest	260
44	<b>Turkey</b>	Erciyas Law Office: Nihat Erciyas & Miraç Arda Erciyas	265
45	<b>Ukraine</b>	Evris Law Firm: Sergii Papernyk	270
46	<b>United Kingdom</b>	Slaughter and May: Rob Sumroy & Ben Kingsley	275
47	<b>USA</b>	Shearman & Sterling LLP: Reena Agrawal Sahni	282

## EDITORIAL

Welcome to the second edition of *The International Comparative Legal Guide to: Fintech*.

This guide provides corporate counsel and international practitioners with a comprehensive worldwide legal analysis of the laws and regulations of fintech.

It is divided into two main sections:

Three general chapters. These chapters provide an overview of artificial intelligence in fintech, the regulation of cryptocurrency as a type of financial technology, and fintech and private equity.

Country question and answer chapters. These provide a broad overview of common issues in fintech laws and regulations in 44 jurisdictions.

All chapters are written by leading fintech lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editors Rob Sumroy and Ben Kingsley of Slaughter and May for their invaluable assistance.

The *International Comparative Legal Guide* series is also available online at [www.iclg.com](http://www.iclg.com).

Alan Falach LL.M.  
Group Consulting Editor  
Global Legal Group  
[Alan.Falach@glgroup.co.uk](mailto:Alan.Falach@glgroup.co.uk)

# U.S. Regulation of Cryptocurrency as a Type of Financial Technology

Franca Harris Gutierrez



Sharon Cohen Levin



Wilmer Cutler Pickering Hale and Dorr LLP

## 1. Introduction

Cryptocurrencies have quickly expanded from their narrow roots to become a particularly popular and widely-discussed fintech product. Cryptocurrencies like Bitcoin simultaneously attract and worry investors with record highs and sudden drops in value.<sup>1</sup> Initial coin offerings (“ICOs”), where startups raise money and gain user adoption by issuing proprietary cryptocurrencies, have gained rapid and widespread embrace, totalling some \$5.6 billion in 2017 compared to \$240 million in 2016.<sup>2</sup> But with this enthusiasm comes questions about how best to regulate cryptocurrencies.

The U.S. financial regulatory regime is “functional,” which means that the laws and regulations governing financial products and services are technology agnostic and look through technology to the product or service being provided through the technology. And when technology is deployed to perform financial services, the company behind the technology enters one of the most heavily-regulated sectors of the economy. The fact that the innovations, such as cryptocurrencies, are attractive and potentially transformative does not exempt them from regulatory oversight.

There is surely a need for sensible regulation, as cryptocurrencies present risk to investors and consumers, and can be used to commit financial crime. The anonymity and global near-real time transaction capability associated with cryptocurrencies mean that cryptocurrencies can more effectively be used to commit financial crime and to launder money. These same elements make regulation challenging, rendering customer identification difficult, transaction monitoring a challenge, and suspicious activity detection especially complicated.

The question then is not whether cryptocurrencies and related technologies should be regulated, but how. And the answer thus far has for the most part been to extend existing regulatory frameworks to cover cryptocurrency products and services rather than to develop something new. Regulatory agencies have moved to regulate cryptocurrency in fits and starts, and have used different tools over time. This in part results from their differing legislative mandates, in part from the distinctive functions played by each regulator, and in part from the diverse uses of cryptocurrency.

In this article, we explain how government agencies have adapted existing regulatory frameworks to cryptocurrency. After briefly describing how regulators have approached issues of consumer and investor protection, the bulk of the article focuses on the application of anti-money laundering (“AML”) and U.S. economic sanctions laws and regulations to cryptocurrency.<sup>3</sup> In addressing new cryptocurrency technology and products, government agencies have not advocated for new laws or issued new regulations. Rather,

they have interpreted existing requirements through guidance and enforcement actions to announce their determination that cryptocurrencies are subject to existing legal obligations.

## 2. Investor and Consumer Protection

Government agencies charged with protecting consumers have moved to address the consumer and investor risks of cryptocurrency by issuing guidance and bringing enforcement actions that clarify the application of existing rules. In particular, the U.S. Commodity Futures Trading Commission (“CFTC”) and the U.S. Securities and Exchange Commission (“SEC”) have issued consumer advisories, provided resources to consumers, and brought enforcement actions on cryptocurrency issues.<sup>4</sup> These agencies have quickly asserted themselves as the primary regulators of cryptocurrency, interpreting their authority broadly to apply existing laws and regulations.

The CFTC became one of the first agencies to assert jurisdiction over cryptocurrencies when it moved to define cryptocurrencies as commodities.<sup>5</sup> Because the CFTC’s powers under the Commodities Exchange Act (“CEA”) generally extend to derivative transactions,<sup>6</sup> the agency has exercised its supervisory jurisdiction over derivatives markets involving cryptocurrency. The agency has also exercised its enforcement authority to police fraud and market manipulation in the cryptocurrency “spot” markets.<sup>7</sup> In *Commodity Futures Trading Commission v. McDonnell*, the CFTC claimed authority to bring enforcement actions in cryptocurrency spot markets under its anti-fraud and anti-manipulation enforcement powers.<sup>8</sup>

More recently, the SEC determined that the coins or tokens offered in an ICO may be securities and subject to federal securities laws depending on the facts and circumstances of an individual ICO.<sup>9</sup> An ICO coin may be a regulated security if the ICO includes an investment contract.<sup>10</sup> If an ICO implicates securities laws, the business must provide applicable disclosures and register with the SEC, among other requirements. In a recent speech at the Securities Regulation Institute, SEC Chairman Jay Clayton said that he has instructed SEC staff “to be on high alert” for ICOs that do not comply with the securities laws.<sup>11</sup> In addition to this public guidance, the SEC (and the CFTC) have brought several enforcement actions against cryptocurrency companies for consumer fraud and market manipulation.<sup>12</sup>

The Consumer Financial Protection Bureau (the “CFPB”) has consolidated responsibility for enforcing over a dozen consumer protection laws.<sup>13</sup> On August 11, 2014, the CFPB issued a consumer advisory warning consumers about the risks of cryptocurrency such as Bitcoin.<sup>14</sup> The advisory warned that exchange rates are volatile and unclear, there is risk with respect to hackers and scammers, and

stolen or lost funds may not be refunded.<sup>15</sup> Unlike the CFTC and SEC, which have been more aggressive with enforcement, the CFPB has yet to bring an enforcement action regarding cryptocurrencies. Established cryptocurrency businesses and businesses looking to enter the market should take heed, however, that the CFPB’s jurisdiction prohibiting unfair, deceptive, and abusive acts and practices, could potentially extend to cryptocurrency activities.<sup>16</sup>

### 3. Financial Crime Prevention

The financial crimes regime in the U.S. – including the U.S. AML regime under the Bank Secrecy Act (“BSA”) and the economic sanctions regime – requires significant investments in compliance. Companies are required to know and understand their customers, continuously monitor transactions for suspicious activity, file required reports, and comply with applicable sanctions laws. Penalties for failing to comply with the BSA and sanctions regulations are severe, ranging from millions of dollars in civil fines to criminal liability in severe cases.<sup>17</sup> BSA penalties apply to companies and individuals alike.

Any form of money movement service or technology presents substantial financial crime risk. Cryptocurrency presents special risks due to its anonymity and decentralisation, and cryptocurrencies are therefore viewed by law enforcement as a favoured tool for criminals. High-profile prosecutions of cryptocurrency criminals animate these concerns. In recent years, individuals associated with two online marketplaces were prosecuted for cryptocurrency activities. The first was Arthur Budovsky, who “ran a digital currency empire built expressly to facilitate money laundering...”<sup>18</sup> followed by Ross Ulbricht, creator of the Silk Road website that that enabled more than \$200 million of drug sales using Bitcoin.<sup>19</sup>

As a result, cryptocurrency businesses are already subject to extensive financial crime regulation. The agencies tasked with enforcing financial crimes regulations – including the prudential banking regulators, the SEC, the CFTC, the Financial Industry Regulatory Authority (“FINRA”), the Financial Crimes Enforcement Network (“FinCEN”), the Treasury Department’s Office of Foreign Asset Control (“OFAC”), and state-level regulators – have also concluded that new cryptocurrencies are subject to the same decades-old regulations that apply to brick-and-mortar banks. Cryptocurrency is a compelling example of how quickly these regulators adapt existing laws and regulations to new technology and businesses.

#### 3.1 Anti-money laundering

FinCEN too, through interpretive guidance, has announced that the BSA applies to “convertible virtual currencies”.<sup>20</sup> Like many developments in cryptocurrency regulation, this guidance did not announce any new laws or rules, but stated FinCEN’s determination that cryptocurrency companies were performing functions to which existing laws already applied. Much as the anonymity and decentralisation of cryptocurrency makes it a favoured tool for bad actors, these attributes also create unique compliance challenges for financial crimes compliance. Anonymity poses a problem because it might be difficult to identify the real identity of the person standing behind a cryptocurrency transaction. And for some cryptocurrencies, there is no central administrator that can implement and enforce financial crimes compliance controls, or whom investigators can contact for help in an investigation.

The BSA requires that all financial institutions implement effective anti-money laundering programmes.<sup>21</sup> “Financial institution” is defined broadly,<sup>22</sup> and the applicable regulations include “money services businesses” (“MSBs”) as a type of financial institution.<sup>23</sup> Most relevant to cryptocurrency, MSBs include a type of financial institution called money transmitters.<sup>24</sup> “Money transmission” under FinCEN’s regulations means “the acceptance of [coin and paper] currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or *other value that substitutes for currency* to another location or person by any means”.<sup>25</sup> This definition of money transmission does not differentiate between so-called “fiat” currencies and convertible virtual currencies.

Under these existing definitions, FinCEN has determined that transmitting a convertible virtual currency (which can be substituted for real currency) is money transmission and any company engaged in convertible virtual currency transmission is therefore a regulated money transmitter.<sup>26</sup> Cryptocurrency businesses dealing in convertible virtual currency are therefore found to be subject to the BSA and its implementing regulations. But only certain actors in a cryptocurrency transaction are money transmitters.

FinCEN’s guidance has become more specific over time, ultimately announcing the status of cryptocurrency users, exchangers, administrators, miners, and trading platforms:

- A user “obtains virtual currency to purchase goods or services”<sup>27</sup> and is not subject to BSA requirements. This means, for example, that an everyday consumer who purchases and uses Bitcoin for online transactions is not a money transmitter subject to the BSA.
- An exchanger is “a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency”.<sup>28</sup> Exchangers exist in two forms, both subject to the BSA.<sup>29</sup> In one form, a seller accepts real currency from a user and transmits that seller’s own cryptocurrency for equivalent value to that user in a virtual currency account. Under this scenario, the transmission of real currency at a user’s bank account to *another location* at the user’s virtual currency account with the cryptocurrency’s administrator constitutes money transmission.<sup>30</sup> In the alternative structure, the exchanger accepts currency from a user and privately credits the user with the exchanger’s own virtual currency, then transmits the internally credited value to third parties at the user’s direction. Under this scenario, the transfer of currency to *another person* at the user’s direction constitutes money transmission.<sup>31</sup>
- An administrator is “a person engaged as a business in issuing (putting into circulation) a virtual currency, who has the authority to redeem (to withdraw from circulation) such virtual currency”. Cryptocurrency administrators are subject to the BSA because, as an administrator of a centralised repository of virtual currency such as the person or business issuing the currency and later accepting it for a service, administrators transmit value between persons *or* from one location to another.<sup>32</sup>
- A miner of Bitcoin or other cryptocurrency would generally be considered a user that is not an MSB to the extent that it uses mined Bitcoins to pay for goods or services or to purchase real currency or other convertible virtual currency.<sup>33</sup> However, a person who transfers mined Bitcoins to a third party at the behest of a counterparty may be engaged in money transmission, and as such be subject to the BSA and FinCEN’s regulation.<sup>34</sup>
- A virtual currency trading platform, whereby users submit orders to the platform to buy or sell a cryptocurrency at a given price and the platform purchases, sells, and transfers the cryptocurrency to the buying user, would be considered a money transmitter subject to the BSA.<sup>35</sup>

One of the most recent examples of innovative cryptocurrency models becoming subject to an existing AML regulation is ICOs. In a letter addressed to U.S. Senator Ron Wyden, FinCEN stated that businesses engaged in issuing ICOs are money transmitters that must comply with AML requirements under the BSA and MSB regulations.<sup>36</sup> Businesses issuing an ICO may be considered an exchanger because, by nature, it exchanges its coin or token for the investor's legal tender or other cryptocurrencies during the ICO. The letter does not formally have the force of guidance or regulations, but because it indicates FinCEN's interpretation of the laws and regulations it enforces, businesses should still take heed. Future guidance or letters may extend FinCEN's reasoning on ICOs to token presales.

FinCEN has also used enforcement as a tool to announce policy, and the criminal penalties against BTC-e and its operator, Alexander Vinnik, underscore the severity of the consequences for cryptocurrency businesses violating the BSA and implementing regulations. In 2017, FinCEN fined the Russian-headquartered, foreign-located money transmitter and cryptocurrency exchange BTC-e \$110 million and operator Vinnik for \$12 million for wilful violations of the BSA, including failing to register as an MSB with FinCEN, failing to implement an effective AML programme, failing to file SARs, and violating recordkeeping requirements.<sup>37</sup> The conduct allegedly included, among other things, "process[ing] thousands of suspicious transactions without ever filing a single SAR"<sup>38</sup> and offering advice to users on how to process and access money obtained from illegal drug sales on the dark net.<sup>39</sup> Vinnik, as the person who administered BTC-e and who was the beneficial owner of its parent company, was prosecuted criminally for his activities. Vinnik, a Russian national, was indicted in the Northern District of California for allegedly laundering more than \$4 billion in Bitcoin through BTC-e, among a range of other crimes.<sup>40</sup> Vinnik was arrested in Greece in July 2017.<sup>41</sup>

### 3.2 Sanctions

Economic sanctions in the United States are administered and enforced principally by OFAC. A wilful sanctions violation is a criminal offence under the International Emergency Economic Powers Act<sup>42</sup> and the Trading With the Enemy Act.<sup>43</sup> Sanctions generally apply to U.S. Persons (citizens and permanent residents), companies incorporated in the U.S. and their foreign branches, and any person physically inside the United States.<sup>44</sup> Broadly, sanctions are either jurisdictional, where they bar imports or exports of goods or services from entire countries or regions (like Iran or Crimea), or list-based, in which sanctions are applied to individuals or entities who are listed for engaging in illicit activity like terrorism, malicious cyberattacks, transnational organised crime, or WMD proliferation. The sanctions themselves can take many forms. List-based sanctions traditionally have involved a requirement that persons subject to U.S. jurisdiction block the assets of listed persons and refrain from providing them with any goods, support, or services of any kind.<sup>45</sup> But more recent sanctions programmes, like some imposed for actions by Russia and Venezuela, have involved innovative restrictions on dealings in certain categories of debt or equity.

Like other regulators, OFAC has confirmed that its existing regulatory structure applies to cryptocurrency. OFAC has also weighed in on issues relating to sanctions compliance by issuing guidance in the form of Frequently Asked Questions ("FAQs"). This is the manner in which OFAC often issues guidance on sanctions

compliance and it has done so with respect to cryptocurrency issues twice. In these pronouncements, OFAC confirmed that sanctions compliance obligations are the same whether a transaction is conducted in virtual currency or fiat currency.<sup>46</sup> It also said that it will use sanctions against those who use virtual currencies to engage in conduct that would otherwise be sanctionable,<sup>47</sup> and that it may begin including digital wallet addresses of sanctioned persons along with other identifying information when it updates its sanctions programmes.<sup>48</sup>

This guidance does not alter existing sanctions compliance obligations; persons subject to U.S. jurisdiction were always prohibited from engaging in virtual currency transactions with designated persons, even before the guidance was issued. However, OFAC's statements clarify certain compliance obligations and may raise compliance expectations for persons subject to U.S. jurisdiction that regularly send/receive cryptocurrency. All persons subject to U.S. jurisdiction will be barred from engaging in transactions with wallet addresses that have been added to the SDN list. But virtual currency exchanges, for example, will be expected to develop a more sophisticated ability to screen out prohibited wallet addresses in their exchange activity.

In March 2018, OFAC developed a sanctions programme oriented specifically around cryptocurrency for the first time. Driven in part by concerns that Venezuela would use its own bespoke cryptocurrency, the Petro, to evade U.S. sanctions imposed in the summer of 2017, OFAC published an Executive Order barring persons subject to U.S. jurisdiction from dealing in any digital currency issued by or for the Government of Venezuela after January 9, 2018.

Given the risks that cryptocurrency will be used to evade sanctions or engage in other forms of criminal behaviour, OFAC will likely remain active on these issues.

## 4. Conclusion

Fintech has and continues to change the financial services industry, but as it does so, it enters a highly regulated field. Nowhere is this more evident than in cryptocurrency, where businesses navigate an increasingly complicated environment in consumer protection and have become subject to extensive anti-financial crimes compliance requirements. Both new and existing cryptocurrency businesses need to be aware that they are not immune from oversight and may find themselves subject to existing regulatory schemes without any change in the underlying law.

## 5. Endnotes

1. See, e.g., Steven Russolillo and Andrew Jeong, *Bitcoin Falls Below \$6,000, Plummeting 70% from December High*, WALL STREET J. (Feb. 6, 2018), <https://www.wsj.com/articles/bitcoin-falls-below-6-000-plummeting-70-from-december-high-1517907009>.
2. See Oscar Williams-Grut, *Only 48% of ICOs were Successful Last Year—But Startups Still Managed to Raise \$5.6 Billion*, BUSINESS INSIDER (Jan. 31, 2018), <http://markets.businessinsider.com/currencies/news/how-much-raised-icos-2017-token-data-2017-2018-1-1014647330>.
3. This article refers to "cryptocurrency" as a comprehensive term encompassing all virtual currencies currently existing in the market, as the best known of which are Bitcoin, Ethereum, and Litecoin; the market currently includes thousands of cryptocurrencies. "Cryptocurrency" is itself a term of art,

- and regulators may use different terminology. For example, the Financial Crimes Enforcement Network uses the term “virtual currency”, meaning “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency”. See DEP’T OF THE TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, APPLICATION OF FINCEN’S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES, FIN-2013-G001 (2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> [hereinafter “FinCEN 2013 Guidance”].
4. See, e.g., U.S. Commodity Futures Trading Comm’n, Virtual Currency Resources, <https://www.cftc.gov/Bitcoin/index.htm>; U.S. Sec. & Exch. Comm’n, Investor Alert: Bitcoin and Other Virtual Currency-Related Investments (May 7, 2014), <https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-bitcoin-other-virtual-currency>; SEC Office of Inv’r Educ. & Advocacy, Investor Alert: Ponzi Schemes Using Virtual Currencies, SEC Pub. No. 153 (7/13), available at [https://www.sec.gov/investor/alerts/ia\\_virtualcurrencies.pdf](https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf).
  5. See U.S. COMMODITY FUTURES TRADING COMM’N, CFTC BACKGROUNDER ON OVERSIGHT OF AND APPROACH TO VIRTUAL CURRENCY FUTURES MARKETS 2 (2018), [http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/backgrounder\\_virtualcurrency01.pdf](http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/backgrounder_virtualcurrency01.pdf) [“CFTC Backgrounder”].
  6. See 7 U.S.C. § 2(a)(1).
  7. See CFTC Backgrounder at 2.
  8. See *Commodity Futures Trading Comm’n v. McDonnell*, No. 1:18-cv-00361-JBW-RLM, slip op. (E.D.N.Y. Mar. 6, 2018) (mem.).
  9. See Sec. & Exch. Comm’n, *Investor Bulletin: Initial Coin Offerings* (Jul. 25, 2017), [https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib\\_coinofferings](https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings).
  10. Which is generally defined as “an investment of money in a common enterprise with a reasonable expectations of profits to be derived from the entrepreneurial or managerial efforts of others”. See Sec. & Exch. Comm’n, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Release No. 81207 at 11–15 (Jul. 25, 2017), <https://www.sec.gov/litigation/investreport/34-81207.pdf>.
  11. See Jay Clayton, SEC Chairman, Opening Remarks at the Securities Regulation Institute (Jan. 22, 2018), <https://www.sec.gov/news/speech/speech-clayton-012218>.
  12. See, e.g., *In re Coinflip, Inc.*, No. 15–29, 2015 WL 5535736 (C.F.T.C. Sept. 17, 2015); *In re BFXNA Inc.*, No. 16–19, 2016 WL 3137612 (C.F.T.C. June 2, 2016); *SEC v. Shavers*, No. 13-CV-00416, 2014 WL 4652121 (E. D. Tex. Sept. 18, 2014).
  13. 12 U.S.C. § 5511; 12 U.S.C. § 5581.
  14. See CONSUMER FIN. PROT. BUREAU, CONSUMER ADVISORY: RISKS TO CONSUMERS POSED BY VIRTUAL CURRENCIES (2014), [https://files.consumerfinance.gov/f/201408\\_cfpb\\_consumer-advisory\\_virtual-currencies.pdf](https://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf).
  15. *Id.*
  16. 12 U.S.C. § 5531(a).
  17. See 31 U.S.C. § 5321; 31 U.S.C. § 5322.
  18. <https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years>.
  19. <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-creator-and-owner-silk-road-website-found-guilty-manhattan-federal-court>.
  20. See FinCEN 2013 Guidance at 3–4.
  21. See 31 U.S.C. § 5311; 31 C.F.R. § 1010.210.
  22. See 31 U.S.C. § 5312(a)(2), (c)(1).
  23. See 31 C.F.R. § 1010.100(t).
  24. 31 C.F.R. § 1010.100(ff).
  25. 31 C.F.R. § 1010.100(f)(5)(i)(A) (emphasis added).
  26. See generally FinCEN 2013 Guidance.
  27. See FinCEN 2013 Guidance at 2.
  28. See *id.*
  29. See FinCEN 2013 Guidance at 4.
  30. See *id.*
  31. See *id.*
  32. See *id.*
  33. See, e.g., U.S. DEP’T OF THE TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, APPLICATION OF FINCEN’S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATION, FIN-2014-R001, at 3 (2014), <https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf>.
  34. See *id.*
  35. See, U.S. DEP’T OF THE TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN’S REGULATIONS TO A VIRTUAL CURRENCY TRADING PLATFORM, FIN-2014-R011, at 1 (2014), [https://www.fincen.gov/sites/default/files/administrative\\_ruling/FIN-2014-R011.pdf](https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf).
  36. See Letter from Drew Maloney, Assistant Sec’y for Leg. Affairs, FinCEN, to Ron Wyden, U.S. Senator, at 3 (Feb. 13, 2018), <https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf>.
  37. See Assessment of Civil Money Penalty, *In re BTC-e*, No. 2017-03 (FinCEN Jul. 27, 2017), [https://www.fincen.gov/sites/default/files/enforcement\\_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf](https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf).
  38. *Id.* at 7.
  39. See Press Release, U.S. Dep’t of the Treasury, FinCEN, FinCEN Fines BTC-e Virtual Currency Exchange \$110 Million for Facilitating Ransomware, Dark Net Drug Sales (Jul. 27, 2017), <https://www.fincen.gov/sites/default/files/2017-07/BTC-e%20July%2026%20Press%20Release%20FINAL1.pdf>.
  40. See Press Release, Dep’t of Justice, U.S. Atty’s Office, 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, (Jul. 26, 2017), <https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged>.
  41. See Samuel Gibbs, “Criminal Mastermind” of \$4bn Bitcoin Laundering Scheme Arrested, THE GUARDIAN (Jul. 27, 2017), <https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik>.
  42. See 50 U.S.C. § 1701 *et seq.*
  43. See 50 U.S.C. § 4301 *et seq.*
  44. The Iran and Cuba sanctions programmes also apply to foreign-incorporated subsidiaries of U.S. companies.
  45. Sanctions programmes typically also include licences that allow persons subject to U.S. jurisdiction to engage in otherwise-prohibited activity with a sanctioned person if it falls within the scope of the licence. Many sanctions programmes, for example, contain licences that allow the provision of humanitarian aid to otherwise prohibited parties.

- 46. See U.S. Dep't of the Treasury, Resource Center, OFAC FAQs: Sanctions Compliance, Questions on Virtual Currency, FAQ 560 (Mar. 19, 2018), [https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq\\_compliance.aspx](https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx).
- 47. See *id.*
- 48. See *id.* at FAQ 562.

### Acknowledgment

The authors would like to acknowledge the assistance of their colleagues Bradford Hardin (Counsel), Jennifer Jacoby Altscher (Senior Associate), Zachary Goldman (Senior Associate), and Nicholas Simons (Associate). The WilmerHale lawyers are members of the Regulatory and Government Affairs Department and the Fintech Working Group, a multi-disciplinary team of lawyers that counsels clients in all of the material issues that financial institutions, corporate clients and Fintech emerging companies must navigate in this rapidly evolving market sector.



**Franca Harris Gutierrez**  
Wilmer Cutler Pickering Hale and Dorr LLP  
1875 Pennsylvania Avenue  
Washington, DC 20006  
USA  
  
Tel: +1 202 663 6557  
Email: [franca.gutierrez@wilmerhale.com](mailto:franca.gutierrez@wilmerhale.com)  
URL: [www.wilmerhale.com](http://www.wilmerhale.com)

Franca Harris Gutierrez is Vice Chair of the Financial Institutions Practice Group at WilmerHale. Since helping to launch the first online bank during the dot-com era, Ms. Harris Gutierrez has provided regulatory counsel to some of the most innovative and successful financial services ventures, including new product development for prominent peer-to-peer, mobile, and online-only lending and payments platforms. She regularly advises clients on the complex regulatory, transactional, outsourcing, and vendor management issues raised by cutting edge financial innovations. Ms. Harris Gutierrez also maintains an active transactional practice, representing financial institutions in the negotiation and documentation of acquisitions and divestitures, reorganisations, joint ventures, and technology transactions. Ms. Harris Gutierrez is an active member of WilmerHale's Consumer Financial Protection Bureau Working Group and the Fintech Group. She joined WilmerHale from the Office of the Comptroller of the Currency.

Ms. Harris Gutierrez's full professional profile is available at: [https://www.wilmerhale.com/franca\\_gutierrez/](https://www.wilmerhale.com/franca_gutierrez/).



**Sharon Cohen Levin**  
Wilmer Cutler Pickering Hale and Dorr LLP  
7 World Trade Center, 250 Greenwich Street  
New York, New York 10007  
USA  
  
Tel: +1 212 230 8804  
Email: [sharon.levin@wilmerhale.com](mailto:sharon.levin@wilmerhale.com)  
URL: [www.wilmerhale.com](http://www.wilmerhale.com)

Sharon Cohen Levin is a leading authority on anti-money laundering ("AML"), Bank Secrecy Act ("BSA"), economic sanctions and asset forfeiture. She served for 19 years as Chief of the Money Laundering and Asset Forfeiture Unit in the US Attorney's Office for the Southern District of New York ("SDNY"). Under her leadership, the SDNY forfeited in excess of \$15 billion. During her tenure at SDNY, Ms. Levin prosecuted and supervised many of the Department of Justice's most complex and significant money laundering, sanctions and asset forfeiture prosecutions, including the investigation and prosecution of BNP Paribas, SAC Capital, Lebanese Canadian Bank and 650 Fifth Avenue. Since joining WilmerHale she has represented a diverse array of financial institutions with respect to AML and sanctions issues, including developing AML and sanctions programmes and counselling clients on AML and sanctions compliance. Ms. Levin represents individuals and institutions in criminal, civil and regulatory investigations and enforcement actions. She brings unique skills to clients seeking representation in complex financial services litigation and compliance requirements for regulated entities.

Ms. Cohen Levin's full professional profile is available at: [https://www.wilmerhale.com/Sharon\\_Levin/](https://www.wilmerhale.com/Sharon_Levin/).



WILMER CUTLER PICKERING HALE AND DORR LLP

WilmerHale provides legal representation across a comprehensive range of practice areas that are critical to the success of our clients. We practice at the very top of the legal profession and offer a cutting-edge blend of capabilities that enables us to handle deals and cases of any size and complexity. WilmerHale is at the forefront of the most challenging litigation, enforcement, compliance, regulatory and transactional issues in banking and financial services.

Clients look to our Financial Institutions Group for assistance with complex matters that impact them as banks, card issuers, insurance companies, broker-dealers, mortgage lenders, student loan servicers, database operators, FinTech firms or investors in the financial sector. We have extensive experience in banking controversies, retail financial services and the Consumer Financial Protection Bureau ("CFPB"), prudential and foreign bank regulatory advice, financial technology, and business transactions.

## Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms



59 Tanner Street, London SE1 3PL, United Kingdom  
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255  
Email: [info@glgroup.co.uk](mailto:info@glgroup.co.uk)