

Accounting Faculty Research and Publications/College of Business Administration

This paper is NOT THE PUBLISHED VERSION; but the author’s final, peer-reviewed manuscript. The published version may be accessed by following the link in the citation below.

Tax Notes, (January, 2018). [DOI](#). This article is © [Tax Notes] and permission has been granted for this version to appear in [e-Publications@Marquette](#). [Tax Notes] does not grant permission for this article to be further copied/distributed or hosted elsewhere without the express permission from [Tax Notes].

Contents

- Abstract2
- Background.....3
- Companies Accepting Bitcoins4
- Currency or Property?4
- U.S. Tax Treatment5
- Issues With Cryptocurrencies.....5
- Blockchain and Network Forks6
- Stolen Funds7
- Problems With Digital Currencies.....8
- Unregulated Markets8
- Accounting for Bitcoins9
- Clone Coins — Bitcoin Cash.....9
- Volume, Volatility, and Value 10
- Liquidity 10
- Conclusion 10
- References 11

Cryptocurrencies Are Taxable and Not Free from Fraud

Joseph Wall

Department of Accounting, Marquette University, Milwaukee, WI

D. Larry Crumbley

Department of Accounting, Louisiana State University, Baton Rouge, LA

Lewis B. Kilbourne

Department of Finance, Louisiana State University, Baton Rouge, LA

Caleb Blair

Student, Texas A&M University, College Station, TX

Abstract

In this report, the authors discuss cryptocurrencies — especially bitcoin — and argue that because the IRS lists them as property, they are taxable, and because they are not as anonymous as once thought, they are not free from fraud.

Cryptocurrencies are digital assets used as a medium of exchange, but they are not really coins. They can be sent electronically from one entity to another almost anywhere in the world with an internet connection. There are many cryptocurrencies in the market, including bitcoin, ethereum, ethereum classic, litecoin, nem, dash, iota, bitshares, monero, neo, and ripple. Many of the cryptocurrency networks are not controlled by a single entity or company; instead, a decentralized network of computers keeps track of the currency using a token ID. A ledger maintains a continuously growing list of date stamped transactions in real time called “blocks.” This technology is known as blockchain, which records, verifies, and stores transactions without a trusted central authority. The network instead relies on [decentralized autonomous organizations](#) (DAOs) with uncertain legal standing.

Background

Using bitcoin as an example, some wallet IDs allow buyers and sellers to remain anonymous when carrying out transactions from bitcoins to bitcoins (but not from U.S. dollars to bitcoins). With no central authority, no one can force new users to reveal their identities. On November 17, 2016, the Justice Department, on behalf of the IRS, filed a John Doe summons demanding that Coinbase, an exchange for digital currency, reveal the identities and full transaction records of customers registered between January 2013 and December 2015.¹ After the government narrowed the scope of the summons, Coinbase indicated that the requested information included more than 8.9 million transactions and 14,355 account holders.² Despite the issuance of [Notice 2014-21](#), 2014-16 IRB 938, which treats digital currency as property for tax purposes, only 802 people informed the IRS about

their Coinbase profits. As a result, the IRS has begun to reverse-engineer the blockchain transactions to identify associated wallets and owners.

The uncertain status of cryptocurrency has led to enormous volatility in the cryptocurrency marketplaces. For example, on June 21, 2017, the price of ethereum plummeted to \$3.74 from a high of \$365 earlier that day.³ As of December 20, 2017, ethereum was trading at \$831.49 according to Coinbase. That volatility makes risk assessment troublesome for an investor or user.

Since then, cryptocurrency prices have again skyrocketed, with bitcoin trading at more than \$18,000 per coin in mid-December 2017, even after JP Morgan CEO Jamie Dimon referred to bitcoin as a “fraud.”⁴ A previous massive drop of nearly 30 percent was triggered by China’s near-total ban on bitcoin trading. Thus, the combination of information asymmetry, actions by world governments, and media coverage tends to result in extreme volatility in the marketplace.

Most cryptocurrencies have built-in supply-limiting features. For example, the bitcoin supply is mathematically limited to approximately 21 million bitcoins.⁵

There are more than 110 cryptocurrency exchanges, with Japan dominating the market,⁶ and it is estimated that there are more than 3 million active cryptocurrency users.⁷ To expand accessibility, several parties have filed requests with the SEC to create exchange-traded funds to track cryptocurrencies. A cryptocurrency futures market became available in mid-December 2017.

Miners use special computers with application-specific integrated circuits to “mine” bitcoins by solving mathematical puzzles using raw computational power and clever algorithms. The winners receive newly created bitcoin rewards and thus increase their so-called hash rate.

The calculation process requires a huge amount of electricity, especially for cooling the computers. Miners in China and Iceland have performed much of the mining because of cheaply available power in those countries. However, with China’s recent ban on initial coin offerings (ICOs), other miners will have to step up. Unless someone commands a tremendous hash rate by themselves, the odds of successfully solo mining and solving a block are extremely low. Thus, miners band together in pools to increase the hash rate.⁸

Each currency has its own supply provision. Ethereum is tied to the creation of “smart contracts” (a counterparty protocol on top of the blockchain), litecoin strives for more universal usage⁹ (and thus a large total supply that can increase), and bitcoin limits its supply based on a mathematical formula.¹⁰ Because many new cryptocurrencies have emulated bitcoin to some degree, they also may find themselves quickly approaching the mathematical limit on supply. Now many, including bitcoin, are copying ethereum’s smart contract feature.

For bitcoin, as the amount that can be mined approaches the 21 million limit, rewards to miners decrease. The number of rewards is reduced by a process of halving, which occurs every four years (or every 210,000 blocks) until the 21 million limit is reached. The next halving occurs in 2020, dropping rewards from 12.5 to 6.25 coins. As of mid-December 2017, 16.8 million bitcoins (or 80 percent of 21 million) had been mined.

Companies Accepting Bitcoins

BitPay is one of the largest bitcoin exchanges. It provides services to 30,000 merchants globally and processes \$1 million in bitcoin transactions daily. Internet retailer Overstock has signed on with Coinbase, which also boasts approximately 30,000 business customers and has shifted to an on-chain transaction fee for its users.¹¹

There is a long list of companies accepting bitcoins, such as Dell, Expedia, Microsoft, Overstock, PayPal, Subway, Target, and Zappos. Overstock CEO Patrick Byrne confirmed August 10, 2017, that he planned to launch an “SEC compliant” ICO by Thanksgiving called tZero.

In practice, the large companies have a bitcoin processing partner (for example, Coinbase or BitPay). The bitcoin partners make money on the transaction fee (around 1 percent) and the companies ask for the bitcoins to be instantly converted to cash. For example, Overstock keeps at least 90 percent of its bitcoin transaction revenue in U.S. dollars. One reason companies favor dollars is that they conduct their accounting and finance operations in dollars.¹²

Currency or Property?

The Bank Secrecy Act (BSA) requires financial institutions to collect and maintain information about their customers and share that information with the Financial Crimes Enforcement Network. However, questions arise when these requirements are applied to cryptocurrencies. When do business dealings with cryptocurrencies fall within the definition of a financial institution? Are BSA obligations triggered when the developer of a new cryptocurrency (or token) sells it to a U.S. person?¹³ Do those sales fit into the definition of money transmission under federal surveillance regulations? How can sales to U.S. citizens avoid BSA rules? FinCEN has said that selling your own bitcoins from your account is not a money transmission.¹⁴

In a settlement agreement with ripple in 2015, however, FinCEN said that selling a token you own is a money transmission. Thus, to do so without registering with FinCEN is a serious offense.¹⁵ Notice 2014-21 treats payments using cryptocurrency as income, like any other in-kind payment. In *Shavers*,¹⁶ a district court treated bitcoins as a currency or form of money. The FBI had seized about \$80 million of bitcoins from Trenton Shavers. Using the three-part *Howey* test,¹⁷ the trial judge found that the bitcoins were investment contracts under the securities regulations regarding Ponzi schemes.

U.S. Tax Treatment

Virtual currency is treated as property for tax purposes and it does not have legal tender status. Thus, wages using virtual currency are taxable to the employee, must be reported by an employer on a Form W-2, and are subject to federal income tax withholding and payroll taxes. Payments using virtual currency made to independent contractors and other service providers are taxable, and self-employment tax rules generally apply. Normally, payers must issue a Form 1099.

Most of the time, bitcoin and other cryptocurrencies are pegged to the U.S. dollar, and they are expressed as a base currency for conversion in dollars. A bitcoin is expressed in the denomination of satoshis, and each bitcoin has 100 million satoshis.

The character of gain or loss from the sale or exchange of virtual currency depends on whether the virtual currency is a capital asset in the hands of the taxpayer. Because the IRS views cryptocurrency holdings as property, income is measured at the fair market value at the time of receipt, and a capital gain or loss may ensue when the currency is later sold or exchanged. A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property.

Issues with Cryptocurrencies

The fact that a taxpayer must determine a gain or loss on each transaction can be a real problem for cryptocurrencies in the United States. Imagine the difficulty of taxpayers keeping track of every gain or loss on each transaction if they use digital money the same way they use cash, credit cards, or checks. Soon virtual currency would be used only for large purchases or sales.¹⁸ Or cryptocurrencies might move to the dark web or the underground economy for dollar-to-bitcoin transactions. So it is still premature to declare that fiat currency is dead and that the days of coin and paper money are over.

Governments may try to outlaw cryptocurrencies. Some countries have restricted cryptocurrencies or not officially permitted them. But countries such as Japan and Australia have embraced cryptocurrencies and officially recognized them as legitimate forms of payment. The actions of India and China — together home to more than 37 percent of the world's population — will likely have significant, long-term effects on the legitimacy and universal acceptance of these transactions and markets. China is reaching out to play a major role in regulating DAOs through licensing.¹⁹

In March 2013 FinCEN issued guidance clarifying which participants in virtual currency systems are subject to anti-money-laundering requirements, and it required virtual currency exchanges to register with FinCEN. In July 2013 the SEC charged an individual and his company with defrauding investors through a bitcoin-based investment scheme. In October 2013 multiple agencies worked together to shut down Silk Road, an online marketplace through which users paid for illegal goods and services with bitcoins. But that action created a hydra — at least 50 illegal markets similar to Silk Road sprung up in its place.

Then there is the long list of issues raised by IMF staff. Their January 2016 compilation, “Virtual Currencies and Beyond: Initial Considerations,” provides foresight on policy as the IMF considers its role in digital currency.

Russia is contemplating the adoption of cryptocurrency rules. In a *Financial Times* interview, Vladimir Putin noted that the use of cryptocurrency poses serious risks, such as “opportunities to launder criminally obtained money, evade taxes, and even finance terrorism, as well as, of course, perpetuating fraudulent schemes that obviously may affect ordinary citizens.” He continued: “But we need to use the advantages that come with any technological solutions in banking. It is important not to set up superfluous barriers, naturally, but to create the essential conditions for the further development and perfection of the national financial system.”²⁰

Putin's comments may reflect a consensus of many users, which might have an influential role in scaling the efficiency and effectiveness of the cryptocurrency system. Even China signaled a conditional acceptance after shutting down exchanges and halting its involvement in licensing bitcoin exchanges.²¹

Blockchain and Network Forks

Blockchain technology is the recordkeeping system underlying most cryptocurrency transactions. It appears to be strong and relatively secure. Through this process, blocks, or transactions sent over the network, are encrypted and connected to previous transaction blocks with exact time and sales transaction data embedded within them. As this sequence of transactions continues over time, a chain is formed. The transactions run through a worldwide peer-to-peer network, ensuring multiple points of redundancy. Once the information in the block becomes part of the chain, the information cannot be changed without a majority consensus within the network. In that situation, all subsequent blocks are altered to account for the point of change of origination.

When the community, through majority consensus, wants to change the underlying code, or when two more different versions of a ledger split from the original single ledger, a chain splits in two, causing a fork in the record of transactions. When a software update is not required by all users to maintain the integrity of the chain, this process is known as a soft fork. A hard fork results when a major change to the software is proposed and accepted by the majority of the community, causing the old and new versions of the code to be incompatible. All users must quickly update their software to the new version to continue to access the ledger.

For example, on June 17, 2016, a hacker exploited a code loophole that allowed one-third of the funds associated with ethereum to be siphoned away.²² A hard fork was decided on, primarily to reimburse losses and reset ownership. However, a major battle ensued and there was a split in the community. Many believed a hard fork would compromise the integrity of the system, and they retained the original blockchain — what is now known as ethereum classic. However, the major players in the market went with the hard fork, and the split gave rise to ethereum.²³ Thus, hard forks can disrupt a community and create an entirely new path for the blockchain to follow.

Stolen Funds

Unfortunately, despite the strength of the technology underlying the blockchain recording process, the security processes have not been nearly as strong. Although the cryptocurrency community has been quick to point fingers at infrastructure problems and user errors, as well as insecurity by users, companies, and exchanges, there is still no system that cannot be hacked.²⁴ It is thus unsurprising that the scale and scope of crypto theft is on the rise.

At the most basic level of crypto theft, personal computers may unwittingly be used to mine crypto coins for someone else. Cybersecurity provider Kaspersky Labs estimates that nearly two million of the computers it monitors had such software running in the background.²⁵ Similarly, security experts note that millions of computers are likely infected with code waiting to be activated. Once a bitcoin address is detected, the software comes alive and reports home, allowing the hacker to steal the private key when generated or used. Hackers can even use simple redirection techniques. For example, in July 2017 Coindash was hacked and the address to send ethereum was changed for three minutes. Within

those three minutes, hackers made off with more than \$7 million.²⁶ Perhaps even more troubling is the increasing pace of theft. More than \$4 billion is estimated to have been stolen thus far, with few recoveries noted.²⁷

Hundreds of millions of dollars have been stolen from individuals. In ethereum alone, more than 30,000 people have been affected, with an average loss exceeding \$7,500 per occurrence.²⁸ There have also been several notable, larger-scale seizures and heists in the brief history of cryptocurrency. When the Silk Road was breached, the FBI recovered 144,000 bitcoins valued at approximately \$30 million.²⁹ Similarly, the Sheep Marketplace (established as a hidden service) was closed upon announcing the theft of \$6 million of users' bitcoins. However, further examination revealed that the true theft — by the principals in the exchange — may have been as high as \$100 million.³⁰

One of the most famous scams involved Mt. Gox. Launched in July 2010, Mt. Gox became the largest cryptocurrency exchange in the world, handling more than 70 percent of all transactions by 2013.³¹ However, because of a lack of proper business practices, internal controls, and security, hackers were able to access the exchange's "hot wallets." This resulted in the loss or theft of 850,000 bitcoins (valued at \$460 million in 2014). The second-largest breach of an exchange came in August 2016, when Bitfinex announced the theft of nearly 120,000 units of cryptocurrency. The multi-signature wallets of individual users were emptied of approximately \$72 million.³²

As noted earlier, ethereum has functional computer programs — smart contracts — within the blockchain to store value. An investor-directed venture capital fund, a DAO, was created to organize for-profit and nonprofit enterprises in relation to ethereum. However, a vulnerability in the DAO code allowed any of its users to steal ethereum. And in June 2016 that flaw resulted in the loss of more than \$50 million — losses enabled by a hard fork in the ethereum blockchain.³³ Further, in July 2017 a popular multi-signature wallet was breached, and more than 150,000 ethereum tokens were stolen as the result of a bug in the code that allowed anyone to access a wallet and send all funds to an account of their choosing. More than \$30 million was lost.³⁴

Unfortunately, complete security is unobtainable. Most people who use cryptocurrency are aware that anyone who discovers their private key can steal their funds. Thus, although exchanges or wallets that can store those keys in the cloud are convenient, their massive vaults make increasingly attractive targets for hackers. Once breached, users' coins are lost. Because of that, many people believe storing their private keys on their own hard drives is a good idea. Others use a paper wallet, generating keys using a QR code, printing the QR code, and deleting all traces of the key from the computer. Typically, they then cut the code into pieces, storing each piece in a different secured location.³⁵ However, any one of those locations may experience theft, water damage, or fire. Also, preexisting malware may activate when keys are generated, enabling hackers to steal the cryptocurrency.

New multistep keys are being tried on different devices to address this problem. However, as reflected in the case of Jared Kenna, discussed below, hackers have already demonstrated their resolve and ability to break even multifactor identification. The only truly secure method may be to generate a key on a computer that has never been connected to the internet.

Problems with Digital Currencies

Obviously, digital currencies can be lost, stolen, or hacked. Jared Kenna, a British IT worker, threw a hard drive containing 7,500 bitcoins into the trash. He had mined the virtual currency four years earlier, when the bitcoin business was in the domain of technology geeks. At current prices, that loss has a value of approximately \$30 million. Kenna then lost 800 bitcoins when he reformatted his hard drive, erasing his associated records of the coins. He also lost millions of dollars in bitcoins when a hacker convinced Kenna's cellphone provider that he was Kenna. The hacker was thus able to steal 30 accounts associated with two-factor authentication and raid Kenna's bank accounts and wallets.³⁶ (In the United States, those types of losses could be capital losses or casualty losses, depending on the circumstances.) There are several devices that can be purchased to protect digital currencies, but hardware wallets should be kept in a safe deposit box.

Unregulated Markets

In general, cryptocurrency is still decentralized and nearly unregulated. As a result, volatility is common, with multiple currency assets having experienced declines of more than 80 percent at some point in their history. Because the currency assets lack the backing of physical assets and the full faith and credit of a central authority, their long-term value is questionable. Will the work performed to create the currency still have value a year later? Ten years later? A hundred years later?

Further, countries differ on the extent of asset recognition for cryptocurrency, so there is often uncertainty about the legality of holdings and how taxation works. As of October 2017, for example, China and South Korea banned all ICOs, with the Chinese government rumored to have been responsible for the closing of all associated exchanges. Similarly, Bangladesh, Bolivia, Ecuador, and Kyrgyzstan have explicitly made cryptocurrencies illegal. On the flip side, Australia and Japan have officially recognized cryptocurrency as legal tender. Note, however, that many of the world's top economic powers, such as Russia, have central banks that are in the development phase of cryptocurrency creation. China appears to be the first to market, with live testing daily.³⁷

Accounting for Bitcoins

There are ownership controls for each coin within the blockchain. For example, the so-called segregated witness (SegWit) protocol addresses a potential malleability bug involving the second part of a bitcoin transaction. The "witness" proves that the owner really wanted to spend the bitcoin. Under some circumstances, crypto signatures can be slightly changed without invalidating the signature. The appearance of the signature and the transaction identifier can be altered, making it harder to build second-layer protocols on top of bitcoins. This bug, which muddies the ledger, led to the closure of Mt. Gox. However, a SegWit protocol, responsible for segregating the witness data and speeding up transactions, has been activated for bitcoin, litecoin, groesticoin, and digibyte exchanges as of August 2017.³⁸ Widespread adoption is expected to take up to a year.

Marty Zigman, a CPA and cryptocurrency expert, suggests three accounting methods that coincide with bitcoin's adoption phases.³⁹ Initially, he says, treat bitcoin as a payment method. That is, define a new payment method in the accounting software, relate it to the bank account that the fund will settle, and then follow the procedures that the bitcoin providers (for example, BitPay or Coinbase) prescribe for accepting bitcoins in the business. When the volatility stabilizes and bitcoins become more widely

accepted, treat them as foreign currency, says Zigman. The third phase he envisions is the (albeit far-off) final adoption wave, in which businesses deem bitcoin the base currency and treat all other currencies as foreign.

Zigman promotes [BTC4ERP](#), a bitcoin transaction coordinator, as a way for companies that run NetSuite to integrate bitcoin with their general ledgers, allowing them to “configure their accounting practices based on the way they see bitcoin used in their business.”⁴⁰

Clone Coins — Bitcoin Cash

Clone coins may be a natural byproduct of the growing cryptocurrency system. Copycat behavior with the name “bitcoin” may end up in the trash can. Or, with the adoption of technology, strong players in the DAOs may make copycat behavior illegal through self-regulation (such as the SegWit protocol). One has to wonder when network exchange owners will require external regulation, much like the self-regulated securities market did with the 1933 and 1934 securities exchange legislation.

As the marketplace finds openings for the entry of clone coins, the barriers are being tested by copying both the code and the blockchain, as was done with bitcoin cash. Several exchanges refused to participate in this scheme to drive up value by limiting the supply of service or exchange providers and thus affect the ability to clear transactions.⁴¹ The bubble is this manipulation.

Volume, Volatility, and Value

The continuing growth in the volume of transactions, users, trading partners, and exchanges creates pressure within the supply of cryptocurrencies to winnow out coins or tokens that are less functional. The idea of the blockchain ledger system will likely be increasingly attractive to the “continuous flow” users, since it allows them to promptly record the time and date of all transactions. Hence, demand will expand for those systems. IBM and Oracle are stepping into the cryptocurrency market with competing blockchain clouds to dampen the volatility and integrate the value into the commercial supply chain.⁴² The exchanges will likely be absorbed as a functional part of the blockchain clouds and potentially satisfy the need for continued validation.

If Goldman Sachs, other major commodity trading bankers, or any of the big server companies enter the cryptocurrency market, they would offer structure to the participants and be able to efficiently handle the exchange between trading partners.⁴³ Those organizations have the size and scale of operations to handle the volume and thus create value. And liquidity would not be a barrier.

Liquidity

Liquidity — the amount of a particular cryptocurrency flowing through the market at any given time — is a key contributor to volatility. For example, the daily quote chart above shows the volatility of bitcoin, ethereum, ripple, and litecoin, among the top 10 currencies. Risk assessment is based on the chart trends.⁴⁴

		Some Information About Cryptocurrencies		
Crypto-Currency	Price	Supply	Trade Volume	Market Capitalization
BitConnect (BCC)	\$200.24 USD	7,250,876 BCC	\$12,617,000 USD	\$1,451,944,411 USD
Dash (DASH)	\$294.00 USD	7,640,957 DASH	\$67,199,200 USD	\$ 2,246,433,649 USD
Monero (XMR)	\$89.36 USD	15,261,882 XMR	\$43,272,100 USD	\$1,363,739,213 USD
Bitcoin (BTC)	\$5,706.05 USD	16,644,025 BTC	\$2,880,170,000 USD	\$94,971,638,851 USD
BitcoinCash (BCH)	\$330.91 USD	16,710,863 BCH	\$278,516,000 USD	\$5,529,741,377 USD
NEO (NEO)	\$30.67 USD	50,000,000 NEO	\$76,911,600 USD	\$1,533,460,000 USD
Litecoin (LTC)	\$57.67 USD	53,519,807 LTC	\$212,541,000 USD	\$3,086,551,515 USD
Ripple (XRP)	\$0.21 USD		\$230,105,000 USD	\$8,227,755,101 USD
Ethereum (ETH)	\$305.27 USD	8,999,999,999 XEM	95,298,755 ETH	\$735,027,000 USD
NEM (XEM)	\$0.21 USD	38,531,538,922	\$5,955,790 USD	\$1,903,923,000 USD

Most marketplaces are assumed to be the best source for pricing an asset. However, with the number of cryptocurrencies and exchanges and the limited liquidity of cryptocurrency, it is difficult to assess from charts alone the risk for volatility resulting from the supply of and demand for prices through miners and their respective exchanges.

The price of bitcoin is very volatile anyhow, and limited liquidity contributes to that volatility. By definition, the cryptocurrency exchange is a supply and demand function, not a value function. Control of that flow is limited and inefficient. Through DAOs and network collaboration, consensus for any change is democratic, which leaves a gap between supporters and dissenters and necessitates a fork.⁴⁵

And, as one technology writer observed, because the trade volumes with bitcoin are relatively small, “single events can make a bigger difference.”⁴⁶

Conclusion

Corporations like IBM and Oracle might present an opportunity for some form of standardization and accounting to know when there is a deviation from the standard in the cryptocurrency market (for example, intentional or negligent acts by a stray miner or exchange participant). Government intervention could provide stability and rules, but that could dissipate rulemaking as a democratic exercise of the DAOs. Comparison with the currency commodity market would require miniscule trade comparisons, even if there is a strong “real” appreciation in the value and use of cryptocurrencies.

Many questions remain. Will the bubble burst on today’s prices? If it does, will we see it coming and understand why it burst? In that case, who would be liable? How do you sue a DAO?⁴⁷ Although it might be more expensive to sue IBM, that might be easier than suing a DAO. There will certainly be a need for many lawyers and expert witnesses.

Troubled waters are still ahead. Controlling the flow, the standards, the integrity of the participants, and the ability to redress grievances in this “democracy” are all of keen interest to those who wish to trade for profit in the cryptocurrency marketplace. Who will come out ahead?

References

- ¹ Stephen Palley, “[How to Sue a DAO](#)” (Mar. 14, 2016).
- ² *United States v. Coinbase Inc.*, [No. 3:17-cv-01431](#) (N.D. Cal. 2017). Some parties have presented amicus briefs opposing the subpoenas as overbroad.
- ³ Arjun Kharpal, “[Ethereum Briefly Crashed From \\$319 to 10 Cents in Seconds on One Exchange After ‘Multimillion Dollar’ Trade](#),” CNBC (June 23, 2017).
- ⁴ See Frank Chapparo, “[JPMorgan Might Be Getting Into Bitcoin Even Though Jamie Dimon Hates It](#),” *Business Insider*, Nov. 21, 2017.
- ⁵ Gwyn D’Mello, “[Bitcoins and Blockchains: Everything You Need to Know About This Crypto Currency and How It Works](#),” *India Times*, Aug. 7, 2017.
- ⁶ Brad Jones, “[The U.S. Is No Longer the World’s Largest Bitcoin Market](#),” *Futurism*, Sept. 18, 2017.
- ⁷ Gautham, “[Three Million Active Cryptocurrency Users Says Cambridge Center for Alternative Finance](#),” *newsBTC*, May 7, 2017.
- ⁸ Melvin Draupnir, “[Will 2017 Be Profitable for Bitcoin Mining?](#)” *bitcoinmining.com*, Feb. 6, 2017.
- ⁹ Amy Castor, “[SegWit Activation Complete, Litecoin Charts a Course for the Future](#),” *Coindesk*, May 19, 2017.
- ¹⁰ Mathematically, the original reward for task completion was 50 bitcoins for completion of a block. The block rewards are based on a four-year cycle of six blocks/hour x 24 hours/day x 365 days/year x four years/cycle = 210,240 blocks available. However, the reward is halved every four years so that the sums of all block reward sizes = 100 (50 + 25 + 12.5 + 6.125 + etc.). If all bitcoins are awarded, this process allows for a market maximum of 210,240 x 100 = 21,024,000 coins. Because of fractional rounding, however, the theoretical maximum is just under 21 million.
- ¹¹ Gilly Wright, “Is Bitcoin Good for Business?” *Global Finance*, June 2014, at 16-19.
- ¹² Jacob Davidson, “[No, Big Companies Aren’t Really Accepting Bitcoins](#),” *Money*, Jan. 9, 2015.
- ¹³ Peter Van Valkenburgh, “[Securities Laws Aren’t the Only Rules Tokens Sales Have to Consider](#),” *Coindesk*, May 20, 2017.
- ¹⁴ See FinCEN, “Guidance on the Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” FIN-2013-G001 (Mar. 18, 2013).
- ¹⁵ *Id.*
- ¹⁶ *SEC v. Shavers*, No. 4:13-cv-416 (E.D. Tex. 2014).
- ¹⁷ See *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
- ¹⁸ Jason M. Tyra, “[What If I Don’t Report My Bitcoin Income?](#)” *Bitcoin Magazine*, Feb. 3, 2014.
- ¹⁹ Josiah Wilmoth, “[China Hints at Licensed Bitcoin Exchanges With ‘Zero Tolerance’ on Cryptocurrency Crime](#),” *cryptocoins news*, Apr. 10, 2017.
- ²⁰ Catherine Zemsikova, “[Russian President Vladimir Putin Backs Cryptocurrency Rules and Warns of ‘Serious Risks’](#),” *Coinspeaker*, Oct. 11, 2017.
- ²¹ See Wilmoth, *supra* note 19.
- ²² Rob Price, “[Digital Currency Ethereum Is Cratering Because of a \\$50 Million Hack](#),” *Business Insider*, June 17, 2016.
- ²³ “[What Is Ethereum Classic? Ethereum vs Ethereum Classic](#),” *BlockGeeks*, June 5, 2017.

- ²⁴ Adam Mann, "[Laws of Physics Say Quantum Cryptography Is Unhackable. It's Not](#)," *Wired*, June 7, 2017.
- ²⁵ "[1.65 Million Hacked Computers Could Be Mining Cryptocurrency for Hackers This Year](#)," *Fossbytes*, Sept. 15, 2017.
- ²⁶ Mohit Kumar, "[Hacker Uses a Simple Trick to Steal \\$7 Million Worth of Ethereum Within 3 Minutes](#)," *The Hacker News*, July 17, 2017.
- ²⁷ "[Cryptocurrency Exchanges Are Increasingly Roiled by Hackings and Chaos](#)," *Fortune*, Sept. 29, 2017.
- ²⁸ "[Ethereum Bandits Stole \\$225 Million This Year](#)," *Fortune*, Aug. 28, 2017.
- ²⁹ Matthew Sparkes, "[US Auctions 50,000 Bitcoins Seized From Silk Road](#)," *The Telegraph*, Dec. 5, 2017.
- ³⁰ Danny Bradbury, "[Users Track \\$100 Million in Stolen Bitcoin After Sheep Marketplace Hack](#)," *Coindesk*, Dec. 3, 2013.
- ³¹ Schumpeter, "[Bitcoin's Woes — Mt. Gone](#)," *The Economist*, Feb. 25, 2014.
- ³² "[Bitcoin Worth \\$72M Was Stolen in Bitfinex Exchange Hack in Hong Kong](#)," *Fortune*, Aug. 3, 2016.
- ³³ Matthew Leising, "[The Ether Thief](#)," *Bloomberg Markets*, June 13, 2017.
- ³⁴ Santiago Palladino, "[The Parity Wallet Hack Explained](#)," *Zeppelin Solutions*, July 19, 2017.
- ³⁵ "[Paper Wallet Guide: How to Protect Your Cryptocurrency](#)," *BlockGeeks*, July 5, 2017.
- ³⁶ Mark Frauenfelder, "[How One Guy Lost Millions of Dollars of Bitcoin to a Hacker](#)," *boingboing*, Dec. 20, 2016.
- ³⁷ Will Knight, "[China's Central Bank Has Begun Cautiously Testing a Digital Currency](#)," *MIT Technology Review*, June 23, 2017.
- ³⁸ Aaron van Wirdum, "[The Long Road to SegWit: How Bitcoin's Biggest Protocol Upgrade Became Reality](#)," *Bitcoin Magazine*, Aug. 31, 2017.
- ³⁹ Marty Zigman, "[Three Methods for Simple Bitcoin Business Accounting](#)," *Bitcoin Magazine*, Mar. 31, 2015.
- ⁴⁰ *Id.*
- ⁴¹ See Samson Mow, "[The Bitcoin Cash Fork Was a Dangerous Trick](#)," *Fortune*, Aug. 7, 2017.
- ⁴² Oracle press release, "[Oracle Launches Enterprise-Grade Blockchain Cloud Service](#)" (Oct. 2, 2017).
- ⁴³ Wilmoth, "[Goldman Sachs Considering Bitcoin Trading Operation: WSJ](#)," *Cryptocoins News*, Feb. 10, 2017.
- ⁴⁴ [Cryptocurrency Chart](#) (Oct. 16, 2016, to Oct. 11, 2017).
- ⁴⁵ Jamie Redman, "[Segwit2x Working Group Announces Hard Fork Roadmap](#)," *Bitcoin.com*, Aug. 10, 2017.
- ⁴⁶ Bradbury, "[Who Sets Bitcoin's Price?](#)" *The Balance*, Feb. 14, 2017.
- ⁴⁷ Palley, *supra* note 1.