

Los Angeles Lawyer

NOVEMBER 2018 / \$5

**SCOTUS
Acceptance
of Patent
Inter Partes
Review**

page 22

.....
**On Direct:
Feminist
Brenda Feigen**

page 10

**LACBA Meets
Veterans'
Legal Needs**

page 60

PLUS

**Civil Code
Section
1714.10
Prefiling
Order**

page 30

The Wild West of Cryptocurrency

EARN MCLE CREDIT

Los Angeles lawyer Nathan J. Hochman presents an overview of strategies used by U.S. government agencies to regulate and control cryptocurrency activity

page 14

MCLE ARTICLE AND SELF-ASSESSMENT TEST

By reading this article and answering the accompanying test questions, you can earn one MCLE credit. To apply for credit, please follow the instructions on the test answer sheet on page 19.



PART ONE OF TWO

by NATHAN J. HOCHMAN

P O L I C I N G T H E

WILD WEST OF CRYPTOCURRENCY

In response to nonreporting by cryptocurrency users, DOJ uses the “stick” of criminal prosecutions to drive compliance and IRS presents taxpayers a “carrot” of voluntary disclosure

ON May 22, 2010, the first reported Bitcoin transaction occurred when a Florida man offered to pay for two large Papa John’s pizzas with 10,000 bitcoins.¹ Those pizzas cost the British man who took up the offer \$25 back then. Today, they would be worth over \$60 million as the “Wild West” of cryptocurrency has arrived. Few would have predicted that when the enigmatic Satoshi Nakamoto published a nine-page White Paper in October 2008 laying out the blockchain foundations of Bitcoin,² less than a decade later the cryptocurrency market would be measured in the hundreds of billions of dollars, having grown exponentially with the capacity to transform every industry across the globe.

The speed with which cryptocurrency has emerged in the

financial world has outstripped the speed with which financial agencies have been able to regulate it and enforce potentially outdated laws to protect financial markets and Main Street participants. In the United States, law enforcement agencies have struggled to decide exactly what cryptocurrency is. To the Internal Revenue Service (IRS), it is “property” potentially subject to capital gains treatment.³ To the Securities and Exchange Commission (SEC), it may be a “security,” depending on how it is issued or used subject to registration and reporting requirements.⁴ To the Commodity Futures Trading Commission (CFTC), it is a “commodity,”⁵ while to the Department of Treasury’s Financial Crimes Enforcement Network (FinCEN), it is treated mostly as a “convertible virtual currency.”⁶

Nathan J. Hochman is deputy chair of Morgan, Lewis & Bockius LLP’s White Collar Litigation and Government Investigations practice. He formerly worked as assistant attorney general for the U.S. Department of Justice’s Tax Division and as an assistant U.S. attorney for the Central District of California.

MICHAEL CALLAWAY



To appreciate how the “crypto-sheriffs” have attempted to enforce the current laws on the books to address “crypto-schemes,” “crypto-fraud,” and other forms of “crypto-crime,” it is important to understand how cryptocurrency works and the types of crimes that may emanate from its use.

What is Cryptocurrency?

Cryptocurrency or virtual currency is broadly speaking a digital representation of value that may function as a medium of exchange, a unit of account, and/or a store of value. The revolutionary aspects of this currency are that it does not require a central authority like a bank to act as the gatekeeper for the currency transactions; instead, it runs on a decentralized peer-to-peer global network of computers that rely on network participants to validate and log transactions on a permanent, public distributed ledger, commonly known as a blockchain.

Bitcoin is the most widely known form of cryptocurrency, though there are over 1,500 alternatives (“altcoins”) including the widely transacted Ether, Litecoin, and Ripple. To understand a cryptocurrency transaction, one can use a hypothetical Bitcoin transaction as an example. Assume “Bob” wants to transfer to “Lisa” 10 bitcoins valued at \$10,000 each to purchase \$100,000 of goods from Lisa. Bob has 10 bitcoins in his Bitcoin wallet, which is like an electronic folder where he stores his digital currency; Lisa also has a digital wallet. Bob and Lisa have “public keys” to their digital wallets, which are cryptographically generated digital addresses analogous to bank account numbers. Bob sends Lisa a message transmitting his 10 bitcoins to Lisa’s public key and “signs” it with his “private key,” a randomly generated string of alphanumeric characters known only to Bob that function like a PIN for his bank account. The difference between a PIN number and a private key, however, is that if Bob loses his private key, there is no way to recover it and thus no way to access any cryptocurrency in his digital wallet. The Bob-Lisa transfer of 10 bitcoins is then broadcast to a decentralized global network for verification. Participants in the network, called miners, use a predetermined verification process to confirm whether Bob is the rightful owner of those 10 bitcoins. If they are the first to solve a mathematical puzzle relating to this transaction, new virtual currency coins are generated and awarded to that miner. After verification, the transaction settles, is time-stamped, and permanently recorded as part of another block on the blockchain. The verification process, which happens very quickly, helps ensure the security of the transaction since no individual entry can be altered without changing every previous entry on the blockchain on the majority of computers in the global network.

The advantages to the financial transaction of Bob and Lisa are manifold. First, the transaction occurs without any intermediary—like a financial institution—but directly between Bob and Lisa. Second, there are no wire transaction fees, credit reports, collateral requirements, or escrow commissions involved in the transaction (other than minor “miner” transaction fees incurred). Third, the transaction transpires in minutes rather than hours or days as the funds do not need to move from one bank to another. Fourth, the transaction does not require Bob or Lisa to know each other; as long as Bob has Lisa’s public key to her digital account, they both can remain anonymous to each other. The blockchain records their digital addresses but does not otherwise reveal any other aspect of identity or location. Fifth, the transaction can occur from anywhere in the world as long as the parties have access to the Internet, whether the parties are literally sitting next to each other in a room or separated across the globe. Sixth, once the transaction is accomplished and recorded on the blockchain, it is final, cannot be reversed, and is transparent

since the entire history of the blockchain can be viewed anywhere in the world at any time of the day or night.⁷

What if Lisa wants to convert her 10 bitcoins into traditional or “fiat” currency (e.g., U.S. dollars, euros, Japanese yen)? There are several options: she can exchange her bitcoins directly with any person willing to buy them for traditional currency or she can exchange them through a virtual currency exchanger—e.g., Coinbase, the largest virtual currency exchanger in the United States. These exchangers function as a link between virtual currencies and traditional currencies since they can accept conventional checks, credit card, debit card, or wire transfer payments in exchange for virtual currency, exchange one virtual currency for another virtual currency, and exchange virtual currency for traditional currency. Through these exchangers, virtual currencies can now be used for purchases from over 100,000 merchants (e.g., Overstock.com, Home Depot, Dell, Amazon, Microsoft, and Expedia). Virtual currency exchangers also provide digital wallet services that help users quickly authorize virtual currency transactions; millions of users have taken advantage of these digital wallets provided by exchangers. For example, Coinbase, which started in 2012, maintains over 5 million wallets with wallet services available in 190 countries and over \$50 billion traded on its exchange.⁸ Its wallets can be readily accessed through a computer or mobile device like a smartphone.

While many champion cryptocurrency as a highly innovative medium for financial transactions, cryptocurrency’s opponents decry it as fraud. For instance, Warren Buffet, the “Oracle of Omaha” and CEO of Berkshire Hathaway, has stated emphatically that “[i]n terms of cryptocurrencies, generally, I can say with almost certainty that they will come to a bad ending.”⁹ Charlie Munger, vice-chairman of Berkshire Hathaway, has been even more pessimistic about the cryptocurrency craze, calling it “totally asinine” and a “noxious poison.”¹⁰ Jamie Dimon, the CEO of JPMorgan Chase, has described cryptocurrency mania as “worse than [the] tulip bulb [craze in the 17th century].... Someone is going to get killed. Currencies have legal support. It will blow up.”¹¹

Enforcement Concerns

For U.S. regulators and law enforcement officials, figuring out how to regulate and enforce laws in a virtual currency world that can operate anonymously, electronically, incredibly quickly, across borders, and without intermediaries or paper trails poses unique problems. These problems include using cryptocurrency to: 1) facilitate crimes ranging from narcotics trafficking and child pornography to money laundering, ransomware, and terrorist financing (Christine Lagarde, the head of the International Monetary Fund, has warned that cryptocurrencies can become a “major new vehicle for money laundering and the financing of terrorism”¹²); 2) promote tax evasion by hiding income; and 3) defraud individuals and companies through Ponzi schemes and similar market manipulations involved in initial coin offerings and cryptocurrency-based businesses.

In addition, outright theft is a serious concern. Since cryptocurrency acts like “cash on steroids” because it is not only anonymous but can be moved instantly to any digital wallet anywhere in the world, thieves have hacked into and stolen cryptocurrency from exchanges. For example, in January 2018, over \$500 million of a digital currency called NEM was stolen when thieves hacked into Coincheck, Inc., one of Japan’s biggest cryptocurrency exchanges.¹³ This followed the 2013-2014 theft of approximately 850,000 bitcoins worth at the time more than \$450 million from Mt. Gox, a Japanese bitcoin exchange handling over 70 percent of all bitcoin transactions worldwide in that

period.¹⁴ Large-scale theft continued in August 2016, when over 115,000 bitcoins worth about \$72 million were stolen from the exchange platform Bitfinex in Hong Kong.¹⁵ In addition, crooks have hacked people's digital wallets to steal their cryptocurrency,¹⁶ stolen powerful computers used to "mine" for virtual currencies,¹⁷ embezzled virtual currency from their employers,¹⁸ and forced individuals through threats and violence to physically hand over their private keys, unlocking all their virtual currency.¹⁹

September 2016, the IRS was criticized by the Treasury Inspector General for Tax Administration for doing very little to identify and address "taxpayer noncompliance issues for transactions involving virtual currencies."²²

In light of this criticism and facing an abysmal rate of virtual currency transaction self-reporting, how has the IRS decided to encourage increasing taxpayer compliance? The answers can be found in the playbook of how the IRS has confronted the problem

As one of the crypto-sheriffs, the IRS has treated cryptocurrencies as "property," a definition that may well work when the number of crypto-transactions are in the millions but not if they are in the hundreds of millions or billions.

In light of the enormity and diversity of the crimes that may be associated with cryptocurrency, U.S. regulatory agencies—the IRS, the SEC, the CFTC, and the FinCEN—have begun to try a number of approaches to enforce current laws and to modify such laws to adapt to this new technology.

Prior to 2014, the IRS had not weighed in on how cryptocurrencies should be treated for tax purposes. It had a choice: it could treat cryptocurrency as a traditional "currency" like a U.S. dollar or European euro that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange, or it could treat it as "property" similar to a stock or bond. If designated as "currency," cryptocurrencies' use in financial transactions would not have intrinsic gain or loss that could be taxed upon sale or exchange. If classified as "property," each time the cryptocurrency was sold or exchanged in any transaction, it would generate a taxable gain or loss depending on the taxpayer's cost to purchase the cryptocurrency, as adjusted (i.e., the taxpayer's adjusted tax basis). In IRS Notice 2014-21, the IRS chose the latter option, viz., treating any virtual currency that could be converted into traditional currencies as property.²⁰ The significance of this ruling cannot be understated. As property, every time a virtual currency is used to buy any goods, pay for any services, or exchanged for any other virtual or traditional currencies, the taxpayer has to determine: 1) its cost basis in the currency (typically, the fair market value (FMV) of the virtual currency at the time he or she obtained it), 2) any adjustments to cost basis after obtaining it, 3) the FMV of the property or service received at the time it is sold or exchanged, and 4) any resulting taxable gain or loss from that sale or exchange. For example, if one buys a pair of \$100 shoes on Amazon with virtual currency, one would have to figure out the cost basis of that virtual currency when it is obtained (e.g., \$50, assuming it was purchased for \$50), any adjustments after obtaining it (assuming none), the FMV of the shoes received for the virtual currency (\$100 in this case), and the amount of gain realized (\$50, the difference of \$100 of FMV received and \$50 adjusted cost basis). That \$50 gain would then have to be reported on one's tax return. There is no de minimis exception to this reporting requirement.

With millions of virtual currency transactions happening annually, the IRS expected a torrential rainstorm of reporting after 2014. Instead, less than a light drizzle of 1,000 taxpayers reported a virtual currency transaction in 2014 or 2015.²¹ In

of unreported offshore income. For years prior to 2008, Congress held numerous hearings complaining that there was \$100 billion of unreported U.S. taxpayers' income overseas. Recently, it was estimated that there was approximately \$25 billion of cryptocurrency-related taxes owed in 2017 with a tremendous amount of underreporting of such taxes in years prior.²³ As in the present situation, the IRS then lacked financial resources to hire thousands of agents to scour the planet to locate that concealed foreign income. Indeed, the resource issue has only worsened since 2010 as the IRS's enforcement budget has actually been cut by approximately 20 percent over the past eight years, reducing the number of agents, audits, and investigations substantially.²⁴ Lacking internal ability to locate these unreported accounts, the IRS turned to third parties—notably large Swiss banks like UBS—to provide that information. Working with the U.S. Department of Justice (DOJ), the IRS participated in having a John Doe summons served on UBS in 2008. A John Doe summons does not identify a particular U.S. taxpayer but a class of U.S. taxpayers that fall within a certain group of those who may have broken the tax laws. With the potential to be held in contempt for not producing records responsive to the summons and facing repercussions to its ability to bank in the United States, UBS eventually agreed to hand over to the DOJ information for over 4,000 Swiss accounts held by U.S. taxpayers as part of a deferred prosecution agreement that included a \$780 million penalty. Having driven a prosecutorial spike into the formerly impenetrable body of the "secret Swiss bank account," the DOJ subsequently entered into agreements with over 80 Swiss financial institutions to obtain an enormous amount of information concerning U.S. taxpayers' unreported overseas accounts.²⁵ Over the same time period, 2009 to the present, the DOJ has brought over 100 criminal prosecutions against U.S. taxpayers, their financial advisors, lawyers, and foreign bankers, as well as a number of foreign banks, obtaining felony convictions and billions of dollars in restitution and penalties.

While the DOJ has used the "stick" of criminal prosecutions to drive compliance, the IRS has offered taxpayers a "carrot" of voluntary disclosure to avoid such prosecutions. Starting in March 2009 and concluding on September 28, 2018, the IRS's Offshore Voluntary Disclosure Program (OVDP) traded criminal amnesty in exchange for taxpayers voluntarily coming forward with their unreported foreign accounts and assets, amending their returns and filing all disclosure forms for the prior eight years, cooperating

with the IRS in disclosing all aspects of their foreign accounts, and paying significant tax, interest, and penalties. To date, the OVDP and its streamlined versions have witnessed over 100,000 taxpayers complete the programs, and the IRS has received over \$10 billion in payments.²⁶ In addition, Congress passed legislation in 2010, the Foreign Account Tax Compliance Act (FATCA), that over the past years has resulted in hundreds of agreements with foreign financial institutions as well as a network of inter-governmental agreements with scores of countries to produce a tsunami of reporting of U.S. taxpayers' foreign bank accounts to the IRS.

This formula—issue a John Doe summons to an entity that has key information about unreported income and use the “carrot and stick” of criminal prosecutions and voluntary disclosure programs as well as targeted legislation to drive taxpayer compliance—is now beginning in the cryptocurrency world. In November 2016, the DOJ filed a lawsuit in Northern California asking the court to authorize the service of a John Doe summons to Coinbase, the largest cryptocurrency exchanger in the United States, seeking information on all of its millions of virtual currency account holders from 2013 to 2015.²⁷ A year later, in November 2017, the court narrowed the summons and ordered Coinbase to provide the IRS with certain records related to all Coinbase users who bought, sold, sent, or received more than \$20,000 worth of cryptocurrencies in a single year between 2013 and 2015.²⁸ Coinbase estimated that this more circumscribed summons affects 14,355 accounts holders involving 8.9 million transactions.

Then Principal Deputy Assistant Attorney General Caroline D. Ciralo, head of the DOJ's Tax Division, warned taxpayers about what was coming: “Tools like the John Doe summons authorized today send the clear message to U.S. taxpayers that whatever form of currency they use—bitcoin or traditional dollars and cents—we will work to ensure that they are fully reporting their income and paying their fair share of taxes.”²⁹ Treasury Secretary Steven Mnuchin later added: “If you have a wallet to own bitcoins, that company has the same obligation as a bank to know [you as a customer]. . . . We can track those activities. The rest of the world doesn't have that, so one of the things we will be working very closely with the G-20 is making sure that this doesn't become the Swiss bank account.”³⁰

If the IRS and DOJ follow their past game plan, they will take the information about virtual currency transactions received

from Coinbase, compare it with the taxpayers' disclosures on their tax returns, and start bringing waves of coordinated civil and criminal prosecutions across the country to try to achieve deterrence through the threat of significant taxes, penalties, and imprisonment. The IRS and DOJ will then seek to serve John Doe summonses on other virtual currency exchangers to obtain more information about taxpayers' malfeasance, seek to have Congress pass legislation concerning third-party reporting of virtual currency transactions, and then have the IRS implement a voluntary disclosure program for those with unreported virtual currency transactions. This potential Virtual Currency Voluntary Disclosure Program will offer the advantages of criminal non-prosecution and minimal penalties if taxpayers with such unreported transactions “come in from the cold,” file amended returns, pay taxes and interest owed, and provide the IRS with details of their virtual currency transactions. The IRS will then build a database of virtual currency transactions, like it did with offshore account information, and use computer analytics and artificial intelligence to determine which taxpayers to audit for noncompliance.

This game plan, premised on the IRS's designation of cryptocurrency as property, may work as long as the use of virtual currencies as a medium of exchange does not explode into the hundreds of millions or billions of transactions or start being used as a country's legal tender. However, as evidenced by statements made by authorities in Venezuela³¹ and the Marshall Islands³² that they will launch their own cryptocurrencies in 2018 and by the growing list of companies who are accepting virtual currencies as payment for goods and services, the IRS may need to consider at some point soon updating its 2014 guidance to deal with the realities of the emerging cryptocurrency world. For instance, rather than treat all virtual currency as property, the IRS should consider creating more defined categories that focus on the particular use of the cryptocurrency (e.g., medium of exchange, investment, utility token, etc.) to determine its taxability. Otherwise, the tidal wave of unreported virtual currency transactions will threaten to undermine the foundations of the American tax self-reporting system.

The Wild West was won when the rule of law—based on fairness, justice, due process, and consistent enforcement—replaced the rule of anarchy. With the explosion of the Wild West of cryptocurrency over the past several years, the crypto-sheriffs have been trying to adapt rules and regulations enacted for a different age to

apply to the unique aspects of virtual currency. As one of these crypto-sheriffs, the IRS has treated cryptocurrencies as “property,” a definition that may well work when the number of crypto-transactions are in the millions but not if they are in the hundreds of millions or billions. Thus, the IRS, like other crypto-law enforcers, will have to quickly adapt to the changing technology to stave off that technology overrunning Main Street and Wall Street. ■

¹ Eric Mack, *The Bitcoin Pizza Purchase That's Worth \$7 Million Today*, FORBES, Dec. 23, 2013, available at <https://www.forbes.com>; Aaron Hankin, *Bitcoin Pizza Day: Celebrating the \$20 Million Pizza Order*, Investopedia (May 22, 2017), <https://www.investopedia.com/news/bitcoin-pizza-day-celebrating-20-million-pizza-order>.

² Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf> (last viewed Sept. 25, 2018).

³ I.R.S. Notice 2014-21, available at https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21 [hereinafter I.R.S. Notice 2014-21].

⁴ Letter from Mary Jo White, S.E.C. Chair, to Hon. Thomas P. Carper, Chairman, U.S. Senate Comm. on Homeland Sec. and Governmental Affairs (Aug. 30, 2013), available at <http://online.wsj.com/public/resources/documents/VCCurrency111813.pdf>; Jay Clayton, S.E.C. Chair, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), available at <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>; Speech of William Hinman, Director, S.E.C. Div. of Corp. Fin., Digital Asset Transactions: When Howey Met Gary (Plastic) (June 14, 2018), available at <https://www.sec.gov/news/speech/speech-hinman-061418>.

⁵ See In re Coinflip, Inc., et al., CFTC No. 15-29, <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliporder09172015.pdf> (Sept. 17, 2015).

⁶ U.S. Dept. of Treasury Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013), available at <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

⁷ Certain types of virtual currencies—e.g., those on the Ethereum blockchain—can embed smart contracts or self-executing contracts onto their blockchain, requiring certain conditions be met before the financial transaction is complete. For a more detailed explanation on the potential use of these smart contracts, see Ameer Rosic, *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*, Blockgeeks, <https://blockgeeks.com/guides/smart-contracts/> (last viewed Sept. 25, 2018).

⁸ See About Coinbase, Coinbase, www.coinbase.com/about (last viewed Sept. 25, 2018).

⁹ Warren Buffett thinks cryptocurrencies will end badly, CNBC, Jan. 10, 2018, <https://www.msn.com/en-us/finance/markets/warren-buffett-thinks-cryptocurrencies-will-end-badly/vi-BBIdryM>.

¹⁰ Tim Bradshaw, *Berkshire's Charlie Munger calls bitcoin "totally asinine"*, FINANCIAL TIMES, Feb. 14, 2018, available at <https://www.ft.com>; Liz Moyer, *Berkshire's Charlie Munger Calls Bitcoin "Noxious Poison"*, CNBC, Feb. 14, 2018, <https://www.cnbc.com>.

¹¹ Thomas Heath, *Is Bitcoin Another Tulip Craze or a Legitimate Investment?* WASH. POST, Sept. 14, 2017, available at <https://www.washingtonpost.com>; Mari-

MCLE Test No. 282

The Los Angeles County Bar Association certifies that this activity has been approved for Minimum Continuing Legal Education credit by the State Bar of California in the amount of 1 hour. You may take tests from back issues online at <http://www.lacba.org/mcleselftests>.

1. Cryptocurrency is a digital representation of value that may function as a medium of exchange, a unit of account, and/or a store of value.
True.
False.
2. Cryptocurrencies require financial institutions to validate their transactions.
True.
False.
3. To validate a Bitcoin transaction, participants in the network called “miners” receive bitcoins for being the first to solve a mathematical puzzle related to the verification of this transaction.
True.
False.
4. The potential advantages to cryptocurrency transactions over financial transactions through banks include being faster, having smaller transaction fees, and the ability to be conducted anywhere in the world as long as the parties have access to the Internet.
True.
False.
5. Purchasers of cryptocurrencies can never exchange them into traditional “fiat” currencies like U.S. dollars or euros.
True.
False.
6. A “private key” to a digital wallet is a randomly generated string of alphanumeric characters that functions like a PIN for a bank account.
True.
False.
7. Virtual currencies cannot yet be used for purchases from retail merchants.
True.
False.
8. Warren Buffet, CEO of Berkshire Hathaway, is a major proponent of the use of cryptocurrencies.
True.
False.
9. Cryptocurrencies concern law enforcement officials since those who use them can operate:
A. Anonymously.
B. Electronically.
C. Very quickly across borders.
D. Without intermediaries or paper trails.
E. All of the above.
10. Cryptocurrency has been used to facilitate crimes ranging from narcotics trafficking to money laundering to terrorist financing.
True.
False.
11. Since cryptocurrencies are digitally based, they cannot be stolen from those who possess or store them.
True.
False.
12. The Internal Revenue Service treats cryptocurrencies transactions for income tax purposes as “property” transactions, subject to capital gains treatment.
True.
False.
13. If one uses cryptocurrency to buy a \$20 pizza at the local pizzeria, there is no possibility that that person will owe the IRS capital gains tax on that transaction.
True.
False.
14. There is a de minimis exception to reporting capital gains on a cryptocurrency transaction on a federal tax return.
True.
False.
15. Over 1 million taxpayers reported virtual currency transactions on their federal tax returns from 2014 through 2015.
True.
False.
16. A “John Doe” summons requires a company that receives it to turn over records for a class of U.S. taxpayers that falls within a certain defined group of those who may have broken the tax laws, e.g., those U.S. taxpayers who have not reported their virtual currency transactions.
True.
False.
17. The IRS was completely thwarted in its effort to get names and records of U.S. account holders from Coinbase, the largest cryptocurrency exchanger in the U.S., when it served Coinbase with a John Doe summons for such names and records.
True.
False.
18. The IRS and the Department of Justice have used the “carrot and stick” approach of voluntary disclosure programs and criminal prosecutions to incentivize taxpayers in the past (e.g., with offshore unreported bank accounts) to report such accounts or face the potential of criminal consequences.
True.
False.
19. The IRS has increased its enforcement staff by over 20 percent in the last eight years.
True.
False.
20. No country has launched its own cryptocurrency.
True.
False.

MCLE Answer Sheet #282



POLICING THE WILD WEST OF CRYPTOCURRENCY

Name _____

Law Firm/Organization _____

Address _____

City _____

State/Zip _____

E-mail _____

Phone _____

State Bar # _____

INSTRUCTIONS FOR OBTAINING MCLE CREDITS

1. Study the MCLE article in this issue.
2. Answer the test questions opposite by marking the appropriate boxes below. Each question has only one answer. Photocopies of this answer sheet may be submitted; however, this form should not be enlarged or reduced.
3. Mail the answer sheet and the \$25 testing fee (\$35 for non-LACBA members) to:

Los Angeles County Bar Association
Attn: Los Angeles Lawyer Test
P.O. Box 55020
Los Angeles, CA 90055
- Make checks payable to: Los Angeles County Bar Association.
4. Within six weeks, Los Angeles Lawyer will return your test with the correct answers, a rationale for the correct answers, and a certificate verifying the MCLE credit you earned through this self-study activity.
5. For future reference, please retain the MCLE test materials returned to you.

ANSWERS

Mark your answers to the test by checking the appropriate boxes below. Each question has only one answer.

1. True False
2. True False
3. True False
4. True False
5. True False
6. True False
7. True False
8. True False
9. A B C D E
10. True False
11. True False
12. True False
13. True False
14. True False
15. True False
16. True False
17. True False
18. True False
19. True False
20. True False

nova, Polina, *Term Sheet—Thursday, September 28*, FORTUNE, Sept. 28, 2018, available at <http://fortune.com/2017/09/28/term-sheet-thursday-september-28>. Query whether cryptocurrency naysayers will have to experience the fate of Robert Metcalfe, the inventor of the Ethernet, who in 1995 predicted that the Internet would soon go spectacularly supernova and in 1996 catastrophically collapse. Two years later, during the sixth International World Wide Web Conference in 1997, he literally ate his words by blending a copy of his prior statement with some water and then consuming the resultant smoothie with a spoon.

¹² Christine Lagarde, *Addressing the Dark Side of the Crypto World*, IMF Blog (March 13, 2018), <https://blogs.imf.org>.

¹³ Olga Kharif, *Record Crypto Heist Raises the Appeal of a New Type of Exchange*, BLOOMBERG, Jan. 29, 2018, available at <https://www.bloomberg.com/news/articles/2018-01-30/record-crypto-heist-raises-the-appeal-of-a-new-type-of-exchange>.

¹⁴ Paul Vigna, *5 Things about Mt. Gox's Crisis*, WALL ST. J., Feb. 25, 2014, available at <https://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis>.

¹⁵ Clare Baldwin, *Bitcoin Worth \$72 Million Stolen from Bitfinex Exchange in Hong Kong*, Reuters (Aug. 2, 2016), <https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP>.

¹⁶ Jen Wiczner, *Hacking Coinbase: The Great Bitcoin Bank Robbery*, FORTUNE, Aug. 22, 2017, available at <http://fortune.com/2017/08/22/bitcoin-coinbase-hack>.

¹⁷ *Bitcoin Heist: 600 Powerful Computers Stolen in Iceland*, Associated Press (March 2, 2018), <https://www.nbcnews.com/news/world/bitcoin-heist-600-powerful-computers-stolen-iceland-n852811>.

¹⁸ Jonathan Stempel, *U.S. Charges Chicago Trader with Stealing Bitcoin*, Yahoo! News (Feb. 15, 2018),

<https://www.yahoo.com/news/u-charges-chicago-trader-stealing-bitcoin-232117784-sector.html>.

¹⁹ Edoardo Maggio, *Criminals Are Reportedly Abducting the "Cryptorich" to Steal their Bitcoin*, Business Insider (Feb. 19, 2018), <https://www.businessinsider.com/criminals-are-reportedly-abducting-the-cryptorich-to-steal-their-bitcoin-2018-2>.

²⁰ I.R.S. Notice 2014-21, *supra* note 3.

²¹ United States v. Coinbase, Inc., et al., Case No. 17-cv-01431-JSC (Order re Petition to Enforce IRS Summons) (Nov. 28, 2017), available at <https://cases.justia.com/federal/districtcourts/california/candce/3:2017cv01431/308850/78/0.pdf?ts=1512035973>.

²² Treasury Inspector General for Tax Administration, *As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions Are Needed to Ensure Taxpayer Compliance*, Reference No. 2016-30-083 (Sept. 21, 2016), available at <https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf>.

²³ Daniel Roberts, *Americans May Owe \$25 Billion in Crypto Taxes—But How Much Will They Report?*, Yahoo! Finance (April 11, 2018), <https://finance.yahoo.com/news/americans-may-owe-25-billion-crypto-taxes-much-will-report-123754863.html>.

²⁴ Skylar Dubelko, *Fewer Tax Cases Being Prosecuted*, 131 (60) DAILY J., Mar. 28, 2018; Chuck Marr & Cecile Murray, *IRS Funding Cuts Compromise Taxpayer Service and Weaken Enforcement*, Ctr. on Budget and Policy Priorities (April 4, 2016), <https://www.cbpp.org/research/federal-tax/irs-funding-cuts-compromise-taxpayer-service-and-weaken-enforcement>.

²⁵ U.S. Dep't of Justice, *Swiss Bank Program*, <https://www.justice.gov/tax/swiss-bank-program> (last viewed on Sept. 13, 2018).

²⁶ Press Release, I.R.S., *Offshore Voluntary Compliance Efforts Top \$10 Billion; More Than 100,000*

Taxpayers Come Back Into Compliance, IR-2016-137 (Oct. 21, 2016), available at <https://www.irs.gov/newsroom/offshore-voluntary-compliance-efforts-top-10-billion-more-than-100000-taxpayers-come-back-into-compliance>.

²⁷ United States v. Coinbase, Inc. et al., No. 17-cv-01431-JSC (N.D. Cal. Nov. 2016).

²⁸ *Id.*, Order re Petition to Enforce IRS Summons (Nov. 28, 2017).

²⁹ Press Release, U.S. Dep't of Justice, *Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency* (Nov. 30, 2016), available at <https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used>.

³⁰ Saleha Mohsin, *Mnuchin Warns Against Bitcoin Becoming the Next "Swiss Bank Account"*, BLOOMBERG, Jan. 12, 2018, available at <https://www.bloomberg.com/news/articles/2018-01-12/mnuchin-warns-against-bitcoin-becoming-next-swiss-bank-account>.

³¹ Venezuela launched the "petro" or "petromonda" in February 2018, which it claims to be backed by the country's oil and mineral reserves to supplement its plummeting bolivar fuerte currency. On March 19, 2018, the United States issued an executive order prohibiting all transactions, financing, and dealings by a U.S. person or within the United States in the Venezuelan digital currency. See Yaya Fanusie & Michaela Frai, *Crypto Investors Should Stay Away from Venezuela's Petro*, Coindesk (March 26, 2018), <https://www.coindesk.com/crypto-investors-stay-away-venezuelas-petro>.

³² Gertrude Chavez-Dreyfuss, *Marshall Islands to Issue Own Sovereign Cryptocurrency*, Reuters (Feb. 28, 2018), <https://www.reuters.com/article/us-crypto-currencies-marshall-islands/marshall-islands-to-issue-own-sovereign-cryptocurrency-idUSKCN1GC2UD>.

NORIEGA CHIROPRACTIC CLINICS, INC.

JESS T. NORIEGA, D.C.

Is proud to announce the opening of our Lynwood location

SERVICING: SOUTHGATE • BELLFLOWER • CUDAHY • NORTH LONG BEACH • WATTS

LYNWOOD HEALTH CENTER

11123 LONG BEACH BLVD.
LYNWOOD, CA 90262
(310) 726-8818

ONTARIO HEALTH SERVICES
602B N. Euclid Ave.
Ontario, CA 91764
(909) 395-5598

HUNTINGTON PARK HEALTH CENTER
3033 E. Florence Ave.
Huntington Park, CA 90255
(323) 582-8401

WHITTIER HEALTH SERVICES
13019 Bailey Ave. Suite F
Whittier, CA 90601
(562) 698-2411

MONTEBELLO HEALTH CENTER
604 North Monetteblllo Blvd.
Montebello, CA 90640
(323) 726-8818

SOUTH CENTRAL HEALTH CENTER
4721 S. Broadway Blvd.
Los Angeles, CA 90037
(323) 234-3100

HIGHLAND PARK HEALTH CENTER
5421 N. Figueroa St.
Highland Park, CA 90042
(323) 478-9771

1•800•NORIEGA

Personal Injury cases accepted on lien basis.

1•800•667•4342