Blockchains

NOTE ON BITCOIN

Bitcoin is simpler than it sounds. It is a "cryptocurrency" not because it is mysterious but because it is based on cryptography. To see how, let us consider what jobs a financial record-keeping system needs to do, and then see how Bitcoin does them.

The most intuitive way of talking about money is as a tangible thing: dollars are pieces of paper that you hold in your hand. On this view, the numbers in a bank account balance also represent a thing: the number of dollars "in" the account. So a bank, or an online substitute for one, needs to keep track of who has which things.

But another way of thinking about money is in terms of verbs, rather than nouns. What matters are the transactions in which it passes from hand to hand. When you deposit a $50 birthday check from your aunt in your bank account, that's a transaction in which your aunt gives you $50. You are now capable of engaging in transactions in which you give away up to $50. So you could write a $50 check to your aunt, or a $25 check to your dentist and a $25 check to your cousin. With credit cards and online payment systems like Paypal, the transactions are electronic rather than paper, but the idea is the same: keep track of who pays how much to whom and when.

In this example, the bank maintains a ledger of transactions involving your account. Your aunt's bank maintains a ledger of transactions involving her account. When you deposit her check, the two banks consult with each other, and then very carefully adjust both of their ledgers. Bitcoin is exactly the same, with three differences:

- The Bitcoin ledger, called the *blockchain*, keeps track of transactions involving everyone's Bitcoin accounts.
- Instead of being maintained by a centralized authority, the blockchain is maintained collectively, by everyone who uses Bitcoin.
- The blockchain is secured using public-key cryptography.

First, start with the blockchain. Suppose that Alice sends Bob two Bitcoins. (Perhaps he mowed her lawn, or perhaps he gave her some U.S. dollars in exchange.) Abstracting slightly from the technical details, this transaction could be represented as:

```
From: Alice          To: Bob       Amount:   2.000 BTC
```

Alice makes the transfer to Bob by appending this new transaction to the blockchain. Suppose that just before she does, the blockchain (ordered with the most recent transaction at the top) read:

```
From: Carol          To: Alice     Amount: 200.000 BTC
From: Sujit          To: Rajiv     Amount:    .500 BTC
From: Dave           To: Alice     Amount:   7.250 BTC
From: Carol          To: Alice     Amount:   5.250 BTC
[millions of previous transactions]
```

After Alice adds her transaction to Bob, the blockchain now reads:

```
From: Alice          To: Bob       Amount:   2.000 BTC
From: Carol          To: Alice     Amount: 200.000 BTC
From: Sujit          To: Rajiv     Amount:    .500 BTC
From: Dave           To: Alice     Amount:   7.250 BTC
From: Carol          To: Alice     Amount:   5.250 BTC
[millions of previous transactions]
```

What keeps Alice honest? It is only possible for Alice to make a transaction giving Bob Bitcoins if there are *previous* transactions giving Alice enough Bitcoins. Just as a bank will bounce a check drawn against an account without sufficient funds, other Bitcoin users will reject the transaction unless there are previous transactions already in the blockchain supplying the necessary Bitcoins.* But if Alice has the Bitcoins to spend, other Bitcoin users will agree to add the transaction to the blockchain. When Bob sees that the blockchain has been extended to include Alice's payment to him, he knows that the payment has succeeded.

Second, the blockchain is publicly maintained. The blockchain is just a large and growing file that lists every Bitcoin transaction ever since the start of time. Instead of a bank storing the file on its servers (with appropriate backups), many different Bitcoin users keep a copy of the blockchain. Every time a new "block" of transactions is added to the chain (hence the name), the user adding the block broadcasts it to other users, who add the new transactions to their own copy of the blockchain. It is this collective process of agreement on which transactions have taken place that most distinguishes Bitcoin from traditional payment systems. Bitcoin relies on a peer-to-peer process of consensus rather than on one authority with the power to say which transactions are valid and which are not. Anyone who wants to take part, or to check up on past Bitcoin transactions, can obtain a copy of the blockchain and examine it. In theory, at least, this makes Bitcoin less vulnerable to arbitrary exercises of power: no single person or government can arbitrarily create new Bitcoins or take them away from their owners.

Third, add security into the mix. Bitcoin uses digital signatures to guard against all of the obvious attacks, and a great many subtle ones as well. Every Bitcoin *address* (the source or destination of a transaction) has its own private-key/public-key pair. The "From: Alice" part of the transaction is a digital signature generated using the private key for Alice's address. If the signature matches, anyone examining the transaction can confirm that Alice authorized it; if the signature doesn't match, the transaction will be rejected. Thus, while it is easy to receive Bitcoins, only someone controlling the appropriate private key can spend them. (This also means that if you lose the private key for a Bitcoin address, the Bitcoins are gone forever; no one can spend them.)

Now we are ready to answer two questions hanging over the system: *Where do Bitcoins come from?* and *Why do Bitcoin users cooperate in maintaining the blockchain?* The answer is that there are rewards for participating. A new block of

* This checking process is substantially easier because each Bitcoin transaction explicitly identifies the previous transaction or transactions providing the necessary funds.

transactions is added to the blockchain roughly every ten minutes: the user who first adds it receives a reward of 25 Bitcoins.* Which user that is is chosen essentially at random through a digital version of a scratch-off lottery in which there is an immense supply of free tickets and scratching one off takes a little bit of work and time.† Since whoever scratches off a winning number first wins, Bitcoin users have an incentive to devote their computers' time to "mining" Bitcoins, as the process is called. Each time someone proves that they have won the lottery by exhibiting the winning number for a block of transactions, everyone adds that block and immediately starts scratching off tickets in the next lottery for the next block. This scheme cleverly harnesses Bitcoin users' greed to get them to participate in keeping the system working.

Bitcoin is interesting for many regulatory reasons, as the materials below explore. But it also raises some interesting questions about anonymity. On the one hand, Bitcoin transactions are not identified with users' names, only with inscrutably opaque Bitcoin addresses like `16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM`, so it can be hard to tell who is behind Bitcoin transactions. On the other hand, the blockchain is public, so anyone can scrutinize its history. It is easy to follow Bitcoins from one address to another, unlike cash, which can circulate in near-total secrecy.

UNITED STATES V. ULBRICHT

31 F. Supp. 3d 540 (S.D.N.Y. 2014)

Forrest, District Judge: ...

The Government alleges that Ross Ulbricht engaged in narcotics trafficking, computer hacking, and money laundering conspiracies by designing, launching, and administering a website called Silk Road ("Silk Road") as an online marketplace for illicit goods and services. ...

A conspiracy claim is premised on an agreement between two or more people to achieve an unlawful end. The Government alleges that by designing, launching, and administering Silk Road, Ulbricht conspired with narcotics traffickers and hackers to buy and sell illegal narcotics and malicious computer software and to launder the proceeds using Bitcoin. ...

The Government alleges that Silk Road was designed to operate like eBay: a seller would electronically post a good or service for sale; a buyer would electronically purchase the item; the seller would then ship or otherwise provide to the buyer the purchased item; the buyer would provide feedback; and the site operator

---

* As of 2014. The number will gradually decrease over time, and be replaced by transaction fees offered by the Alices of the world as an incentive to process their transactions.

† To be a little more precise, Bitcoin miners are computing hash values. The winner is the one who finds a 32-bit number with a hash that is sufficiently close to zero. Since the hash function used by Bitcoin (SHA-256) produces outputs that are all but indistinguishable from random, there is no way to speed up the process other than to try one 32-bit number after another. The Bitcoin protocol automatically calibrates the difficulty of the hashing problem – i.e., the number of winning tickets in the lottery, or how close is "sufficiently close" to zero – so that someone will find a matching hash and add a block roughly every ten minutes. There is no way to save up winning numbers from one block to the next, since the details of the hashing depend on the transactions in the block.

(i.e., Ulbricht) would receive a portion of the seller's revenue as a commission. Ulbricht, as the alleged site designer, made the site available only to those using Tor, software and a network that allows for anonymous, untraceable Internet browsing; he allowed payment only via Bitcoin, an anonymous and untraceable form of payment.

Following the launch of Silk Road, the site was available to sellers and buyers for transactions. Thousands of transactions allegedly occurred over the course of nearly three years – sellers posted goods when available; buyers purchased goods when desired. As website administrator, Ulbricht may have had some direct contact with some users of the site, and none with most. This online marketplace thus allowed the alleged designer and operator (Ulbricht) to be anywhere in the world with an Internet connection (he was apprehended in California), the sellers and buyers to be anywhere, the activities to occur independently from one another on different days and at different times, and the transactions to occur anonymously. ...

VIII. Count Four

Count Four charges the defendant with participation in a money laundering conspiracy in violation of 18 U.S.C. § 1956(h). The Government has alleged the requisite statutory elements. First, the Government has alleged that a conspiracy existed between the defendant and one or more others, the object of which was to engage in money laundering. In paragraph 20, the Indictment recites the specific elements required for money laundering:

> It was a part and an object of the conspiracy that ... the defendant, and others known and unknown, ... knowing that the property involved in certain financial transactions represented proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions, which in fact involved the proceeds of specified unlawful activity, to wit, narcotics trafficking and computer hacking ... with the intent to promote the carrying on of such unspecified unlawful activity ....

The defendant argues that the factual allegation that Bitcoins constituted the exclusive "payment system that served to facilitate [ ] illegal commerce" on Silk Road cannot constitute the requisite "financial transaction." The Court disagrees.

As an initial matter, an allegation that Bitcoins are used as a payment system is insufficient in and of itself to state a claim for money laundering. The fact that Bitcoins allow for anonymous transactions does not ipso facto mean that those transactions relate to unlawful activities. The anonymity by itself is not a crime. Rather, Bitcoins are alleged here to be the medium of exchange – just as dollars or Euros could be – in financial transactions relating to the unlawful activities of narcotics trafficking and computer hacking. It is the system of payment designed specifically to shield the proceeds from third party discovery of their unlawful origin that forms the unlawful basis of the money laundering charge.

The money laundering statute defines a "financial transaction" as involving, inter alia, "the movement of funds by wire or other means, or [ ] involving one or more monetary instruments, [ ] or involving the transfer of title to any real property, vehicle, vessel, or aircraft." 18 U.S.C. § 1956(c)(4). The term "monetary instrument" is defined as the coin or currency of a country, personal checks, bank checks, and money orders, or investment securities or negotiable instruments. 18 U.S.C. § 1956(c)(5).

The defendant argues that because Bitcoins are not monetary instruments, transactions involving Bitcoins cannot form the basis for a money laundering conspiracy. He notes that the IRS has announced that it treats virtual currency as property and not as currency. The defendant argues that virtual currencies have some but not all of the attributes of currencies of national governments and that virtual currencies do not have legal tender status. In fact, neither the IRS nor FinCEN purport to amend the money laundering statute (nor could they). In any event, neither the IRS nor FinCEN has addressed the question of whether a "financial transaction" can occur with Bitcoins. This Court refers back to the money laundering statute itself and case law interpreting the statute.

It is clear from a plain reading of the statute that "financial transaction" is broadly defined. It captures all movements of "funds" by any means, or monetary instruments. "Funds" is not defined in the statute and is therefore given its ordinary meaning. "Funds" are defined as "money, often money for a specific purpose." See Cambridge Dictionaries Online, http://dictionary. cambridge.org/us/dictionary/american-english/funds?q=funds (last visited July 3, 2014). "Money" is an object used to buy things.

Put simply, "funds" can be used to pay for things in the colloquial sense. Bitcoins can be either used directly to pay for certain things or can act as a medium of exchange and be converted into a currency which can pay for things. See *Bitcoin*, https://bitcoin.org/en (last visited July 3, 2014); *8 Things You Can Buy With Bitcoins Right Now*, CNN Money, http://money.cnn. com/gallery/technology/2013/11/25/buy-with-bitcoin/ (last visited July 3, 2014). Indeed, the only value for Bitcoin lies in its ability to pay for things – it is digital and has no earthly form; it cannot be put on a shelf and looked at or collected in a nice display case. Its form is digital – bits and bytes that together constitute something of value. And they may be bought and sold using legal tender. See *How to Use Bitcoin*, https://bitcoin.org/en/getting-started (last visited July 3, 2014). Sellers using Silk Road are not alleged to have given their narcotics and malicious software away for free – they are alleged to have sold them.

The money laundering statute is broad enough to encompass use of Bitcoins in financial transactions. Any other reading would – in light of Bitcoins' sole raison d'etre – be nonsensical. Congress intended to prevent criminals from finding ways to wash the proceeds of criminal activity by transferring proceeds to other similar or different items that store significant value. With respect to this case, the Government has alleged that Bitcoins have a value which may be expressed in dollars. (Ind. ¶ 3 (alleging that Ulbricht "reaped commissions worth tens of millions of dollars, generated from the illicit sales conducted through the site").)

There is no doubt that if a narcotics transaction was paid for in cash, which was later exchanged for gold, and then converted back to cash, that would constitute a money laundering transaction.

One can money launder using Bitcoin. The defendant's motion as to Count Four is therefore denied.

QUESTIONS

1. Silk Road, the "Amazon.com of illegal drugs," was reachable only through the Tor network, which hides users' IP addresses. Buyers of obviously illegal substances like heroin or LSD paid sellers using Bitcoins. How secure was this approach?

2. In 2013, the FBI shut down Silk Road by arresting Ulbricht, a/k/a Dread Pirate Roberts, as he logged in from a public library. As part of the arrest, the FBI seized about 174,000 Bitcoins. What does that mean? How do you "seize" a Bitcoin? The government plans to auction them off under the asset forfeiture laws. What does that mean? How do you "auction" a Bitcoin?

ILLINOIS DEPT. OF FINANCIAL AND PROFESSIONAL REGULATION

DIGITAL CURRENCY REGULATORY GUIDANCE

2017

Digital currencies such as Bitcoin, Dogecoin, Ethereum, Litecoin, and ZCash have raised questions with respect to money transmission and exchange of currency. This guidance outlines the policy of the Illinois Department of Financial and Professional Regulation (the "Department") with regards to digital currencies. This guidance expresses the Department's interpretation of Illinois' Transmitters of Money Act ("TOMA") and its application to various activities involving digital currencies. This guidance seeks to establish the regulatory treatment of digital currencies under TOMA as it currently exists. ...

Whether or not an Illinois money transmitter license is required for an entity to engage in the transmission of decentralized digital currencies turns on the question of whether digital currency is considered "money" as defined in TOMA. Accordingly, Section 5 of TOMA defines a "[m]oney transmitter" as:

> [A] person who is located in or doing business in this State and who directly or through authorized sellers does any of the following in this State:
>
> 1) Sells or issues payment instruments
>
> 2) Engages in the business of receiving money for transmission or transmitting money.
>
> 3) Engages in the business of exchanging, for compensation, money of the United States Government or a foreign government to or from money of another government. ...

Section 5 of TOMA defines "[m]oney" as:

> [A] medium of exchange that is authorized or adopted by a domestic or foreign government as a part of its currency and that is customarily used and accepted as a medium of exchange in the country of issuance.

Accordingly, although digital currencies are a digital representation of value that is used as a medium of exchange, store of value, or unit of account, they are not considered money for the purposes of TOMA as digital currencies have not been "authorized or adopted by a domestic or foreign government as a part of its currency." A person or entity engaged in the transmission of solely digital currencies, as defined, would not be required to obtain a TOMA license. However, should transmission of digital currencies involve money in a transaction, that transaction may be considered money transmission depending on how the transaction is organized. ...

In order to provide further guidance and clarity on the application of digital currencies to TOMA, listed below are some examples of common types of digital currency transactions. Please note this is a non-exhaustive list.

Activities Generally Qualifying as Money Transmission

- Exchange involving both digital currency and money through a third party exchanger is generally considered to be money transmission. For example,

some digital currency exchange sites facilitate exchanges by acting as an escrow-like intermediary. In a typical transaction, the buyer of digital currency sends money to the exchanger who holds the funds until it determines that the terms of the sale have been satisfied before transmitting the funds to the seller. Irrespective of its handling of the digital currency, the exchanger conducts money transmission by receiving the buyer's money in exchange for a promise to make it available to the seller.

- Exchange of digital currency for money through an automated machine is generally considered to be money transmission. For example, several companies have begun selling automated machines commonly called "Bitcoin ATMs" that facilitate contemporaneous exchanges of digital currency for money. Most such machines currently available, when operating in their default mode act as an intermediary between a buyer and seller, typically connecting through one of the established exchange sites. When a customer buys or sells digital currency through a machine configured this way, the operator of the machine receives the buyer's money and is engaging in the "business of receiving money for transmission or transmitting money."

  Some digital currency ATMs, however, can be configured to conduct transactions only between the customer and the machine's operator, with no third parties involved. If the machine never involves a third party, and only facilitates a sale or purchase of digital currency by the machine's operator directly with the customer, there is no money transmission because at no time is money received and neither party is engaging in the "business of receiving money for transmission or transmitting money."

Activities Not Qualifying as Money Transmission

- Exchange of digital currency for money directly between two parties does not qualify as money transmission. This is essentially a sale of goods between two parties. The seller gives units of digital currency to the buyer, who pays the seller directly with money. The seller does not receive money with the intent to transmit it to another entity or "engage in the business of exchanging, for compensation, money of the United States Government or a foreign government to or from money of another government."
- Transfer of digital currency by itself is not transmitting money. Because digital currency is not money, the receipt of it with the intent to transmit it to another entity is not "transmitting money." This includes intermediaries who receive digital currency for transfer to a third party, and entities who, akin to depositories (commonly referred to as wallets), hold digital currency on behalf of customers and can either unilaterally execute or prevent a digital currency transaction.
- Exchange of one digital currency for another digital currency is not money transmission.
- A merchant who accepts digital currency as payment for goods or services or an individual who pays for goods or services with digital currency are commonly referred to as "users" of digital currency. Regardless of how many parties are involved, no money is involved at any point in this transaction, so "transmitting money" does not occur.
- Miners do not receive money for verifying transactions. Instead, Miners receive digital currency as payment for verifying transactions, typically by contributing software, connectivity, or computing power to process transactions.

Because money is not involved in the payment of this work, "transmitting money" does not occur.

- Blockchain 2.0 technologies refer to the use of a digital currency's decentralized or distributed ledger system for non-monetary purposes such as verifying ownership or authenticity in a digital capacity. This technology includes software innovations such as colored coins (i.e. coins that are marked specifically to represent a non-monetary asset), smart contracts (i.e. agreements implemented on a distributed ledger), and smart property (i.e. property that is titled using a decentralized distributed ledger). These uses for non- monetary purposes may use digital currency as a medium of exchange, but do not involve the exchange or transmission of money or the sale or issuance of a "payment instrument" and as a result "transmitting money" does not occur.

QUESTIONS

1. What is the difference between money *laundering* and money *transmission*?
2. Maura mines Bitcoins. Every few months, she uses the Erebor exchange to convert them into U.S. dollars. She also occasionally transfers some Bitcoins directly to Barrow Burgers to buy dinner. Is she required to register as a money transmitter? Should any of them have to pay income taxes on their Bitcoin transactions?
3. The Bank Secrecy Act and other federal laws require that money transmitters keep detailed records and report on suspicious transactions. These laws are designed to prevent tax evasion, money laundering, black markets, and other skulduggery. Does it make sense to extend them to Bitcoin transactions?
4. State money transmission laws go further. They require money transmitters to make numerous disclosures to consumers and maintain a sufficient reserve of assets, among many other things. Does it make sense to extend these laws to Bitcoin transactions?

INTERNAL REVENUE SERVICE NOTICE 2014-21

(Mar. 25, 2014)[*]

Section 1. Purpose

This notice describes how existing general tax principles apply to transactions using virtual currency. The notice provides this guidance in the form of answers to frequently asked questions.

Section 2. Background

The Internal Revenue Service (IRS) is aware that "virtual currency" may be used to pay for goods or services, or held for investment. Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account,

---

* [Ed: The IRS describes Notices as follows:

> A notice is a public pronouncement that may contain guidance that involves substantive interpretations of the Internal Revenue Code or other provisions of the law. For example, notices can be used to relate what regulations will say in situations where the regulations may not be published in the immediate future.

Understanding IRS Guidance - A Brief Primer, Internal Revenue Service, http://www.irs.gov/uac/Understanding-IRS-Guidance-A-Brief-Primer.]

and/or a store of value. In some environments, it operates like "real" currency – i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance – but it does not have legal tender status in any jurisdiction.

Virtual currency that has an equivalent value in real currency, or that acts as a substitute for real currency, is referred to as "convertible" virtual currency. Bitcoin is one example of a convertible virtual currency. Bitcoin can be digitally traded between users and can be purchased for, or exchanged into, U.S. dollars, Euros, and other real or virtual currencies.

Section 3. Scope

In general, the sale or exchange of convertible virtual currency, or the use of convertible virtual currency to pay for goods or services in a real-world economy transaction, has tax consequences that may result in a tax liability. ...

Section 4. Frequently Asked Questions

Q-1: How is virtual currency treated for federal tax purposes?

A-1: For federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency.

Q-2: Is virtual currency treated as currency for purposes of determining whether a transaction results in foreign currency gain or loss under U.S. federal tax laws?

A-2: No. Under currently applicable law, virtual currency is not treated as currency that could generate foreign currency gain or loss for U.S. federal tax purposes.

Q-3: Must a taxpayer who receives virtual currency as payment for goods or services include in computing gross income the fair market value of the virtual currency?

A-3: Yes. A taxpayer who receives virtual currency as payment for goods or services must, in computing gross income, include the fair market value of the virtual currency, measured in U.S. dollars, as of the date that the virtual currency was received. ...

Q-5: How is the fair market value of virtual currency determined?

A-5: For U.S. tax purposes, transactions using virtual currency must be reported in U.S. dollars. Therefore, taxpayers will be required to determine the fair market value of virtual currency in U.S. dollars as of the date of payment or receipt. If a virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of the virtual currency is determined by converting the virtual currency into U.S. dollars (or into another real currency which in turn can be converted into U.S. dollars) at the exchange rate, in a reasonable manner that is consistently applied.

Q-6: Does a taxpayer have gain or loss upon an exchange of virtual currency for other property?

A-6: Yes. If the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis* of the virtual currency, the taxpayer has taxable gain. The taxpayer has a loss if the fair market value of the property received is less than the adjusted basis of the virtual currency. ...

Q-8: Does a taxpayer who "mines" virtual currency (for example, uses computer resources to validate Bitcoin transactions and maintain the public Bitcoin transaction ledger) realize gross income upon receipt of the virtual currency resulting from those activities?

A-8: Yes, when a taxpayer successfully "mines" virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income. ...

Q-12: Is a payment made using virtual currency subject to information reporting?

A-12: A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property. For example, a person who in the course of a trade or business makes a payment of fixed and determinable income using virtual currency with a value of $600 or more to a U.S. nonexempt recipient in a taxable year is required to report the payment to the IRS and to the payee. Examples of payments of fixed and determinable income include rent, salaries, wages, premiums, annuities, and compensation. ...

QUESTIONS

1. Consider Maura and Erebor again. According to the IRS, which of them owe income tax?
2. Smug Investments Inc. buys 100 Bitcoins on January 1, when Bitcoins are trading for $5,000. As of July 1, Bitcoins are trading for $15,000 each. Balrog sells 50 Bitcoins on October 19, when they are trading for $10,000. At the end of the year on December 31, Bitcoins are trading for $20,000 each. How much income does Smug owe income tax on?

IN THE MATTER OF MUNCHEE INC.

Administrative Proceeding File No. 3-18304 (S.E.C. Dec. 11, 2017)

I.

The Securities and Exchange Commission deems it appropriate that cease- and-desist proceedings be, and hereby are, instituted pursuant to Section 8A of the Securities Act of 1933 against Munchee Inc. ("Munchee" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. ...

III.

On the basis of this Order and Respondent's Offer, the Commission finds that: ...

---

* [Ed: The "basis" of property is a tax concept designed to capture how much a taxpayer paid to acquire property. If I buy a widget on Monday for $1,000, we say that I have a $1,000 basis in the widget. If I then sell the widget on Tuesday for $1,500, I can subtract the $1,000 basis, leaving me with a taxable "gain" of $500.]

Summary

Munchee is a California business that created an iPhone application ("app") for people to review restaurant meals. In October and November 2017, Munchee offered and then sold digital tokens ("MUN" or "MUN token") to be issued on a blockchain or a distributed ledger. Munchee conducted the offering of MUN tokens to raise about $15 million in capital so that it could improve its existing app and recruit users to eventually buy advertisements, write reviews, sell food and conduct other transactions using MUN. In connection with the offering, Munchee described the way in which MUN tokens would increase in value as a result of Munchee's efforts and stated that MUN tokens would be traded on secondary markets.

Based on the facts and circumstances set forth below, MUN tokens were securities pursuant to Section 2(a)(1) of the Securities Act. MUN tokens are "investment contracts" under *SEC v. W. J. Howey Co.*, 328 U.S. 293 (1946), and its progeny, including the cases discussed by the Commission in its Report of Investigation Pursuant To Section 21(a) Of The Securities Exchange Act of 1934: The DAO (Exchange Act Rel. No. 81207) (July 25, 2017) (the "DAO Report"). Among other characteristics of an "investment contract," a purchaser of MUN tokens would have had a reasonable expectation of obtaining a future profit based upon Munchee's efforts, including Munchee revising its app and creating the MUN "ecosystem" using the proceeds from the sale of MUN tokens. Munchee violated Sections 5(a) and 5(c) of the Securities Act by offering and selling these securities without having a registration statement filed or in effect with the Commission or qualifying for exemption from registration with the Commission. On the second day of sales of MUN tokens, the company was contacted by Commission staff. The company determined within hours to shut down its offering, did not deliver any tokens to purchasers, and returned to purchasers the proceeds that it had received.

Facts

1. Munchee is a California business that created an app (the "Munchee App") for use with iPhones. The company began developing the app in late 2015 and launched the app in the second quarter of 2017.
2. The Munchee App allows users to post photographs and reviews of meals that they eat in restaurants. The Munchee App is available only in the United States.
3. Munchee and its agents control the content on multiple web pages, including but not limited to its website (the "Munchee Website"), an additional site where it posted Munchee's "white paper" (the "MUN White Paper"), a Twitter account, a Facebook page, and posts on various message boards (collectively, the "Munchee Web Pages").

Munchee Offers To Sell MUN To The General Public

4. By Fall 2017, Munchee had developed a plan to improve the Munchee App during 2018 and 2019 that included raising capital through the creation of the MUN token and incorporating the token into the Munchee App. The MUN is a token issued on the Ethereum blockchain. Munchee created 500 million MUN tokens and stated that no additional tokens could be created.

5. On or about October 1, 2017, Munchee announced it would be launching an "initial coin offering" or "ICO"[1] to offer MUN tokens to the general public. Munchee posted the MUN White Paper that described MUN tokens, the offering process, how Munchee would use the offering proceeds to develop its business, the way in which MUN tokens would increase in value, and the ability for MUN token holders to trade MUN tokens on secondary markets. Munchee posted information about the offering and the MUN White Paper through posts on the Munchee Web Pages, including on a blog, Facebook, Twitter, BitcoinTalk, and the Munchee Website.
6. MUN tokens were to be available for purchase by individuals in the United States and worldwide through websites and social media pages including, but not limited to, the Munchee Web Pages.
7. Pursuant to the MUN White Paper, Munchee sought to raise about $15 million in Ether by selling 225 million MUN tokens out of the 500 million total MUN tokens created by the company. Purchasers of MUN tokens in the earlier stages of the offering were offered discounts of 15% and 10% on the offering price. Munchee said it would keep the remaining 275 million MUN tokens and use those MUN tokens to support its business, including by paying rewards in the Munchee App with MUN tokens, paying its employees and advisors with MUN tokens, and "facilitating advertising transactions in the future." In the MUN White Paper and elsewhere, Munchee said that it would spend 75% of the offering proceeds to hire people for its development team and to market and promote the Munchee App, use 15% "for maintenance and to ensure the smooth operation of the MUN token ecosystem" and use 10% for "legals to make sure Munchee is compliant in all countries." Munchee described a timeline that provided for various development milestones in 2018 and 2019, including the development of a smart contract on the Ethereum blockchain to integrate "in-app" use of the MUN token and setting up in-app wallets for end-users.
8. The MUN White Paper referenced the DAO Report and stated that Munchee had done a "Howey analysis" and that "as currently designed, the sale of MUN utility tokens does not pose a significant risk of implicating federal securities laws." The MUN White Paper, however, did not set forth any such analysis.

---

1. An "initial coin offering" or "ICO" is a recently developed form of fundraising event in which an entity offers participants a unique digital "coin" or "token" in exchange for consideration (most commonly Bitcoin, Ether, or fiat currency). The tokens are issued and distributed on a "blockchain" or cryptographically-secured ledger. Tokens often are also listed and traded on online platforms, typically called virtual currency exchanges, and they usually trade for other digital assets or fiat currencies. Often, tokens are listed and tradeable immediately after they are issued.

   Issuers often release a "white paper" describing the particular project they seek to fund and the terms of the ICO. Issuers often pay others to promote the offering, including through social media channels such as message boards, online videos, blogs, Twitter, and Facebook. There are websites and social media feeds dedicated to discussions about ICOs and the offer, sale and trading of coins and tokens.

Munchee's Plan To Create An "Ecosystem" And Take Other Steps To Increase The Value Of MUN

9. Munchee offered MUN tokens in order to raise capital to build a profitable enterprise. Munchee said that it would use the offering proceeds to run its business, including hiring people to develop its product, promoting the Munchee App, and ensuring "the smooth operation of the MUN token ecosystem."

10. While Munchee told potential purchasers that they would be able to use MUN tokens to buy goods or services in the future after Munchee created an "ecosystem," no one was able to buy any good or service with MUN throughout the relevant period.

11. On the Munchee Website, in the MUN White Paper and elsewhere, Munchee described the "ecosystem" that it would create, stating that it would pay users in MUN tokens for writing food reviews and would sell both advertising to restaurants and "in-app" purchases to app users in exchange for MUN tokens. Munchee also said it would work with restaurant owners so diners could buy food with MUN tokens and so that restaurant owners could reward app users – perhaps those who visited the restaurant or reviewed their meal – in MUN tokens. As a result, MUN tokens would increase in value. ...

13. Munchee intended for MUN tokens to trade on a secondary market. In the MUN White Paper, Munchee stated that it would work to ensure that MUN holders would be able to sell their MUN tokens on secondary markets, saying that "Munchee will ensure that MUN token is available on a number of exchanges in varying jurisdictions to ensure that this is an option for all token-holders." ...

Munchee Promoted MUN Tokens And Purchasers Had A Reasonable Expectation Of Obtaining A Future Profit

14. Purchasers reasonably would have viewed the MUN token offering as an opportunity to profit. ... Purchasers would reasonably believe they could profit by holding or trading MUN tokens, whether or not they ever used the Munchee App or otherwise participated in the MUN "ecosystem," based on Munchee's statements in its MUN White Paper and other materials. ...

15. For example, Munchee published a blog post on October 30, 2017 that was titled "7 Reasons You Need To Join The Munchee Token Generation Event." Reason 4 listed on the post was "As more users get on the platform, the more valuable your MUN tokens will become" and then went on to describe how MUN purchasers could "watch[] their value increase over time" and could count on the "burning" of MUN tokens to raise the value of remaining MUN tokens. ...

17. In addition, Munchee made public statements or endorsed other people's public statements that touted the opportunity to profit. For example, on or about October 25, 2017, Munchee created a public posting on Facebook, linked to a third-party YouTube video, and wrote "199% GAINS on MUN token at ICO price! Sign up for PRE-SALE NOW!" The linked video featured a person who said "Today we are going to talk about Munchee. Munchee is a crazy ICO. If you don't know what an ICO is, it is called an initial coin offering. Pretty much, if you get into it early enough, you'll prob-

ably most likely get a return on it." This person went on to use his "ICO investing sheet" to compare the MUN token offering to what he called the "Top 15 ICOs of all time" and "speculate[d]" that a $1,000 investment could create a $94,000 return.

18. Munchee and its agents targeted the marketing of the MUN tokens offering to people with an interest in tokens or other digital assets that have in recent years created profits for early investors in ICOs. This marketing did not use the Munchee App or otherwise specifically target current users of the Munchee App to promote how purchasing MUN tokens might let them qualify for higher tiers and bigger payments on future reviews. Nor did Munchee advertise the offering of MUN tokens in restaurant industry media to reach restaurant owners and promote how MUN tokens might let them advertise in the future. Instead, Munchee and its agents promoted the MUN token offering in forums aimed at people interested in investing in Bitcoin and other digital assets, including on BitcoinTalk.org, a message board where people discuss investing in digital assets. These forums are available and attract viewers worldwide, even though the Munchee App was only available in the United States. ...

MUN Token Purchasers Reasonably Expected They Would Profit From The Efforts Of Munchee And Its Agents

21. Purchasers would reasonably have had the expectation that Munchee and its agents would expend significant efforts to develop an application and "ecosystem" that would increase the value of their MUN tokens.

22. Munchee highlighted the credentials, abilities and management skills of its agents and employees. For example, in the MUN White Paper and elsewhere, Munchee highlighted that its founders had worked at prominent technology companies and highlighted their skills running businesses and creating software.

23. As discussed above, Munchee said in the MUN White Paper that the value of MUN tokens would depend on the company's ability to change the Munchee App and create a valuable "ecosystem" that would inspire users to create new reviews, inspire restaurants to obtain MUN tokens to reward diners and pay Munchee for advertising, and inspire users to obtain MUN tokens to buy meals and to attain higher status within the Munchee App. Munchee said that it and its agents would undertake that work during 2018 and 2019. ...

Legal Analysis

28. Under Section 2(a)(1) of the Securities Act, a security includes "an investment contract." *See* 15 U.S.C. § 77b. An investment contract is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. *See SEC v. Edwards*, 540 U.S. 389, 393 (2004); *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946); *see also United Housing Found., Inc. v. Forman*, 421 U.S. 837, 852-53 (1975) (The "touchstone" of an investment contract "is the presence of an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others."). This definition embodies a "*flexible rather than a static principle*, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the

promise of profits." *Howey*, 328 U.S. at 299 (emphasis added). The test "permits the fulfillment of the statutory purpose of compelling full and fair disclosure relative to the issuance of 'the many types of instruments that in our commercial world fall within the ordinary concept of a security.'" *Id.* In analyzing whether something is a security, "form should be disregarded for substance," *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967), "and the emphasis should be on economic realities underlying a transaction, and not on the name appended thereto." *Forman*, 421 U.S. at 849.

29. As the Commission discussed in the DAO Report, tokens, coins or other digital assets issued on a blockchain may be securities under the federal securities laws, and, if they are securities, issuers and others who offer or sell them in the United States must register the offering and sale with the Commission or qualify for an exemption from registration.

A. The MUN Tokens Were Securities

30. As described above, the MUN tokens were securities as defined by Section 2(a)(1) of the Securities Act because they were investment contracts.

31. Munchee offered and sold MUN tokens in a general solicitation that included potential investors in the United States. Investors paid Ether or Bitcoin to purchase their MUN tokens. Such investment is the type of contribution of value that can create an investment contract.

32. MUN token purchasers had a reasonable expectation of profits from their investment in the Munchee enterprise. The proceeds of the MUN token offering were intended to be used by Munchee to build an "ecosystem" that would create demand for MUN tokens and make MUN tokens more valuable. Munchee was to revise the Munchee App so that people could buy and sell services using MUN tokens and was to recruit "partners" such as restaurants willing to sell meals for MUN tokens. The investors reasonably expected they would profit from any rise in the value of MUN tokens created by the revised Munchee App and by Munchee's ability to create an "ecosystem" – for example, the system described in the offering where restaurants would want to use MUN tokens to buy advertising from Munchee or to pay rewards to app users, and where app users would want to use MUN tokens to pay for restaurant meals and would want to write reviews to obtain MUN tokens. In addition, Munchee highlighted that it would ensure a secondary trading market for MUN tokens would be available shortly after the completion of the offering and prior to the creation of the ecosystem. Like many other instruments, the MUN token did not promise investors any dividend or other periodic payment. Rather, as indicated by Munchee and as would have reasonably been understood by investors, investors could expect to profit from the appreciation of value of MUN tokens resulting from Munchee's efforts.

33. Investors' profits were to be derived from the significant entrepreneurial and managerial efforts of others – specifically Munchee and its agents – who were to revise the Munchee App, create the "ecosystem" that would increase the value of MUN (through both an increased demand for MUN tokens by users and Munchee's specific efforts to cause appreciation in value, such as by burning MUN tokens), and support secondary markets. Investors had little choice but to rely on Munchee and its expertise. At the time of the offering and sale of MUN tokens, no other person could make changes to the

Munchee App or was working to create an "ecosystem" to create demand for MUN tokens.

34. Investors' expectations were primed by Munchee's marketing of the MUN token offering. To market the MUN token offering, Munchee and its agents created the Munchee Website and the MUN White Paper and then posted on message boards, social media and other outlets. They described how Munchee would revise the Munchee App and how the new "ecosystem" would create demand for MUN tokens. They likened MUN to prior ICOs and digital assets that had created profits for investors, and they specifically marketed to people interested in those assets – and those profits – rather than to people who, for example, might have wanted MUN tokens to buy advertising or increase their "tier" as a reviewer on the Munchee App. Because of the conduct and marketing materials of Munchee and its agents, investors would have had a reasonable belief that Munchee and its agents could be relied on to provide the significant entrepreneurial and managerial efforts required to make MUN tokens a success.

35. Even if MUN tokens had a practical use at the time of the offering, it would not preclude the token from being a security. Determining whether a transaction involves a security does not turn on labelling – such as characterizing an ICO as involving a "utility token" – but instead requires an assessment of "the economic realities underlying a transaction." *Forman*, 421 U.S. at 849. All of the relevant facts and circumstances are considered in making that determination. See *Forman*, 421 U.S. at 849 (purchases of "stock" solely for purpose of obtaining housing not purchase of "investment contract").

B. Munchee Offered And Sold MUN Tokens In Violation Of The Securities Act

36. As described above, Munchee offered and sold securities to the general public, including potential investors in the United States, and actually sold securities to about 40 investors. No registration statements were filed or in effect for the MUN token offers and sales and no exemptions from registration were available.

37. As a result of the conduct described above, Munchee violated Section 5(a) of the Securities Act, which states that unless a registration statement is in effect as to a security, it shall be unlawful for any person, directly or indirectly, to make use of any means or instruments of transportation or communication in interstate commerce or of the mails to sell such security through the use or medium of any prospectus or otherwise; or to carry or cause to be carried through the mails or in interstate commerce, by any means or instruments of transportation, any such security for the purpose of sale or for delivery after sale.

38. Also as a result of the conduct described above, Munchee violated Section 5(c) of the Securities Act, which states that it shall be unlawful for any person, directly or indirectly, to make use of any means or instruments of transportation or communication in interstate commerce or of the mails to offer to sell or offer to buy through the use or medium of any prospectus or otherwise any security, unless a registration statement has been filed as to such security.

IV.

In view of the foregoing, the Commission deems it appropriate to impose the sanctions agreed to in Respondent's Offer.

Accordingly, it is hereby ORDERED that:

A. Pursuant to Section 8A of the Securities Act, Respondent Munchee cease and desist from committing or causing any violations and any future violations of Sections 5(a) and (c) of the Securities Act.

QUESTIONS

1. Was the MUN ICO a scam? Was it a good investment? Why did the SEC shut it down? Was there anything that Munchee could have done differently to make the ICO acceptable? If so, why didn't it?
2. There are many other kinds of financial regulation, each with its own complicated statutory scheme. There are "commodities," *see* 7 U.S.C. § 1a(9), "banks," *see* 12 U.S.C. § 1813(a)(1), "negotiable instrument[s]," *see* U.C.C. § 3-104, and many more. With such a well-developed regulatory apparatus, why is it so hard to figure out how Bitcoins fit in?
3. Does Bitcoin raise any new jurisdictional issues?

KEVIN WERBACH & NICOLAS CORNELL

CONTRACTS EX MACHINA

67 Duke L.J. (forthcoming)

In 1996-97, cryptographer Nick Szabo published a series of articles and blog posts outlining the functions and technical requirements for what he labeled "smart contracts." Szabo's starting point was that networked digital protocols "both challenge and enable us to formalize and secure new kinds of relationships in this new environment, just as contract law, business forms, and accounting controls have long formalized and secured business relationships in the paper-based world." He suggested that, "[t]he contractual phases of search, negotiation, commitment, performance, and adjudication...can be embedded in [] hardware and software...." Many of those functions were already being implemented electronically at the time, or would be soon with the rise of e-commerce. The visionary aspect of Szabo's concept was that hardware and software *alone* would handle the full lifecycle of contractual activity. Human action could be completely replaced in various parts of contractual exchange.

Szabo's smart contracts did not require fancy technology. His primary example was the humble vending machine. The simple electronic mechanism of a vending machine performs two critical functions. First, it directly effectuates performance, by taking in money and dispensing products. Second, it incorporates enough security to make the cost of breach (breaking into the machine) exceed the potential rewards. For all practical purposes, the vending machine is the entirety of the contractual environment for its transactions. ...

Szabo's original conception of smart contracts envisioned that cryptography would secure agreements, but had no mechanism to guarantee enforcement or transfer of value. Everything changed with the development of Bitcoin. Bitcoin's success in decentralizing trusted financial transactions gives hope to those who advocate similar decentralization of trusted contractual agreements. Smart contracts may actually be a bigger idea than Bitcoin as a currency.

The blockchain's distributed trust is what facilitates smart contracts with unknown or untrusted counterparties. And its radical decentralization is what potentially makes smart contracts into substitutes for the state-based legal system, rather than merely screens in front of it. For example, a financial trading program that automatically buys certain stocks when their prices match a pre-defined algorithm could be described as a smart contract in some sense. If a dispute arises, however, the parties to that self- executing transaction will still turn to the courts, which will apply traditional legal doctrines to evaluate the agreement, ascertain breach, and impose a remedy if appropriate. With smart contracts, the situation is novel because parties do not have that option. The transaction is irreversibly encoded on a distributed blockchain.

Smart contracts are possible with Bitcoin because its protocols include a scripting language that allows limited programmable logic to be incorporated into transactions. The vast majority of transactions on the Bitcoin blockchain are simple transfers of Bitcoins between accounts. However, when computers on the Bitcoin network process those transfers, they can be tasked with other function such requiring confirmation from multiple accounts. This allows for more complicated arrangements such as delaying payment until confirmation is received from a specified number of parties.

Bitcoin's native scripting language is limited. Companies are developing more powerful systems that execute the contractual logic on application servers outside the blockchain, or through alternate blockchains supporting more sophisticated scripts. The most heralded is Ethereum, a general-purpose computing platform on a blockchain foundation. The promise of Ethereum is almost comically broad: one article suggested it might "transform law, finance, and civil society." While such enthusiasm may be excessive, Ethereum has gained a substantial and passionate following among developers and cryptocurrency enthusiasts. Roughly a year after Ethereum launched, there were already over 300 distributed apps built on the platform. ...

The scripting language on a blockchain platform such as Bitcoin or Ethereum can be used to determine whether the conditions for performance of a smart contract have been met, and then execute the contractual transaction without human interference. In the simplest case, parties place Bitcoins or other digital currency into a suspended state on the blockchain, and once certain terms are met, those Bitcoins are transferred to the appropriate account. The Bitcoins may represent payment directly, or they may be used as tokens, associated with digital rights in assets.

This algorithmic enforcement allows contracts to be executed as quickly and cheaply as other computer code. The cost savings occur at every stage, from negotiation to enforcement, especially in the replacement of judicial enforcement with automated mechanisms. If contracts are substantially cheaper and more efficient, more kinds of activities are opened up to contractual agreement. The second broad attraction of smart contracts is their fundamentally distributed nature. Those who wish to avoid trust in centralized private or governmental actors, whether for political reasons or otherwise, can now do so and still benefit from the advantages of contract.

Blockchain transactions are irrevocable. There is no technical means, short of undermining the integrity of the entire system, to unwind a transfer. It is, however, possible to incorporate logic into a smart contract that allows for various forms of exceptions or conditions. Or enforcement could, in theory, be structured to allow

for arbitration. Such flexibility, however, has to be coded into the smart contract out the outset, and it takes away from the decentralization and efficiency that are the attractions of smart contracts to begin with.

Sometimes a smart contract may need to refer to facts in the world, such as when a contract pays out if a stock exceeds a certain price on a certain date. The Bitcoin blockchain knows nothing about stock prices; that information must be provided through an external data feed. In the language of smart contracts, systems that interpret such external feeds and verify contractual performance are referred to as oracles. Unlike the blockchain, oracles are not fully decentralized. The contractual parties must, to some degree, trust the operator of the oracle and the authenticity of the data feed.

Using these capabilities, smart contracts can be employed for a wide variety of purposes. These could include not just simple financial arrangements but more complex vehicles such as wills and crowdfunding systems (in which funds are only disbursed if projects hit a target threshold, and otherwise returned.) Another category is so-called smart property, in which the rights associated with objects attach to the objects themselves. Networked door locks on shared cars (through a system such as Zipcar) could automatically open (only for that individual) when someone paid the access fee. Or, access to a leased car could be shut off from a delinquent lessee and given to the bank, but only until full payment of the principal. More broadly, with over 25 billion devices, from light switches to crop moisture monitors, expected to have internet connectivity in 2020, smart contracts would allow devices to operate autonomously, share resources, and exchange data without central management.