MURPHY & McGONIGLE
A Professional Corporation

Cryptocurrency Regulatory Developments

April 19, 2018

Katherine Cooper

Daniel Alter

Matthew Comstock

Joseph Facciponti

Daniel Payne

TABLE OF CONTENTS

CHAPTER I
SECURITIES ISSUANCE AND TRADING

Companies that either intentionally issue securities in digitized form on a blockchain, or unwittingly issue tokens that are deemed to be securities, are subject to the federal securities laws. Digitized securities, like all other securities, must be issued, resold, traded and custodied in accordance with the federal securities laws outlined below.

I. OFFERINGS OF SECURITIES

A. Registered Offerings

1. Governed by Section 5 of the Securities Act of 1933 (the "Securities Act").
2. Section 5 prohibits the sale of securities to the public unless:
    a. A registration statement for such securities has been filed with the SEC and is in effect, and
    b. The issuer has delivered a prospectus to investors.[1]
3. Prospectus
    a. Must conform to the requirements of Section 10 of the Securities Act, and
    b. Generally must contain the same information set out in the registration statement.[2]
4. Securities sold to the public in a registered offering are freely tradeable.

B. Exempt Offerings

1. Securities can be sold without SEC registration
2. Securities sold without registration in reliance on a so-called private placement exemption in compliance with specified provisions of the Securities Act and certain rules and regulations adopted under the Securities Act[3]
3. Section 4(a)(2) of the Securities Act
    a. Permits sales of securities without SEC registration if those sales do not involve a public offering and meet other, specified criteria[4]

---

[1] 15 U.S.C. §77e.

[2] 15 U.S.C. §77j. Issuers typically use one of two basic registration forms under the Securities Act (although there are others). Form S-1, with limited exceptions, contains all the required registration statement information, including a description of the business and the issuer's financial condition. This is the form used for initial public offerings. Companies that have already issued securities and are so-called "reporting companies," meaning that they have registered the securities they issued under the Exchange Act, and they file periodic reports with the SEC, as required under the Exchange Act, may register additional securities sale on Form S-3. Form S-3 allows the issuer to incorporate by reference information contained in its periodic reports it files under the Exchange Act.

[3] Transactions exempt from the registration requirements of Section 5 of the Securities Act are not exempt from the anti-fraud, civil liability, or other provisions of the federal securities laws.

[4] 15 U.S.C. § 77d(a)(2).

b. Sales must be limited to "sophisticated investors," who must have sufficient knowledge and experience in finance and business to evaluate the risks and merits of investment, or be able to bear the investment's economic risk

c. No general solicitation of investors from the public. Issuers, however, historically took the view that the limits of the registration exemption under Section 4(a)(2) were unclear.

4. Regulation D under the Securities Act

a. Intended to provide clarity on the circumstances in which securities can be sold without SEC registration.[5]

b. Issuer relying on Regulation D must file Form D with the SEC within 15 days after the first sale of securities in the offering.

c. Many states also require Form D to be filed with them.

d. Regulation D does not have any filing requirements beyond Form D.

e. Relevant exemptions are set out in Rules 504 and 506 of Regulation D.

f. Rule 504

i. Permits an issuer to raise up to $5 million in a 12-month period.[6]

ii. Prohibits general solicitation of investors and advertising the private placement, with limited exceptions (see below).

iii. Does not preempt state blue sky laws.[7]

iv. Securities issued under the rule are restricted, meaning that they cannot be resold without SEC registration or an exemption from registration, subject to limited exceptions.

v. Not limited to accredited investors, as that term is defined below.

vi. An issuer may be able to sell securities under Rule 504 with general solicitation and advertising if it: (x) sells in accordance with state law that requires the public filing and delivery to investors of a substantive disclosure document; (y) sells in accordance with a state law that requires registration and disclosure delivery and also sells in a state without those requirements, as long as the issuer delivers to all purchaser the disclosure documents mandated by a state in which it registered; or (z) sells exclusively according to state law

[5] Paragraph (b) of Rule 500 of Regulation D states that "[n]othing in Regulation D obviates the need to comply with any applicable state law relating to the offer and sale of securities." 17 CFR § 230.500.
[6] 17 CFR § 230.504.
[7] "Blue sky laws" are state securities registration and anti-fraud laws.

exemptions that permit general solicitation and advertising, so long as sales are made only to accredited investors.

g. Rule 506(b)

   i. Safe harbor for the non-public offering exemption in Section 4(a)(2) of the Securities Act.

   ii. Allows issuers to raise unlimited amounts of cash without registering the offering with the SEC.

   iii. Sell to unlimited number of accredited investors.

   iv. No more than 35 non-accredited investors;[8] non-accredited investors must be "sophisticated" within the meaning of Section 4(a)(2).

   v. No general solicitation to market the offering and must provide specified disclosures and financial statements to investors.

   vi. Issuer must be available to answer questions from prospective purchasers who are non-accredited investors.[9]

   vii. Offerings under 506(b) are exempt from state blue sky laws.

h. 506(c)

   i. Permits issuers to raise unlimited cash without registering the offering with the SEC.

   ii. Eliminates the prohibition on general solicitation if (x) all purchasers are accredited investors, and (y) the issuer takes reasonable steps to verify accredited status.

   iii. Offerings exempt from state blue sky laws.

   iv. Securities issued in reliance on Rule 506 are restricted with respect to resale.

   v. Although Rule 506 offerings are exempt from registration under the Securities Act, if an issuer sells equity securities to 2000 or more persons, or 500 or more non-accredited investors, the issuer must register the securities with the SEC under Section 12(g) of the Securities Exchange Act of 1934 (the "Exchange Act"), which subjects the issuer to certain SEC reporting requirements.[10]

---

[8] Under Rule 501 of Regulation D, the term "accredited investor" includes, among others, certain financial institutions, such as broker-dealers, registered investment companies and insurance companies. It also includes natural persons whose net worth, or joint net worth with that person's spouse, exceeds $1 million (excluding the value of the person's residence). The term also includes natural persons whose income in each of the two most recent years was in excess of $200,000 or jointly with that person's spouse was in excess of $300,000.

[9] 17 CFR § 230.504(b).

[10] 15 U.S.C. § 78l(g).

5. Regulation A Offerings

    a. Regulation A under the Securities Act (often referred to as "Regulation A+") permits a public offering and sale of securities without registering the offering with the SEC.[11]

    b. Issuer can engage in general solicitation of investors and advertise offering.

    c. Purchasers are not limited to accredited investors.

    d. Securities sold in a Regulation A+ offering are not restricted securities.

    e. Two Tiers of Regulation A+ offerings.

    f. Tier 1

        i. Allows the sale of up to $20 million of equity, debt, or convertible securities in a 12-month period.

        ii. Subject to state blue sky registration and filing requirements on a state-by-state basis.

        iii. No limit on the type of investors who may participate in Tier 1 offerings.[12]

    g. Tier 2

        i. Allows the sale of up to $50 million of equity, debt, and convertible debt securities in a 12-month period.

        ii. Tier 2 offerings are not limited to specific types of investors, but non-accredited investors are subject to investment limits. Such investors may purchase securities in a Tier 2 offering with a value equal to no more than 10 percent of the greater of the investor's annual income or net worth.

    h. Exempt from state blue sky review for offerings to "qualified purchasers" or with respect to securities listed on a national securities exchange. A "qualified purchaser" includes all offerees and purchasers in a Tier 2 offering.[13]

    i. Resales of securities issued under Regulation A+ are permissible, subject to specified limitations:

---

[11] 17 CFR § 230.251 et seq.

[12] 17 CFR § 230.251(a)(1).

[13] 17 CFR § 230.251(a)(2). A Regulation A+ issuer must file an offering statement with the SEC. After the statement is filed, the issuer can make oral offers and written offers under specified circumstances, but the issuer cannot sell the securities until the SEC has qualified the offering statement. Underwriters and dealers also may need to deliver to purchasers a Final Offering Circular. 17 CFR § 230.251(d).

i. For 12 months from initial qualification, security holder sales cannot exceed 30% of the aggregate Regulation A+ offering; and

ii. After the first year, the limitation on secondary sales falls away for non-affiliates.[14]

j. Securities issued under Regulation A+ are exempt from registration under Section 12(g) of the Exchange Act if:

i. The issuer remains current on its Regulation A+ reporting obligations and has a public float of less than $75 million; or

ii. In the absence of a public float, annual revenues of less than $50 million.

k. Securities issued under Regulation A+ could be listed on a national securities exchange. Listing would need to comply with Section 12(b) of the Exchange Act.[15]

L. Securities issued under Regulation A+ also could be resold in the over-the-counter. Broker-dealers publishing quotes with respect to such securities would need to do so in compliance with Rule 15c2-11 under the Exchange Act.

II. RESALES OF SECURITIES

A. Securities issued in a private transaction are not freely tradeable in the secondary market.

B. A holder of restricted securities must resell into the market either by registering the securities with the SEC, or subject to a valid exemption from registration.

C. Rule 144 under the Securities Act

1. Provides a safe harbor that allows holders to resell restricted securities without SEC registration.[16]

2. Absent safe harbor, a reseller of restricted securities could be viewed as participating in the distribution of that security and, thus, an underwriter, as that term is defined in Section 2(a)(11) of the Securities Act.[17]

---

[14] 17 CFR § 230.251(a)(3).

[15] Securities traded on a national securities exchange must be registered with the SEC under Section 12 of the Exchange Act. 15 U.S.C. § 78l. Section 12(b) of the Exchange Act imposes requirements with which national securities exchange must comply in listing securities to trade on their exchanges. Section 12(b) requires the listing exchange to gather specified information about the securities being listed, and about the issuer, such as financial information and information about certain officers, directors and other issuer personnel who hold significant positions in security.

[16] 17 CFR § 230.144. Rule 144 provides a means of complying with Section 4(a)(1) of the Securities Act, which provides a resale exemption for sales of unregistered securities by persons who are not issuers, dealers or underwriters.

[17] 15 U.S.C. § 77b(a)(11). Section 2(a)(11) defines an "underwriter" as:

> any person who has purchased from an issuer with a view to, or offers or sells for an issuer in connection with, the distribution of any security, or participates or has a direct or indirect

3. Complying with Rule 144 takes the reseller out of the definition of underwriter.
4. Criteria for complying with Rule 144 are somewhat different for a non-affiliate versus an affiliate of the issuer of restricted securities.
    a. Non-affiliate criteria vary depending on whether the issuer of the securities is a so-called "reporting issuer" under Section 13 or 15(d) of the Exchange Act.[18]
    b. If a reporting issuer, a non-affiliate holder of restricted securities can resell those securities provided that the issuer, subject to the holding periods described below:
        i. Has available current public information;
        ii. Has filed all required reports under Section 13 or 15(d) of the Exchange Act during the 12 months preceding a sale; and
        iii. Has submitted required data and posted it on its website.
    c. If the issuer meets the preceding requirements, the restricted securities holder can then sell securities without registration, provided that at least six months have elapsed since the later of (i) the date of acquisition of the security from the issuer or its affiliate, and (ii) the date of any resale by the acquirer or any subsequent holder of the securities.
    d. If the issuer has not met the Section 13 or Section 15(d) reporting requirements, then the securities must be held for a period of one year since the later of the date the securities were acquired from the issuer or an affiliate of the issuer.
    e. If the issuer is not, or has not been for a period of 90 days before the sale, subject to reporting requirements under Section 13 or 15(d) of the Exchange Act, the seller would be subject to a one-year holding period under paragraph (d)(ii) of Rule 144.
5. The same holding periods apply to resellers of restricted securities who are affiliates of the issuer:

---

participation in any such undertaking, or participates or has a participation in the direct or indirect underwriting of any such undertaking; but such term shall not include a person whose interest is limited to a commission from an underwriter or dealer not in excess of the usual and customary distributors' or sellers' commission. As used in this paragraph the term ''issuer'' shall include, in addition to an issuer, any person directly or indirectly controlling or controlled by the issuer, or any person under direct or indirect common control with the issuer.

[18] Section 13 of the Exchange Act requires an issuer who has securities registered with the SEC under Section 12 of the Exchange Act to file certain periodic reports with the SEC containing specified information about the issuer and its securities. 15 U.S.C. § 78m. Section 15(d) of the Exchange Act requires an issuer who has securities registered with the Securities Act to file certain information with the SEC as specified in Section 13 of the Exchange Act. 15 U.S.C. § 78o(d).

a. Six-months if the issuer that has reporting obligations under Section 13 or 15(d), and one-year if the issuer does not have such obligations.

b. Securities holders affiliated with the issuer are subject to paragraph (c)(1) of Rule 144, which requires a reporting issuer to have met its reporting obligations during the 12-month period preceding a sale.

c. If the condition is not met, i.e., the issuer has not filed the requisite reports, the affiliate would have prohibited from selling its restricted securities.

6. A holder must sell restricted securities as follows:

   a. A broker's transaction within the meaning of Section 4(a)(4) of the Securities Act;

   b. A transaction directly with a market maker; or

   c. A riskless principal transaction.

7. Seller of restricted security under Rule 144 may not solicit or arrange for the solicitation of orders to buy the securities in anticipation or in connection with the sale. Rule 144 also prohibits the seller from making payments in connection with the sale other than to the broker-dealer executing the sale.

D. Publishing Quotations and Rule 15c2-11

1. Broker-dealers must be able to publish quotations in the securities to help maintain liquid markets.

2. A broker-dealer that is a member of an exchange generally can publish quotations on that exchange.

3. If a security is not registered with the SEC, or is registered, but not listed on an exchange, a broker-dealer nevertheless can publish quotations if it complies with Rule 15c2-11.[19]

4. Quoting under Rule 15c2-11

   a. A broker-dealer may publish quotations with respect to a given, unlisted security in a "quotation medium,"[20] which would include an ATS, only if it has in its records the documents and information that Rule 15c2-11 requires.

---

[19] 17 CFR § 240.15c2-11.

[20] Paragraph (e)(1) of Rule 15c2-11 defines a "quotation medium" as:

> any "interdealer quotation system" or any publication or electronic communications network or other device which is used by brokers or dealers to make known to others their interest in transactions in any security, including offers to buy or sell at a stated price or otherwise, or invitations of offers to buy or sell.

Paragraph (e)(2) of Rule 15c2-11, in turn, defines an "interdealer quotation system" as "any system of general circulation to brokers or dealers which regularly disseminates quotations of identified brokers or dealers."

b. Broker-dealer must obtain information from one of the sources set out in paragraph (a) of Rule 15c2-11 and have a reasonable basis to believe that such information is accurate in all material respects. The information a broker-dealer must obtain under paragraph (a) includes:

i. A prospectus as specified by Section 10(a) of the Securities Act (provided the prospectus is not subject to a stop order that is in effect when the quotation is published or submitted);

ii. A Regulation A offering circular for an issuer that has filed a notification under Regulation A. The issuer must have been authorized to commence offering less than 40 days before the day on which the broker-dealer publishes or submits quotation to a quotation medium;

iii. The report filed under Section 13 or 15(d) or Regulation A, or a copy of the annual statement referred to in Section 12(g);

iv. Information the issuer has published under Rule 12g3-2(b) (foreign private issuers) and that the broker-dealer shall make reasonably available upon request;[21] or

v. Information specified in paragraph (a)(5) of the Rule, including the name of the issuer, name of officers, nature of business, title and class of securities, and number of shares outstanding, among other items. Paragraph (d) of Rule 15c2-11 requires a broker-dealer to submit the information regarding the issuer set out in paragraph (a)(5) at least three days before the quotation is published or submitted.

5. FINRA Rule 6432

a. Requires a broker-dealer submitting or publishing quotations to gather the information set out in Rule 15c2-11.

b. Broker-dealers also must submit Form 211 to FINRA, which contains specified information about the security/issuer for which it intends to submit or publish quotations.

6. Records

a. A broker-dealer must maintain the records regarding its submission or publication of a quotations under paragraph (b) of Rule 15c2-11.

b. Paragraph (c) of Rule 15c2-11 requires a broker-dealer to maintain those records for a period of three years

[21] 17 CFR § 240.12g3-2. Paragraph (b) of Rule 12g3-2 exempts foreign private issuers of securities from registering securities with the SEC under Section 12(g) of the Exchange Act under specified circumstances.

7. Paragraph (f) of Rule 15c2-11 contains exceptions the allow broker-dealers to publish or submit quotations without gathering the information set out in paragraph (a):

    a. (f)(1) - publication or submission of a quotation with respect to a security is not subject to Rule 15c2-11 if the security is admitted to trading on an exchange and trades on the same day as, or on the preceding business day, as the day the quotation is published or submitted.

    b. (f)(2) - publication or submission by a broker-dealer, solely on behalf of a customer, of a quotation that represents the customer's indication of interest and is not solicited by the broker-dealer is not subject to Rule 15c2-11. The quotation cannot consist of both a bid and an offer.

    c. (f)(3) - the publication or submission by a broker-dealer of unsolicited customer interest involving a security that has been subject to quotation in an interdealer quotation system ("IDQS") on at least 12 days within the previous 30 calendar days, with no more than 4 consecutive business days without a quote is exempt from the information-gathering requirements of Rule 15c2-11.

    d. A broker-dealer also can publish or submit a two-sided quotation in an IDQS that is not identified as unsolicited customer interest subject to the preceding conditions.

    E. A market maker[22] that has published or submitted a quotation with respect to a security in an IDQS in reliance on an exception under paragraph (f)(3) of the Rule may continue publish or submit quotations without compliance with Rule 15c2-11 information-gathering requirements until it ceases to act in a market making capacity with respect to the security.

III. TRADING SECURITIES

A. Trading on an Exchange

1. A national securities exchange must register with the SEC under Section 6 of the Exchange Act.
2. The SEC must approve its application for registration filed on Form 1.
3. A national securities exchange's registration application, as well as the SEC's order approving registration, are public and subject to public comment.
4. Members must be broker-dealers.
5. Disclosure of operations

[22] Section 3(a)(38) of the Exchange Act defines a "market maker" as "any specialist permitted to act as a dealer, any dealer acting in the capacity of block positioner, and any dealer who, with respect to a security, holds himself out (by entering quotations in an inter-dealer communications system or otherwise) as being willing to buy and sell such security for his own account on a regular or continuous basis." 15 U.S.C. § 78c(a)(38).

a. Subject to comprehensive rule filing requirements under Section 19(b) of the Exchange Act, requiring both their trading rules as well as details regarding their trading operations to be made public.[23]

b. Any time a national securities exchange seeks to change its rules, it must file a rule amendment with the SEC on Form 19b-4, which, if non-controversial, can become immediately effective upon filing, or otherwise be subject to public comment before SEC approval.

c. The national securities exchange must submit these filings before it can implement any change

d. Exchanges typically submit proposed rule filings to the SEC staff for a review on an informal basis to avoid rejection of a formal rule filing.

6. Listing of Securities

a. Section 12 of the Exchange Act prohibits a security from trading on a national securities exchange unless there is an effective registration with respect to such security for the exchange.[24]

b. Once a security is registered and listed on an exchange, other exchanges may extend unlisted trading privileges to the security pursuant to Section 12(f) of the Exchange Act.[25]

7. Display of Quotations

a. All national securities exchanges make available the best bid, the best offer, and aggregate quotation sizes for each security traded on that exchange for so-called "NMS securities."[26]

b. Must disseminate best bids and best offers (and respective sizes) from all exchanges in the public quote stream.

B. Trading on an ATS

1. Does not have to obtain SEC approval before commencing operations.

2. Rule 301(b) of Regulation ATS requires an entity to register as a broker-dealer and to file Form ATS with the SEC.

3. Broker-dealer registration

a. ATS must file Form BD with the SEC.[27]

---

[23] 15 U.S.C. § 78o.
[24] 15 U.S.C. § 78l.
[25] 15 U.S.C. § 78l(f).
[26] 17 CFR § 242.602.
[27] 17 CFR § 242.301(b). Within 45 days of filing a completed Form BD, the SEC will either grant registration or begin proceedings to determine whether it should deny registration. Typically, the SEC grants registration of a broker-dealer on Form BD within a few days if the form has been properly completed.

b. Broker-dealer must become a member of a self-regulatory organization ("SRO"),[28] typically FINRA.[29]

4. ATS must file a Form ATS with the SEC 20 days before commencing operations as an ATS.[30] Form ATS is not an application and the SEC does not "approve" an alternative trading system before it begins to operate, but the SEC staff will often undertake an informal review of a Form ATS and provide comments, and the ATS will need to address any deficiencies noted by the SEC staff during this informal review

5. Membership - ATS can have both broker-dealer and non-broker-dealer institutional subscribers that directly access the ATS.

6. Disclosure of Operations

   a. ATS has limited disclosure requirements, even to the SEC.[31]

   b. Form ATS is deemed confidential when filed; unless voluntarily provided to the public, the Form ATS is generally not available even to subscribers to the ATS .

   c. Only material changes must be filed with the SEC before implementation;[32] all other changes need to be filed on an amended Form ATS within 30 days after the end of each calendar quarter.[33]

   d. ATS typically submits a material change to the SEC staff for an informal review before submitting it formally. Unlike an exchange, which has to submit all rule changes to the SEC, an ATS only has to submit material changes.

7. Listing of Securities

   a. ATS must satisfy a similar gating function with respect to securities traded on the ATS, but no form "listing" of securities on an ATS.

---

[28] Section 3(a)(26) of the Exchange Act defines "self-regulatory organization" as "any national securities exchange, registered securities association, or registered clearing agency, or (solely for purposes of sections 19(b), 19(c), and 23(b) of this title) the Municipal Securities Rulemaking Board established by section 15B of this title."

[29] Unless a broker-dealer limits its security transactions solely to a national securities exchange of which it is a member, Section 15(b)(8) of the Exchange Act and Rule 15b9-1 thereunder require the broker-dealer to become a member of FINRA.

[30] *See* 17 CFR § 242.301(b)(2)(i).

[31] The SEC has proposed rules to expand the disclosure requirements for ATSs trading an "NMS Stock," which includes any security or class of securities (other than an option) for which transaction reports are collected, processed, and made available pursuant to an effective transaction reporting plan, other than a listed option. *See* Securities Exchange Act Release No. 76474 (Nov. 18, 2015). A security that is traded solely in the over-the-counter market is unlikely to fall within this definition. To date, the SEC has not taken further action on this proposal.

[32] 17 CFR § 242.301(b)(2)(ii).

[33] 17 CFR § 242.301(b)(2)(iii).

b. Rule 15c2-11 requires a broker-dealer wishing to publish any quotation for a security in a "quotation medium" (which includes an ATS) to gather specified information regarding the issuer.[34]

c. Once a broker satisfies the requirements of Rule 15c2-11 and has begun quoting in the subject security, other brokers can "piggyback" on such quotations without having to satisfy the requirements of Rule 15c2-11.[35]

8. Display of Quotations

a. An ATS only has to display its quotations for inclusion in the public quote stream under specified circumstances.

b. An ATS is only required to make its quotations available with respect to NMS stocks.[36]

c. Unless the security on the ATS is also being traded on a national securities exchange, it is unlikely that the ATS would ever have to provide its quotations in such a security to the public quote stream.

d. Even if the security is an NMS stock, trading volume on the ATS would have to cross certain thresholds (five percent or more of the average daily trading volume) with respect to such security for at least four of the preceding six months before the ATS would be required to disseminate its quotation information in the public quote stream.[37]

e. An ATS could decide to remain completely dark (not display its quotations to any person other than an employee of the ATS) and thus not subject to publishing its quotations in the public quote stream.

C. Transaction Processing

1. If a securities transaction is effected on an exchange or ATS, the securities and associated payment must be processed and transferred between the parties. This activity raises potential issues with respect to "clearing agency" and "transfer agent" regulation.

2. Clearing Agency – defined in Section 3(a)(23) of the Exchange Act as any person who, among other things:

a. Acts as an intermediary in making payments or deliveries or both in connection with transactions in securities;

---

[34] 17 CFR § 240.15c2-11.

[35] 17 CFR § 240.15c2-11(f)(3).

[36] 17 CFR § 242.301(b)(3)(i). Rule 300(g) of Regulation ATS provides that that neither a debt security nor a convertible debt security is an NMS stock for purposes of Regulation ATS. 17 CFR § 242.300(g). We do not think that, at least initially, the securities that will trade on the Platform will be NMS securities because they are not likely to be securities for which transaction reports are collected, processed, and made available pursuant to an effective transaction reporting plan.

[37] 17 CFR § 242.301(b)(3)(i)(B).

b. Provides facilities for the comparison of data respecting the terms of settlement of securities transactions;

c. Acts as a custodian of securities in connection with a system for the central handling of securities whereby all securities of a particular class or series of any issuer deposited within the system are treated as fungible and may be transferred, loaned, or pledged by bookkeeping entry without physical delivery of securities certificates; or

d. Otherwise permits or facilitates the settlement of securities without physical delivery of securities certificates.

3. If an exchange or ATS, in addition to executing transactions, also performs a function described above in effecting the transfer of securities and payments between transaction parties, it may be performing the functions of a clearing agency.[38]

4. Transfer Agent

a. Defined in Exchange Act Section 3(a)(25), and includes a person who engages on behalf of an issuer in "transferring record ownership of securities by bookkeeping entry without physical issuance of securities certificates"

b. If an exchange or ATS performs a transfer agent function for issuers, registration as a transfer agent may be required

D. Custody

1. Rule 15c3-3 under the Exchange Act requires a broker-dealer (which includes an ATS) that carries customer accounts to maintain physical possession or control over the securities held in customers' accounts.

2. There is a question as to how a broker-dealer can obtain control over securities held in digitized form on the blockchain.

3. The issue is whether auditors can verify that securities that the broker-dealer holds for its customers exist on the blockchain.

[38] It should be noted that Section 3(a)(23)(B) contains an exception from this definition for, among other entities, brokers and dealers that perform clearing agency-type functions as part of "customary" brokerage or dealing activities.

CHAPTER II
COMMODITY DERIVATIVES LAW ISSUES

Cryptocurrency is subject to regulation under the federal Commodity Exchange Act and Commodity Futures Trading Commission Regulations where it is the product underlying a derivatives contract or in situations the CFTC has jurisdiction over transactions in the cash market for such a product.

I. LISTED VIRTUAL CURRENCY DERIVATIVE CONTRACTS

A. Bitcoin Swaps

1. TeraExchange

On September 11, 2014, TeraExchange, a CFTC-registered swap execution facility ("SEF"), self-certified the first virtual currency derivative to trade on a US registered platform. It was a USD / Bitcoin Non-Deliverable Swap.[1]

2. LedgerX

On September 19, 2017. LedgerX , a CFTC-registered SEF and derivative clearing organization ("DCO") self-certified the first non-cash settled virtual currency derivatives contract in the United States. LedgerX listed for trading US Dollar / Bitcoin options which call for the delivery of Bitcoin.[2] To address price volatility in Bitcoin and protect the financial integrity of its DCO, LedgerX's rules require the party obligated to deliver Bitcoin under the contract to be fully-funded at the time of trade execution.[3]

B. Bitcoin Binary Options

1. North American Derivatives Exchange

On November 26, 2014, the North American Derivatives Exchange ("NADEX") followed by self-certifying Bitcoin Binary Contracts for trading. These contracts were daily and weekly cash-settled binary option contracts based on the Tera Bitcoin Price Index.[4]

2. Cantor Futures Exchange

On December 1, 2017, the Cantor Futures Exchange self-certified for trading cash-settled Bitcoin binary options for one bitcoin listing contracts at the

[1] Available at: https://www.cftc.gov/sites/default/files/filings/ptc/14/09/ptc091114teraexcsef001.pdf
[2] Available at: https://www.cftc.gov/sites/default/files/filings/ptc/17/09/ptc092017lgxsef001.pdf
[3] Id. at 7.
[4] Available at: https://www.cftc.gov/sites/default/files/filings/ptc/14/12/ptc121614nadexdcm001.pdf

beginning of each calendar month which expire at the end of three months. It is cleared by the Cantor DCO, with market participants directly self-clearing their transaction with the DCO. Final settlement is based on an aggregation of cash prices during the last 10 minutes of an expiring contract, "bitcoin price arbitrage matrices and the Exchange's own bids, offers and traded prices." [5]

C. Bitcoin Cash-Settled Futures Contracts

1. CBOE Futures

On December 1, 2017, the CBOE Futures Exchange ("CFE") self- certified Bitcoin futures contracts. The contracts which commenced trading on December 11, 2017, are cash settled based on the auction price of Bitcoin in U.S. Dollars on the Gemini Exchange.[6] The Gemini Exchange is a facility of Gemini Trust Company, LLC, which is regulated by the New York State Department of Financial Services. [7] Each contract is based on one Bitcoin, with the March, June, September and December quarterly expirations along with four near-term expirations weeks and three near-term serial months.[8]

2. CME

Also on December 1, 2017, the Chicago Mercantile Exchange self-certified a cash-settled futures contract on Bitcoin which commenced trading on December 17, 2017. Each contract is for five Bitcoins and is cash-settled to the CME CF Bitcoin Reference Rate (the "BRR") on the last day of trading. At the time of the CME's self-certification, the BRR was based on Bitcoin cash prices on 4 cash virtual currency exchanges: Bitstamp, GDAX, itBit, and Kraken. CME's self-certification notes that these four exchanges "collectively represent up to 35% of the BTC:USD trade globally." The BRR methodology considers prices between 3:00 pm and 4:00 pm London time.

3. Controversy Over Listing Bitcoin Futures

a. Thomas Petterfy, Interactive Brokers: There is No Fundamental Basis for Valuing Bitcoins

In an open letter on November 14, 2017 to CFTC Chairman Giancarlo, Thomas Petterfy, the Chairman of Interactive Brokers, requested the CFTC "require that any clearing organization that wishes to clear any cryptocurrency

[5] Available at: https://www.cftc.gov/sites/default/files/filings/ptc/17/12/ptc120117cfedcm001.pdf
[6] Available at: https://www.cftc.gov/sites/default/files/filings/ptc/17/12/ptc120117cfedcm001.pdf
[7] Id. at 2.
[8] Id. at 9.

or derivative of a cryptocurrency do so in a separate clearing system isolated from other products."[9] Peterffy argued that

> There is no fundamental basis for valuation of Bitcoin and other cryptocurrencies, and they may assume any price from one day to the next. This has been illustrated quite clearly in 2017 as the price of Bitcoin has increased by nearly 1000% [and that margining] such a product in a reasonable manner is impossible. While the buyer (the long side) of a cryptocurrency futures contract or call option could be required to put up 100% of the value to ensure safety, determining the margin requirement for the seller (the short side) is impossible.[10]

Peterffy expressed fear that if "the Chicago Mercantile Exchange or any other clearing organization clears a cryptocurrency together with other products, then a large cryptocurrency price move that destabilizes members that clear cryptocurrencies will destabilize the clearing organization itself." He noted that even clearing firms that chose not to clear cryptocurrency futures and options were still exposed to their unquantifiable risk due to their clearing fund contributions and default waterfall assessment obligations.[11]

b. Walter Lukken, Futures Industry Association: Is the Self-Certification Process Appropriate for Such Novel Futures Contracts?

Following the CFE, CME and Cantor self-certifications, on December 6, 2017, Futures Industry Association President Walt Lukken also wrote to Chairman Giancarlo. Lukken shared the FIA's concerns regarding the launch of bitcoin futures and options. In light of the potential risk to the futures industry clearing infrastructure these products may pose that Peterffy had highlighted, Lukken questioned the use of the self-certification process for such novel products:

> While suited for standardized products, this process does not distinguish for a product's risk profile or unique nature. We believe that this expedited self-certification process for these novel products does not align with the potential risks that underlie their trading and should be reviewed. Given the lack of historical data on these products, it is further concerning to clearing members that they will bear the brunt of the risk associated with them through their guarantee fund contributions

[9] Letter dated Nov. 14, 2017 from Thomas Peterffy to J. Christopher Giancarlo available at: http://online.wsj.com/public/resources/documents/Peterffy_Bitcoin_Letter.pdf
[10] Id.
[11] Id.

> and assessment obligations, even if not participating in these markets directly, rather than the exchanges and clearinghouses who have listed them. A public discussion should have been had on whether a separate guarantee fund for this product was appropriate or whether exchanges put additional capital in front of the clearing member guarantee fund. [12]

Nonetheless, the CFTC took no action to stay the listing of the bitcoin futures and options contracts.

4. CFTC Response to Concerns Expressed by Market Participants

   a. CFTC issued a "CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products." [13] The Backgrounder notes that:

> when an exchange self-certifies a new contract that it must determine that the contract complies with the CEA and Commission regulations, including that the new contract is not readily susceptible to manipulation.[14]
>
> Unless the Commission finds that a new product would violate the CEA or Commission regulations, the DCM may list the new product no sooner than one full business day following the self-certification.[15]

It states that the CFTC "has limited ability to require the DCMs to make changes to their contracts or to require the DCOs to change their approaches to clearing the contracts." In response to calls from many quarters for the clearinghouses clearing bitcoin contracts to establish a separate clearing fund for them to insulate the risks posed by the products from the rest of the clearing ecosystem, the Backgrounder stated: "the Commission does not have the authority to require the DCOs to establish separate clearing systems or guaranty funds to clear these contracts." [16]

Thus, the backgrounder stresses that the CFTC was not "approving" the contracts and says it had limited ability to require the exchanges "to make changes to their contracts."

---

[12] Letter dated Dec. 6, 2017 from Walter Lukken to j. Christopher Giancarlo available at: https://fia.org/articles/open-letter-cftc-chairman-giancarlo-regarding-listing-cryptocurrency-derivatives
[13] CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products (CFTC Dec. 1, 2017) available at: http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/bitcoin_factsheet120117.pdf
[14] Id. at 1.
[15] Id.
[16] Id.

b. CFTC Issues a Second Backgrounder

The CFTC issued an additional backgrounder: "CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets." It describes a five-pronged approach to the CFTC's regulatory approach currencies:

i. Consumer Education. Amidst the wild assertions, bold headlines, and shocking hyperbole, there is a need for greater public understanding.

ii. Asserting Legal Authority. Asserting legal authority over virtual currency derivatives in support of the CFTC's anti-fraud and[17] manipulation efforts, including in underlying spot markets, is a key component in the CFTC's ability to effectively regulate these markets.

iii. Market Intelligence. Gaining the ability to monitor markets for virtual currency derivatives and underlying settlement reference rates through the gathering of trade and counterparty data will provide regulatory and enforcement insights into those markets.

iv. Robust Enforcement. In addition to its general regulatory and enforcement jurisdiction over the virtual currency derivatives markets, the CFTC has jurisdiction to police fraud and manipulation in cash or spot markets. The CFTC intends to continue to exercise this jurisdiction to enforce the law and prosecute fraud, abuse, manipulation or false solicitation in markets for virtual currency derivatives and underlying spot trading.

v. Government-wide Coordination. The CFTC actively coordinates its approach to Bitcoin and other virtual currencies with other Federal regulators, including the Securities and Exchange Commission (SEC), Federal Bureau of Investigation (FBI), Justice Department and Financial Stability Oversight Council (FSOC). The CFTC also coordinates with state entities, including state Attorneys General, in addition to working with the White House, Congress and other policy-makers.[18]

[17] CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets (CFTC Jan. 4, 2018) available at:
http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/backgrounder_virtualcurrency01.pdf
[18] Id. at 1-2.

The Backgrounder states that in the case of the CME and CFE certifications none of the "limited grounds" for the CFTC to "stay" the certifications.[19]

II. CFTC JURISDICTION OVER FRAUDULENT MANIPULATIONS OF THE CASH MARKET FOR VIRTUAL CURRENCIES

In general, the CFTC's jurisdiction has been primarily limited to the derivatives markets. Prior to the amendments made to the CEA by the Dodd Frank Act, the CFTC only had jurisdiction over manipulations of "any commodity in interstate commerce."[20] Dodd Frank expanded that jurisdiction to cover fraud in the cash market, and certain leveraged transactions in cash commodities.[21]

A. Virtual Currencies as "Commodities" Under the CEA

Three CFTC speaking orders declare that Bitcoin is a "commodity" under the CEA's definition of that term, and two of those decisions also declare that other virtual currencies are commodities as well.

The first step in determining whether a virtual currency is a "commodity" and thus subject to the CFTC's jurisdiction is the CEA's definition of the term "commodity." After specifically enumerating some 30 odd agricultural products, the definition of the term "commodity" continues on to include "all goods and services" for tangible products, and then go on to include "all services, rights or interests" for intangible products. To address concerns of overlapping jurisdiction with the US Treasury Department and the Securities and Exchange Commission, the "commodity" definition for intangible products limits the phrase "all rights, interests and services" with the phrase "in which contracts for future delivery are presently or in the future dealt in."[22]

1. *In re Coinflip*

In *In re Coinflip Inc., d/b/a Derivabit, and Francisco Riordan*, CFTC Docket No. 15-29 (Sept. 17, 2015), the CFTC found that the respondents had violated various sections of the CEA and CFTC regulations by providing a trading platform through which users could buy and sell options on Bitcoin without the trading platform being registered as required with the CFTC. Pertinent here, the CFTC wrote:

> Section 1a(9) of the Act defines "commodity" to include, among other things, "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in." 7U.S.C. §1a(9). The definition of a "commodity" is broad. See, e.g., Board of Trade of City of Chicago v. SEC, 677 F.2d 1137,

[19] Id. at 2.
[20] CEA § 9(3); & 7 U.S.C. § 13.
[21] Pub. L. 110-_____; §§ 741 & 753.
[22] CEA § 1a(9); 7 U.S.C. § 1a(9).

> 1142 (7th Cir. 1982). Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.

The CFTC was correct to claim Bitcoin was a "commodity" because at the time, as summarized above, Bitcoin swaps were offered for trading on TeraExchange and Bitcoin binary options were traded on NADEX. In contrast, it is not clear what basis the CFTC had for asserting that "other virtual currencies are encompassed in the definition and properly defined as commodities," as there were (and currently still are) no futures, swaps or options trading on other virtual currencies.

2. *In re TeraExchange*

In re TeraExchange LLC CFTC Docket No. 15-33 (2015) involved a CFTC-registered SEF that arranged for an illegal wash trade in Bitcoin swaps to occur on its trading platform. In a footnote, CFTC stated "Bitcoin is a commodity under Section 1a of the Act . . . and is therefore subject as a commodity to applicable provisions of the Act and Regulations." Bitcoin was plainly a commodity because swaps on Bitcoin were traded on TeraExchange, a registered SEF

3. *In re Bitfinex*

In re BFXNA Inc., d/b/a Bitfinex CFTC Docket No. 16-19 (2016),[23] the CFTC fined Bitfinex for a margin lending program it provided to retail investors which enabled them to trade Bitcoin on margin in violation of Section 2(c)(2)(D) of the CEA which prohibits certain margined transactions in commodities with retail customers.[24] In its legal discussion, the *Bitfinex* order makes the same claim that the CFTC made in *Coinflip*: that Bitcoin and "other virtual currencies" meet the definition of a "commodity" under the CEA.[25] Other than citing its own *Coinflip* speaking order, however, the CFTC again offered no basis for asserting that virtual currencies other than Bitcoin are "commodities" under the CEA.

4. Conclusion: Bitcoin is a "Commodity" – Unclear if Other Virtual Currencies Are Commodities Too

> The reasoning of these three speaking orders seems sound with regard to Bitcoin. There are CFTC-supervised derivatives contracts trading on Bitcoin starting with the Bitcoin swaps listed on TeraExchange in September 2014. It is less plainly evident that the dictum in the Coinflip and Bitfinex cases that other virtual currencies are also "commodities"

[23] Available at: https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfbfxnaorder060216.pdf
[24] 7 U.S.C. § 2(c)(
[25] Id. at 5-6.

as defined in the CEA as there are no futures, options or swaps on such virtual currencies listed at either a SEF or DCM.

B. Fraud in the Cash Market

1. Dodd Frank Adds Section 6(c)(1) to the CEASection 753 of the Dodd Frank Act added Section6(c)(1) to the Commodity Exchange Act which provides:

> Prohibition against manipulation It shall be unlawful for any person, directly or indirectly, to use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance, in contravention of such rules and regulations as the Commission shall promulgate by not later than 1 year after July 21, 2010 . . . . 7 U.S.C. § 9(1) (emphasis in original)

2. CFTC Promulgates Regulation Section 180.1

Pursuant to Section 6(c)(1), the CFTC promulgated Regulation 180.1, [26] which provides:

> It shall be unlawful for any person, directly or indirectly, in connection with any swap, or contract of sale of any commodity in interstate commerce, or contract for future delivery on or subject to the rules of any registered entity, to intentionally or recklessly:
>
> > Use or employ, or attempt to use or employ, any manipulative device, scheme, or artifice to defraud;
> >
> > Make, or attempt to make, any untrue or misleading statement of a material fact or to omit to state a material fact necessary in order to make the statements made not untrue or misleading;

[26] *Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation*, 76 Fed. Reg. 41398 (CFTC July 14, 2011). The rule promulgated essentially mimics the antifraud provisions contained in the Securities Exchange Act of 1934 ("34 Act") and rules thereunder. This is likely no coincidence given the plethora of case law developed under the 34 Act and its implementing regulation that the CFTC would expect courts to rely upon when the CFTC brings an action under its antifraud provisions.

> Engage, or attempt to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person . . . .[27]

3. Legislative History

The legislative history of Section 753 of the Dodd Frank Act which added Section 6(c)(1) to the CEA indicates that Congress's primary intent for giving the CFTC the additional authority provided under the new provision was to combat manipulations.

a. Senator Maria Cantwell in introducing Section 753 stated

> My amendment strengthens the Commodity Futures Trading Commission's authority to go after manipulation and attempted manipulation in the swaps and commodities markets. . . .[28]

b. The comments of the Chair of the Senate Agriculture and Forestry Committee, Senator Blanche Lincoln, echo those of Senator Cantwell:

> Section 753 adds a new anti-manipulation provision to the Commodity Exchange Act (CEA) addressing fraud-based manipulation, including manipulation by false reporting. Importantly, this new enforcement authority being provided to the CFTC supplements, and does not supplant, its existing anti-manipulation authority for other types of manipulative conduct.[29]

c. The CFTC's rulemaking pursuant to Section 6(c)(1) of the CEA, however, seems to have expanded the scope of the conduct prohibited to involve both fraud and manipulation or possibly fraud ***or*** manipulation.[30]

4. CFTC Enforcement Actions: Does CFTC have authority over either fraud ***or*** manipulation in the cash markets?

a. *CFTC v. Hunter Wise Commodities, LLC*[31]

> In what was a precious metals fraud case, the court found that the defendants had "made material misrepresentations and materially

---

[27] 17 C.F.R. § 180.1(a).
[28] 156 Cong. Rec., 111th Cong., No. 67 S3348 (May 6, 2010).
[29] 156 Cong. Rec., 111th Cong., No. 105 S5924 (July 15, 2010) (emphasis added).
[30] [30] *Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation*, 76 Fed. Reg. 41398, 41401 (CFTC July 14, 2011).
[31] 21 F. Supp. 3d 1316 (S.D. Fla. 2014).

misleading omissions with scienter regarding the risk of the commodities transactions, I need only determine whether it did so in connection with the purchase or sale of commodities." Id. at 1347. Accordingly, the Southern District of Florida found that proven accusations of fraud alone could make out a violation of Section 6(c)(1) and Reg 180.1.

b. *CFTC v. Kraft Foods Group, Inc*.[32]

The CFTC's theory that Reg 180.1 prohibits either fraud or manipulation was rejected:

> Based upon the plain language of the [CEA] and Regulation 180.1, along with a comparison of those provisions to the well-established reading of the Securities Exchange Act of 1934, this Court finds that Section 6(c)(1) and Regulation 180.1 prohibit only fraudulent conduct..[33]

5. CFTC's Use of Section 6(c)(1) and Reg 180.1 in Virtual Currency Cases

a. *CFTC v. Gelfman* [34]

On September 21, 2017, the CFTC filed a complaint against Gelfman Blueprint, Inc. and Nicholas Gelfman with operating a Bitcoin Ponzi scheme in violating of Section 6(c)(1) and Reg 180.1 by defrauding customers, misappropriate of customer funds and issuing false account statements. The court, however, addressed the merits of the CFTC's allegations nor the defendants' defenses as the defendants defaulted.

b. *CFTC v. My Big Coin Pay, Inc*.[35]

In *CFTC v. My Big Coin Pay, Inc.*, the CFTC charged the defendants with violating Section 6(c)(1) and Reg 180.1 by selling the virtual currency My Big Coin ("MBC") to customer and misappropriating the customers' money. Defendants moved to dismiss the complaint on March 29, 2018, arguing, among other things, that MBC is not a "commodity" under Section 1a(9) because it is not a "service, right or interest" in which a futures or other derivatives, contract is traded on.[36]

[32], 153 F. Supp. 3d 996 (N.D. Ill 2015).
[33] 153 F.Supp.3d at 1009.
[34] Docket No. 17-7181 (S.D.N.Y. Sept. 21, 1017)
[35] Docket No. 1:18-cv-10077 (RYZ) (D. Mass Jan.24, 2018).
[36] Note that Murphy & McGonigle represents Defendant Randall Crater in that action.

c. *CFTC v. McDonnell*[37]

In *CFTC v. McDonnell*, the CFTC charged the defendants with violating Section 6(c)(1) and Reg 180.1 by running a program (i) providing advice for trading Bitcoin, Litecoin and other virtual currencies, and (ii) providing a managed account in which the defendants traded virtual currency in customers' accounts.

On March 6, 2018, the court granted the CFTC's motion for preliminary injunction over the objections of pro se defendant Patrick McDonnell.[38] The court's reasoning is less than clear. On the one hand, the court concluded that virtual currencies were "commodities" as defined by the CEA, but at the same time acknowledged the futures trading requirement for services, rights or interests to be products to be subject to the CFTC's jurisdiction.

III. LEVERAGE OR MARGIN PROVIDED TO RETAIL PURCHASERS OF VIRTUAL CURRENCY

A. Section 742 of the Dodd Frank added Section 2(c)(2)(D) to the act. It prohibits offering or providing retail customers with margin or leverage to enter into a commodity transaction unless "actual delivery" occurs in 28 days.

B. Legislative History

The Seventh Circuit's decision in *CFTC v. Zelener*,[39] gutted the CFTC's ability to regulate fraud in the retail foreign currency market. Zelener and his companies were offering customer the ability to enter into spot forex transaction with contractual terms that called for delivery in two days. Much of the time, however, the customer was able to offset the contract before delivery and enter a new one. Being able to roll the position forward allowed customers to speculate on foreign currency rates without ever taking delivery and essentially trade a futures contract without the protections provided to retail customers in the regulated futures markets.

The CFTC sued Zelener and his companies on the theory that his business was offering what in reality were unregulated futures contracts. The Seventh Circuit rejected this theory. The panel pointed out that the Commission's proposed analysis depended on *ex post* facts such as what percentage of contracts went to delivery and subjective facts of what the parties' intentions were in entering into the transactions. Accordingly, at the time that any particular contract was entered into it would be unclear whether the contract was a futures or a spot contract: "That would leave people adrift and make it

[37] Docket No. 18-CV-0361 (E.D.N.Y. Jan. 18, 2018),
[38] 2018 WL 1175156.
[39] 373 F.3d 861 (7th Cir. 2004), rehearing en banc denied, 387 F.3d 624 (7th Cir. 2004)

difficult, if not impossible, for dealers (technically futures commission merchants) to know their legal duties in advance."[40]

The hole left in the CFTC's jurisdiction to combat retail forex fraud was plugged by Congress with the 2018 Farm Bill[41] which added Section 2(c)(2)(c) to the CEA. That provision expressly gave the CFTC jurisdiction over retail foreign currency trading. This prompted fraudsters to simply move onto to other commodities with Zelener-like contracts.

Section 742 was meant to fix this problem. Senator Blanche Lincoln explained,

> Section 742, the Dodd Frank provision which added Section 2(c)(2)(D), to the Act was meant to extend the Farm Bill's "Zelener fraud fix" to retail off-exchange transactions in all commodities. Further, a transaction with a retail customer that meets the leverage and other requirements set forth in Section 742 is subject not only to the anti-fraud provisions of CEA Section 4b (which is the case for foreign currency), but also to the on-exchange trading requirement of CEA Section 4(a), "as if" the transaction was a futures contract.[42]

C. Application of Section 2(c)(2)(D) to the Virtual Currency Cash Market

In re BFXNA Inc., d/b/a Bitfinex CFTC Docket No. 16-19 (2016), the CFTC fined Bitfinex for a margin lending program it provided to retail investors which enabled them to trade Bitcoin on margin in violation of Section 2(c)(2)(D) of the CEA. When customers bought Bitcoin on margin through Bitfinex's margin lending program, they were delivered to Bitfinex's omnibus settlement wallet:

> Bitfinex [only] released them, following satisfaction of the Financing Recipient's outstanding loan. Bitfinex considered bitcoins held in the omnibus wallet to belong to the Financing Recipients, but subject to a lien in the amount of any outstanding loan plus fees owed to the Margin Funding Provider.

Later, Bitfinex changed its settlement process to deliver the Bitcoins bought on margin to a multi-signature wallet operated by a third-party firm which placed the Bitcoins into individually enumerated wallets for each customer. Bitfinex retained control though over the wallets.

Bitfinex again changed its settlement procedure so that the Bitcoins bought on margin were delivered to individually enumerated wallets run by Bitfinex but Bitfinex retained control over the wallets by holding the private keys.

The CFTC thought none of these three different settlement procedures resulted in "actual delivery" under 2(c)(2)(D). The CFTC explained:

---

[40] *Zelener*, 373 F.3d at 866.
[41] Food, Conservation and Energy Act of 2008, Public Law 110-246, 122 Stat. 1651 (2008).
[42] 156 Cong. Rec. at S5,924 (daily ed. July 15, 2010) (statement of Sen. Lincoln).

Thus, physical delivery of the entire quantity of the commodity, including the portion purchased using leverage, margin or financing, into the possession of the buyer, or a depository other than the seller, the seller's parent company, partners, agents and affiliates will satisfy the actual delivery exception, provided that the purported delivery is not a sham. By contrast, actual delivery will not have occurred if only a "book entry" is made by the seller purporting to show that delivery of the commodity has been made.

D. CFTC's Proposed Interpretation of "Actual Delivery" in the Context of Virtual Currency Transactions

On December 20, 2017, the CFTC issued a proposed interpretation of "actual delivery" in the context of virtual currency transactions.[43] Its proposed interpretative guidance offered two examples where "actual delivery" would be deemed to occur, and two examples where it would not.

Actual delivery occurs where, within 28 days, the full amount of virtual currency purchased, including that purchased on margin, is delivered to the wallet, and the seller retains no interest in or control over the virtual currency.

Actual delivery occurs where, within 28 days, the full amount is transferred to a depository other than one affiliated with the seller, and no interest or control in the virtual currency.

Actual delivery will not occur, if within 28 days, a book entry is made by the seller showing delivery but has not delivered the virtual currency in keepings scenario one or two.

Actual delivery will not have occurred if, within 28 days of entering into a transaction, the agreement, contract, or transaction for the purchase or sale of virtual currency is rolled, offset against, netted out, or settled in cash or virtual currency (other than the purchased virtual currency) between the buyer and the seller (or persons acting in concert with the seller).

[43] *Retail Commodity Transactions Involving Virtual Currency*, 82 Fed. Reg. 60335 (CFTC Dec. 20, 2017)

CHAPTER III
FEDERAL AND STATE BANKING LAW AND REGULATION

I. OCC'S PROPOSED "FINTECH" CHARTER

A. Administrative Proceedings

1. Exploring Special Purpose National Bank Charters for Fintech Companies (December 2016).[1] White paper proposing grant of "special purpose" bank charters pursuant to 12 F.F.R. § 5.20(e)(1) to fintech companies in order to "advance important policy objectives, such as enhancing the ways in which financial services are provided in the 21st century, while ensuring that new fintech banks operate in a safe and sound manner, support their communities, promote financial inclusion, and protect customers."
2. Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies (March 15, 2017).[2] Concluding that it is "in the public interest" for the OCC to grant non-depository special purpose bank charters to financial technology companies.
3. Evaluating Charter Applications from Financial Technology Companies (March 15, 2017).[3] Draft supplement to OCC licensing manual describing the process through which financial technology companies may apply for a special purpose bank charter.

B. Judicial Challenges

1. Conference of State Bank Supervisors v. Office of the Comptroller of the Currency, 1:17-cv-00763-JEB (D.D.C. April 26, 2017)

    a. Association of state banking regulators challenges the OCC's constitutional, statutory, and regulatory authority to grant non-depository special purpose bank charters.

    b. OCC's motion to dismiss the action is still pending.

2. *Vullo v. Office of the Comptroller of the Currency*, 1:17-cv-03574-NRB (S.D.N.Y. 2017)

---

[1] *Available at* https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf

[2] *Available at* https://www.occ.gov/topics/responsible-innovation/summary-explanatory-statement-fintech-charters.pdf

[3] *Available at* https://www.occ.treas.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf

a. New York State Department of Financial Services (DFS) challenges the OCC's constitutional, statutory, and regulatory authority to grant non-depository special purpose bank charters.

b. On December 12, 2017, the federal district court dismissed DFS's action without prejudice, holding that the claim was not ripe for adjudication because the OCC had not taken any actions towards granting a fintech charter.[4]

C. To date, the OCC has not accepted any applications for a Fintech Charter.

II. FINCEN REGULATIONS

A. Interpretive Guidance

1. FIN-2013-G001 (March 18, 2013)[5]

a. Interpretive guidance issued to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.[6]

b. Defined "virtual currency" as "a medium of exchange that operates like currency in some environments, but does not have all the attributes of real currency[7] [and] [i]n particular … legal tender status in any jurisdiction."

c. Applies to "convertible" virtual currency, which either has (i) an equivalent value in real currency; or (ii) acts as a substitute for real currency.

d. Clarified the following:

i. A *user* of virtual currency is not a money service business ("MSB") under FinCEN's regulations and is therefore not subject to MSB registration, reporting, and recordkeeping requirements.[8] "User" is defined as "a person that obtains virtual currency to purchase goods or services."

[4] *Available at* https://www.scribd.com/document/367024626/Vullo-v-Office-of-the-Comptroller-Order-granting-OCC-motion-to-dismiss

[5] *Available at* https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[6] FinCEN regulations are codified in the Code of Federal Regulations, Title 31, Chapter X, Part 1010.

[7] FinCEN regulations define "real" currency as "the coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance." 31 C.F.R. § 1010.100(m).

[8] The term "MSB" also does not include (i) a bank or foreign bank; or (ii) a person registered with, and functionally regulated or examined by, the Securities and Exchange Commission ("SEC") or the CFTC, or a foreign financial agency that engages in financial activities that, if conducted in the United States, would require the foreign financial agency to be registered with the SEC or CFTC. 31 C.F.R. §1010.100(ff)(8)(i)–(iii).

ii. An *administrator* or *exchanger* is a MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. "Administrator" is defined as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency." "Exchanger" is defined as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency."

2. FinCEN regulations provide that whether a person is a money transmitter is a matter of fact and circumstance, and further provide that the term "money transmitter" shall not include a person that only:

   a. Provides the delivery, communication, or network access services used by a money transmitter to support money transmission services;

   b. Acts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller;

   c. Operates a clearance and settlement system or otherwise acts as an intermediary solely between BSA regulated institutions;

   d. Physically transports currency, other monetary instruments, other commercial paper, or other value that substitutes for currency as a person primarily engaged in such business, such as an armored car, from one person to the same person at another location or to an account belonging to the same person at a financial institution, provided that the person engaged in physical transportation has no more than a custodial interest in the currency, other monetary instruments, other commercial paper, or other value at any point during the transportation;

   e. Provides prepaid access; or

   f. Accepts and transmits funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds.[9]

[9] *See* 31 CFR § 1010.100(ff)(5)(ii)(A)-(F).

3. FinCEN guidance indicates that the definition of "money transmitter" also excludes any person, such as a futures commission merchant, that is registered with, or regulated and examined by, the CFTC.[10]

III. ADMINISTRATIVE RULINGS[11]

A. FIN-2014-R001 (January 30, 2014)[12] - Stated that, to the extent a user creates or "mines" a convertible virtual currency solely for a user's own purposes, the user is not a money transmitter under the BSA.

B. FIN-2014-R002 (January 30, 2014)[13]- Stated that a company purchasing and selling convertible virtual currency as an investment exclusively for the company's benefit is not a money transmitter under the BSA.

C. FIN-2014-R007 (April 29, 2014)[14] - Clarified that a company renting computer systems to third parties for use to obtain convertible virtual currency is not a money transmitter under the BSA.

D. FIN-2014-R011 (October 27, 2014)[15] - Stated that setting up a trading and booking platform for virtual currencies would subject a company to FinCEN regulations as a MSB.

E. FIN-2014-R012 (October 27, 2014)[16] - Stated that a company would be considered a money transmitter if it accepted customers' credit card payments and then transferred the payments to merchants in virtual currencies.

F. FIN-2015-R001 (August 14, 2015)[17] - Stated that a company is subject to the BSA where it (i) provided Internet-based brokerage services between buyers and sellers of precious metals; (ii) bought and sold precious metals on its own account; and (iii) held precious metals in custody, opened a digital wallet, and issued digital proof of custody certificates evidencing ownership of such metals.

---

[10] See Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and other Commodities, FIN-2008-G008 (Sept. 10, 2008).

[11] Publication of an administrative ruling on FinCEN's website indicates that the administrative ruling is a regulatory interpretation valid for any situation that fits the description of the facts and circumstances as contained in the ruling. *See FinCEN Publishes Two Rulings on Virtual Currency Miners and Investors* (Jan. 30, 2014), *available at* https://www.fincen.gov/sites/default/files/news_release/20140130.pdf.

[12] *Available at* https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R001.pdf

[13] *Available at* https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R002.pdf

[14] *Available at* https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R007.pdf

[15] *Available at* https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf

[16] *Available at* https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf

[17] *Available at* https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2015-R001.pdf

IV. FINCEN CIVIL ENFORCEMENT ACTIONS

A. Ripple Labs Inc. (May 5, 2015)[18]

FinCEN, working in conjunction with the U.S. Attorney's Office for the Northern District of California, assessed a $700,000 civil monetary penalty against Ripple Labs Inc. and its wholly-owned subsidiary, XRP II, LLC (formerly known as XRP Fund II, LLC) for willfully violating several requirements of the Bank Secrecy Act (BSA) by (i) acting as a MSB and selling its virtual currency, known as XRP, without registering with FinCEN; and (ii) by failing to implement and maintain an adequate anti-money laundering ("AML") program designed to protect its products from use by money launderers or terrorist financiers.

B. BTC-e a/k/a Canton Business Corporation (July 26, 2017)[19]

FinCEN, working in conjunction with the U.S. Attorney's Office for the Northern District of California, assessed a $110,003,314 civil monetary penalty against BTC-e, a foreign digital currency exchange, and a $12 million penalty against one of its operators, a Russian national, for willfully violating U.S. AML laws by (i) failing to obtain required information from customers beyond a username, password, and email address; (ii) allowing money laundering to openly take place on its exchange; and (iii) processing transactions involving funds stolen between 2011 and 2014 from one of the world's largest bitcoin exchanges, Mt. Gox (BTC-e processed over 300,000 bitcoin in transactions traceable to the theft).

C. Letter Pertaining to ICOs[20]

In a February 13, 2018 letter to U.S. Senator Ron Wyden, FinCEN's assistant secretary for legislative affairs, Drew Maloney, explained that both developers and exchanges involved in the sale of an ICO-derived token would be liable to register as a money transmitter and comply with the relevant statutes around AML and KYC rules.

V. STATE MONEY TRANSMITTER LAWS FOR VIRTUAL CURRENCY

State	Money Transmitter Laws	Pending Legislation
Alabama	Requires a license to transmit "virtual currencies." Ala. Code § 8-7A-2(8).	None

[18] See FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger (May 5, 2015), available at https://www.fincen.gov/sites/default/files/2016-08/20150505.pdf

[19] See FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales (July 26, 2017), available at https://www.fincen.gov/sites/default/files/2017-07/BTC-e%20July%2026%20Press%20Release%20FINAL1.pdf

[20] *Available at* https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf

State	Money Transmitter Laws	Pending Legislation
Alaska	None	Proposes to require the licensing of virtual currency transmission. H.B. 180, 30th Legislature, First Sess. (introduced Mar. 14, 2017).
Arizona	Recognizes the validity and enforceability of "smart contracts" on the "blockchain" as electronic signatures and records. Ariz. Rev. Stat. § 44-7061. Prohibits the use of blockchain firearm tracking. Ariz. Rev. Stat. § 13-3122.	Proposes reclassifying crowdfunding and ICOs under state law regarding securities, with exemptions for certain intrastate offerings. N.B. 2601, 53rd Legislature, 2nd Reg. Sess. (introduced Feb. 6, 2018).
Arkansas	None	None
California	Prohibits the purchase of raffle tickets with cryptocurrency. Cal. Penal Code § 320.6.	Introduced legislation to require anyone involved in a "virtual currency business" in the state to first register with California's Commissioner of Business Oversight. A.B. 1123, California Legislature, 2017–2018 Reg. Sess. introduced on Feb. 17, 2017).
Colorado	None	None
Connecticut	Requires the licensing of virtual currency storage and transmission. Conn. Gen. Stat. § 36a-598.	Proposed act concerning the uniform regulation of virtual currency businesses. H.B. 5496, Connecticut General Assembly, February Sess., 2018 (introduced on Mar. 7, 2018).
Delaware	Authorizes the use of blockchain for corporate record storage and stock trading. Del. Code tit. 8, §§ 219, 224, 232.	None
Florida	Prohibits the laundering of virtual currency. Fla. Stat. § 896.101.	Introduced legislation to recognize the validity and enforceability of "smart contracts" on the "blockchain" as electronic signatures and records. H.B. 1357, Reg. Sess. 2018 (filed Jan. 8, 2018).

State	Money Transmitter Laws	Pending Legislation
Georgia	Requires a license to transmit "virtual currencies." Ga. Code § 7-1-680(26). Authorizes virtual currency transmission regulations to encourage economic development. Ga. Code § 7-1-690(b)(1).	None
Hawaii	Requires a license and fiat reserves equal to value of virtual currency held. Hawaii Division of Financial Institutions Application.	Proposes to exempt virtual currency transmission from licensing requirements. S.B. 949, 29th Legislative Sess. (introduced Mar. 24, 2017). Proposes working group to examine blockchain technology. H.B. 1481, 29th Legislative Sess. (introduced Jan. 25, 2017). Proposed act concerning the uniform regulation of virtual currency businesses. S.B. 2129, 29th Legislative Sess. (introduced Jan. 19, 2018).
Idaho	Exempts the sale of virtual currency via Bitcoin ATMs from licensing. Idaho Dep't of Finance, No Action Letter (Oct. 10, 2014). Requires the licensing of the brokering of virtual currency sales. Idaho Dep't of Finance, No Action Letter (July 26, 2016).	None
Illinois	Exempts the exchange of "digital currencies" from "money transmission" licensing requirements. Illinois Dep't of Financial and Professional Regulation, *Digital Currency Regulatory Guidance*.	None
Indiana	None	None
Iowa	None	None
Kansas	Exempts the exchange of "virtual currencies" from "money transmission"	None

State	Money Transmitter Laws	Pending Legislation
	licensing requirements. Kansas Office the State Bank Commissioner, *Guidance Document* MT 2014-01 (June 6, 2014).	
Kentucky	None	None
Louisiana	None	None
Maine	None	None
Maryland	Advises the sale and exchange of virtual currency is money transmission and should be federally regulated as a money service business. Maryland Comm'r of Financial Regulation, Advisory Notice 14-01 (Apr. 24, 2014).	None
Massachusetts	Exempts Bitcoin ATMs from "financial institution" and bitcoins from foreign currency transmission regulations. Mass. Division of Banks, Opinion 14-004 (May 12, 2014).	None
Michigan	Exempts virtual currency from sales tax and requires that retailers instantly convert the value of the virtual currency to USD as of the day and the exact time of the transaction. Mich. Dep't of Treasury, Tax Policy Division, Treasury Update (Nov. 2015).	None
Minnesota	None	None
Mississippi	None	None
Missouri	Exempts Bitcoin ATM transactions from sales tax. Missouri Dep't of Revenue, LR 7411, *Collection of Sales Tax on Bitcoin Transfers Through an Automated Teller Machine (ATM)*, (Sept. 12, 2014).	None
Montana	Authorizes political candidates to accept Bitcoin contributions. Mont. Admin. R. § 44.11.408.	None

State	Money Transmitter Laws	Pending Legislation
	Montana also invests in Bitcoin mining. Office of Governor Steve Bullock, *Governor Bullock Announces $1.1 Million to Help Main Street Businesses Create Jobs, Train Employees, and Plan for Growth*.	
Nebraska	Attorneys may (i) accept digital currencies as payment for legal services so long as they immediately convert it to fiat currency; (ii) receive digital currencies as payment from third-party payors so long as the payment prevents possible interference with the attorney's independent relationship with the client and the attorney implements KYC procedures within the transaction; and (iii) may receive and hold digital currencies in trust or escrow so long as certain conditions are met. *See* Nebraska Ethics Advisory Opinion for Lawyers, No. 17-03 (Sept. 11, 2017).	Proposed act that would penalize those who knowingly commit illegal acts using cryptocurrency. L.B. 691, 105th Legislature, Second Sess. (introduced Jan. 3, 2018). Proposed bill that would prohibit cities and counties from taxing or regulating distributed ledger technology. L.B. 694, 105th Legislature, Second Sess. (introduced Jan. 3, 2018). Proposed bill that would make smart contracts enforceable. L.B. 695, 105th Legislature, Second Sess. (introduced Jan. 3, 2018). Proposed act concerning the uniform regulation of virtual currency businesses. L.B. 987, 105th Legislature, Second Sess. (introduced Jan. 11, 2018).
Nevada	Prohibits local governments (counties and cities) from taxing "blockchain" use and recognizes blockchain as an "electronic record" for evidentiary purposes in judicial proceedings. Nev. Rev. Stat. SB 398, § 6.	None
New Hampshire	Exempts the exchange of "virtual currencies" from "money transmission" licensing requirements. N.H. Rev. Stat. § 399-G:3	None

State	Money Transmitter Laws	Pending Legislation
New Jersey	Virtual currency is treated as intangible property and is subject to sales tax. See Technical Advisory Memorandum, N.J. Division of Taxation, Convertible Virtual Currency (TAM – 2015-1(R)) (July 28, 2015).]	Proposed act that would authorize executors, agents, guardians, or trustees, under certain circumstances, to manage electronic records – including virtual currencies – of decedents, principals, incapacitated persons, or trust creators. A.B. 344, State of New Jersey Assembly, 217th Legislature (introduced Mar. 7, 2016).
New York	Requires a license to engage in any Virtual Currency Business Activity. N.Y. Comp. Codes R. & Regs. tit. 23, § 200.3.	Proposed bill that relates to (i) allowing signatures, records and contracts secured through blockchain technology to be considered in an electronic form and to be an electronic record and signature; and (ii) allows smart contracts to exist in commerce. A.B. 8780, State of New York Assembly, 2017–2018 Reg. Sess. (introduced Nov. 27, 2017). Proposed bill to direct the state board of elections to study and evaluate the use of blockchain technology to protect voter records and election results. A.B. 8792, State of New York Assembly, 2017–2018 Reg. Sess. (introduced Nov. 27, 2017). Proposed bill related to establishing a task force to study and report on the potential implementation of blockchain technology in state record keeping, information storage, and service delivery. A.B. 8793, State of New York Assembly, 2017–2018 Reg. Sess. (introduced Nov. 27, 2017).

State	Money Transmitter Laws	Pending Legislation
		Proposed bill to create a digital currency task force to provide the governor and the legislature with information on the potential effects of the widespread implementation of digital currencies on financial markets in the state. A.B. 8783, State of New York Assembly, 2017–2018 Reg. Sess. (introduced Nov. 27, 2017).
North Carolina	Requires virtual currency transmitters to obtain a license and additional insurance. N.C. Gen. Stat. § 53-208.41, *et seq.*	None
North Dakota	None	None
Ohio	Prohibits the use of Bitcoin to purchase alcohol. *See* Janet H. Cho, *Cleveland Heights Merchants Banking on Bitcoin to Draw Global Spotlight; Skeptics Warn of Risks* (Apr. 24, 2014).	None
Oklahoma	Subordinates the rights of merchants accepting Bitcoin to the rights of any security interest in the Bitcoin (traditional money transfers are free and clear of any security interest). Okla. Stat. § 1-9-332.	None
Oregon	None	None
Pennsylvania	None	None
Rhode Island	None	None
South Carolina	None	None
South Dakota	None	None
Tennessee	Exempts the exchange of "virtual currencies" from "money transmission" licensing requirements. Tenn. Dep't of Financial Institutions, *Regulatory*	None

State	Money Transmitter Laws	Pending Legislation
	Treatment of Virtual Currencies under the Tennessee Money Transmitter Act (Dec. 16, 2015).	
Texas	Exempts the exchange of "virtual currencies" from "money transmission" licensing requirements. Tex. Dep't of Banking, Supervisory Memorandum 1037, Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act (Apr. 3, 2014).	Proposed constitutional amendment that would protect the right to own and use digital currencies. H.J.R 89, 85th Leg., Reg. Sess. (Tx. 2017).
Utah	None	Studying whether to accept virtual currencies for tax payments. H.C.R. 6., 2015 General Sess. (Feb. 26, 2015).
Vermont	Requires virtual currency transmitters to obtain a license. Vt. Stat. tit. 8, § 2500, *et seq.* Allows blockchain transactions to be authenticated like any other business record for evidentiary purposes in judicial proceedings. Vt. Stat. tit. 12, § 1913.	None
Virginia	Requires virtual currency transmitters to obtain a license. Va. Code § 6.2-1900.	None
Washington	Requires virtual currency transmitters to obtain a license, maintain fiat reserves equal to value of virtual currency held, and third-party auditing. Wash. Rev. Code § 19.230.010, et seq.	None
West Virginia	Prohibits the laundering of cryptocurrencies. W. Va. Code § 61-15-1, et seq.	None
Wisconsin	Prohibits virtual currency transmitters from obtaining a license. State of Wisconsin Dep't of Financial Institutions, *available at* https://www.wdfi.org/fi/lfs/soc/.	None

State	Money Transmitter Laws	Pending Legislation
	Exempts the sale of the virtual currency from sales tax, but requires payment of sales and use tax on the use of virtual currency as consideration for goods or services. Wisconsin Dep't of Revenue, *Sales and Use Tax Report* (Mar. 2014).	
Wyoming	Requires virtual currency transmitters to obtain a license, WY Money Transmitter License, and maintain fiat reserves equal to value of virtual currency held. Wyo. Stat. § 40-22-107. Exempts those who develop, sell, or facilitate the exchange of open blockchain tokens from specified securities and money transmission laws. H.B. 70, 64th Legislature, 2018 Budget Sess. (Signed into law on Mar. 7, 2018).	Proposed bill that would exempt virtual currencies from Wyoming's money transmitter laws. H.B. 19, 64th Legislature, 2018 Budget Sess. (introduced on Feb. 13, 2018). Proposed "blockchain records bill" that would modify Wyoming's Business Corporations Act to allow for blockchain-based records storage, shareholder management, and shareholder votes. H.B. 101, 64th Legislature, 2018 Budget Sess. (introduced on Feb. 14, 2018). Proposed act that would allow allows for the creation of "series LLCs," a LLC structure is favorable towards decentralized protocols, as it enables LLCs to establish a compartmentalized series of members/managers, transferable interests or assets, and distributions to members. H.B. 126, 64th Legislature, 2018 Budget Sess. (introduced on Feb. 14, 2018). Proposal to amend the Wyoming Statues to create a property tax exemption for cryptocurrencies. S.F. 111, 64th Legislature, 2018 Budget Sess. (introduced on Feb. 16, 2018).

VI. DFS BITLICENSE; NYS-CHARTERED VIRTUAL CURRENCY FIRMS

A. DFS BitLicense

1. Background. The New York State Department of Financial Services ("DFS") established a comprehensive regulatory framework for virtual currency businesses called "BitLicense" that requires operations related to transactions involving any form of virtual currency to obtain a license from the state.[21]

2. Key Definitions

   a. "Virtual currency" means "any type of digital unit that is used as a medium of exchange or a form of digitally stored value [and] shall be broadly construed to include digital units of exchange that

      i. have a centralized repository or administrator;

      ii. are decentralized and have no centralized repository or administrator; or

      iii. may be created or obtained by computing or manufacturing effort." 23 NYCRR § 202.2(p).

   b. Definition of Virtual Currency Provides Three Exceptions. Virtual currency shall <u>not</u> be construed to include any of the following:

      i. Digital units that (i) are used solely within online gaming platforms, (ii) have no market or application outside those gaming platforms, (iii) cannot be converted into, or redeemed for, Fiat Currency or Virtual Currency, and (iv) may or may not be redeemable for real-world goods, services, discounts, or purchases;

      ii. Digital units that can be redeemed for goods, services, discounts, or purchases as part of a customer affinity or rewards program with the issuer and/or other designated merchants or can be redeemed for digital units in another customer affinity or rewards program, but cannot be converted into, or redeemed for, Fiat Currency or Virtual Currency; or

      iii. Digital units used as part of Prepaid Cards" (emphasis added).[22]

[21] BitLicense is codified in Title 23, Chapter I, Part 200 of the New York Codes, Rules and Regulations. 23 NYCRR § 200.2

[22] Id.

c. "Virtual currency business activity" means "the conduct of any one of the following types of activities involving New York or a New York resident:

   i. Receiving virtual currency for transmission or transmitting virtual currency;

   ii. Storing, holding, or maintaining custody or control of virtual currency on behalf of others;

   iii. Buying and selling virtual currency as a customer business;

   iv. Performing exchange services as a customer business; or

   v. Controlling, administering, or issuing a virtual currency." [23]

d. Exceptions to "virtual currency business activity" are"

   i. Receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency; and

   ii. The development and dissemination of software in and of itself.[24]

3. License Requirement[25]

   a. "No person shall, without a license … engage in any virtual currency business activity." [26]

   b. Exemptions:

      i. Persons that are chartered under the New York Banking Law and are approved by the superintendent to engage in virtual currency business activity; and

      ii. Merchants and consumers that utilize virtual currency solely for the purchase or sale of goods or services for investment purposes.

4. Out-of-State Businesses.[27] Out-of-state businesses are required to obtain a BitLicense to obtain if they engage in virtual currency business activity involving New York State or persons that reside, are located, have a place of business, or are

[23] 23 NYCRR § 202.2(q).
[24] See id.
[25] 23 NYCRR § 200.3
[26] 23 NYCRR § 202.3(a).
[27] 23 NYCRR § 202.3(c)(1)–(2).

conducting business in New York. *See* New York State Department of Financial Services.[28]

5. Other Statutory Requirements. BitLicense regulations also require licensees to, *inter alia*, maintain certain minimum standards and programs to help ensure customer protection, cyber-security and anti-money laundering compliance. *See generally* NYCRR §§ 202.15–202.16 & 200.19.

6. Current BitLicense Licensees

7. Circle Internet Financial (9/22/2015)

   a. XRP II, LLC, an Affiliate of Ripple (6/13/2016)

   b. Coinbase, Inc. (1/17/2017)

   c. Bitflyer USA, Inc. (11/28/2017)

B. NYS-Chartered Virtual Currency Limited Trust Companies

1. itBit Trust Company, LLC (5/7/2015)

2. Gemini Trust Company, LLC (10/5/2015)

3. Note: These charters were granted pursuant to Chapter 2 of the New York Consolidated Laws (*i.e.*, N.Y. Banking Law). The Authorization Certificates do not provide any further specificity.[29]

VII. ULC UNIFORM REGULATION OF VIRTUAL-CURRENCY BUSINESSES ACT

A. Background. The Uniform Law Commission released its final version of the Uniform Regulation of Virtual-Currency Businesses Act (the "URVCBA") on October 9, 2017. The stated purpose of the URVCBA is to regulate virtual currency business activity, and the act provides a licensing and regulatory framework for businesses whose products and services include:

1. The exchange of virtual currencies;

2. The transfer of virtual currencies from one person to another; or

[28]BitLicense Frequently Asked Questions *Available at* http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework_faq.htm

[29] itBit Trust Company LLC's Authorization Certificate from NYS can be accessed here: http://www.dfs.ny.gov/banking/auth_cert_itBit_052015.pdf

3. Certain custodial or fiduciary services in which the property or asset under the custodian's control are considered "virtual currency."

B. To date, no state has adopted the URVCBA, but the following three states have introduced legislation adopting a version of it:

1. Connecticut (H.B. 5496, introduced on 3/7/2018);

2. Hawaii (S.B. 2129, introduced on 1/19/2018); and

3. Nebraska (L.B. 987, introduced on 1/11/2018).

C. Key Definitions

1. "Virtual currency," as defined in § 102(23), is "a digital representation of value that (1) is used as a medium of exchange, unit of account, or store of value; and (2) is not legal tender" (which is defined as government-issued coin or paper money in § 102(8)).

2. Expressly excluded from the definition of virtual currency are:

a. Transactions involving merchant rewards programs, if the value of the reward cannot be exchanged for legal tender, bank credit, or virtual currency; and

b. Digital representations of value issued by a publisher and used solely within an online game or game platform.

3. "Virtual-currency business activity," as defined in § 102(25), means "exchanging, transferring, or storing virtual currency or engaging in virtual-currency administration, whether directly or through an agreement with a virtual-currency control-services vendor." The definition of "virtual-currency business activity" turns on whether the activity involves one of the following four verbs—control, exchange, store, and transfer (*i.e.*, if the person or entity controls, exchanges, stores, or transfers virtual currency, then the URVCBA will apply, unless there is an applicable exemption).

4. "Control" is defined in § 102(3)(A) as "the power to execute unilaterally or prevent indefinitely a virtual-currency transaction."

5. "Exchange" is defined in § 102(5) as "to assume control of virtual currency from or on behalf of a resident, at least momentarily, to sell, trade, or convert: (A) virtual currency for legal tender, bank credit, or for one or more forms or virtual currency; or (B) legal tender or bank credit for one of more forms of virtual currency."

6. "Store" is defined in § 102(20) as "to maintain control of virtual currency on behalf of a resident by a person other than the resident, similar to safe deposit business."

7. "Transfer" is defined in § 102(21) as "to assume control of virtual currency from or on behalf of a resident to (A) credit the virtual currency to the account of another person; (B) move the virtual currency from one account of a resident to another account of the same resident; or (C) relinquish control of virtual currency to another person."

D. Three-Factor Test. The ULC outlines the following three-factor test for determining whether a transaction is subject to the URVCBA:

1. Does the transaction involve "virtual currency" as defined in § 102?

2. Does the transaction involve "virtual-currency business activity" as defined in § 102?

3. If the first two factors are met, is the transaction subject to any of the exemptions listed in § 103?

E. Exemptions. The URVCBA expressly states that it does not apply to the exchange, transfer, or storage of virtual currency to the extent that the activity is governed by the Electronic Funds Transfer Act of 1978, 15 U.S.C. §§ 1693 through 1693r, the Securities Exchange Act of 1934, 15 U.S.C. §§ 78a through 78oo, the Commodities Exchange Act of 1936, 7 U.S.C. §§ 1 through 27f, or the state's applicable blue-sky laws. *See* § 103(b). In § 103(b)(1)–(14), the URVSBA also provides that the act does not apply to activity by:

1. The United States, a state, political subdivision of a state, agency or instrumentality of federal, state, or local government, or a foreign government or a subdivision, department, agency or instrumentality of a foreign government;

2. A bank;

3. A person engaged in money transmission that (A) holds a license under [insert citation to money-services or money-transmission statute of this state]; (B) is authorized by the department to engage in virtual-currency business activity; and (C) complies with [Articles] 2, 3, 5, and 6;

4. A person whose participation in a payment system is limited to providing processing, clearing, or performing settlement services solely for transactions between or among persons that are exempt from the licensing or registration requirements of this [act];

5. A person engaged in the business of dealing in foreign exchange to the extent the person's activity meets the definition in 31 C.F.R. Section 1010.605(f)(1)(iv) [as amended];

6. A person that (A) contributes only connectivity software or computing power to a decentralized virtual currency, or to a protocol governing transfer of the digital representation of value; (B) provides only data storage or security services for a business engaged in virtual-currency business activity and does not otherwise engage in virtual-currency business activity on behalf of another person; or (C) provides only to a person otherwise exempt from this [act] virtual currency as one or more enterprise solutions used solely among each other and has no agreement or relationship with a resident that is an end-user of virtual currency;

7. A person using virtual currency, including creating, investing, buying or selling, or obtaining virtual currency as payment for the purchase or sale of goods or services, solely: (A) on its own behalf; (B) for personal, family, or household purposes; or (C) for academic purposes;

8. A person whose virtual-currency business activity with or on behalf of residents is reasonably expected to be valued, in the aggregate, on an annual basis at $5,000 or less, measured by the U.S. Dollar equivalent of virtual currency;

9. An attorney to the extent of providing escrow services to a resident;

10. A title insurance company to the extent of providing escrow services to a resident;

11. A securities intermediary, as defined in [insert citation to U.C.C. Section 8-102 of this state], or a commodity intermediary, as defined in [insert citation to U.C.C. 9-102 of this state], that: (A) does not engage in the ordinary course of business in virtual-currency business activity with or on behalf of a resident in addition to maintaining securities accounts or commodities accounts and is regulated as a securities intermediary or commodity intermediary under federal law, law of this state other than this [act], or law of another state; and (B) affords a resident protections comparable to those set forth in Section 502;

12. A secured creditor under [insert citation to U.C.C. Article 9 of any state] or creditor with a judicial lien or lien arising by operation of law on collateral that is virtual currency, if the virtual-currency business activity of the creditor is limited to enforcement of the security interest in compliance with [insert citation to U.C.C. Article 9 of any state] or lien in compliance with the law applicable to the lien;

13. A virtual-currency control-services vendor; or

14. A person that (A) does not receive compensation from a resident for: (i) providing virtual-currency products or services; or (ii) conducting virtual currency business activity; or (B) is engaged in testing products or services with the person's own funds. (c) The department may determine that a person or class of persons, given facts particular to the person or class, should be exempt from this [act], whether the

person or class is covered by requirements imposed under federal law on a money-service business.

15. Lastly, § 103(c) provides that "[t]he department may determine that a person or class of persons, given facts particular to the person or class, should be exempt from this [act], whether the person or class is covered by requirements imposed under federal law on a money-service business."

F. Licensing and Registration Requirements. The URVCBA provides that a person may not engage in virtual-currency business activity, or hold itself out as being able to engage in virtual-currency business activity, with or on behalf of a resident unless the person is:

1. Licensed in this state by the department under § 202 ["License by Application"];

2. Licensed in another state to conduct virtual-currency business activity by a state with which this state has a reciprocity agreement and has qualified under § 203 ["License by Reciprocity"];

3. Registered with the department and operating in compliance with § 207 ["Registration In Lieu of License"]; or

4. Exempt from licensure or registration by § 103(b) or (c).

G. The URVCBA also imposes a myriad of recordkeeping and reporting requirements including, *inter alia*:

1. Keeping records of each transaction for five years;

2. Making extensive disclosures to residents using licensees' or registrants' products and services;

3. Creating and maintaining policies related to cybersecurity, business continuity, and AML, among other things.

CHAPTER IV
LITIGATION

I. REGULATORY ENFORCEMENT ACTIONS

A. Securities and Exchange Commission

1. In the matter of Bitcoin Investment Trust and SecondMarket, Inc., Admin. Proceeding No. 3-17335 (SEC July 11, 2016)

   a. Respondent: BIT is a private Delaware trust whose sole assets are bitcoin. SecondMarket is headquartered in New York and is a wholly-owned subsidiary of Digital Currency Group, Inc. SecondMarket is BIT's sole Authorized Participant.

   b. Allegations: BIT continuously offered shares to accredited investors under Rule 506(c). BIT later implemented a shareholder redemption program, which violated Reg M.

   c. Theory: BIT shares are securities under Section 2(a)(1) of the Securities Act and Section 3(a)(10) of the Exchange Act and are an investment contract under *Howey*. The offering constitutes a Reg M "distribution" due to its magnitude and the special selling efforts and methods used to facilitate the distribution. The restricted period was continuous.

   d. Settlement: Cease and desist from violation Reg M Rules 101 and 102; SecondMarket to pay disgorgement of $53,755. The Commission considered Respondents' reliance on counsel. Respondents neither admit nor deny the allegations.

2. *In the matter of Voorhees*, Admin. Proceeding No. 3-15902 (SEC June 3, 2014)

   a. Respondent: Voorhees is a U.S. Citizen. He controlled two corporations, FeedZeBirds and SatoshiDICE.

   b. Allegations: Voorhees offered unregistered offerings of shares in FeedZeBirds and SatoshiDICE. The shares were sold for bitcoin. Voorhees later bought back SatoshiDICE shares at a premium to their market value on the MPEx exchange on which they were trading as well as a premium to the price per share in the original offering.

   c. Theory: the offered shares were securities. Voorhees failed to register the offerings and no exemption applied.

   d. Settlement: cease-and-desist from violations of 5(a) and 5(c) of the Securities Act; undertake not to offer any unregistered securities in exchange for virtual currencies for five years; pay $15,843 in disgorgement; pay a civil monetary penalty of $35,000.

3. In *the matter of Munchee, Inc.,* Admin. Proceeding 3-18304 (SEC Dec. 11, 2017)

a. Respondent: Privately-owned Delaware corporation based in San Francisco that launched an iPhone app for reviewing meals

b. Allegations: Munchee offered and sold digital tokens (called "MUN") to be issued on a blockchain. Munchee accepted Bitcoin and ether. MUN would be sold on secondary markets. MUN tokens were securities, but Munchee failed to register its ICO. It shut down its offering after being contacted by the SEC and returned any proceeds it had received.

c. Theory: MUN tokens are "investment contracts" under *Howey* and the DAO Report. A purchaser of MUN 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.

d. Settlement: cease and desist from causing any future violations of Sections 5(a) and (c) of the Securities Act.

4. *In the matter of BTC Trading, Corp. and Ethan Burnside*, Admin. Proceeding 3-16307 (SEC Dec. 8, 2014)

a. Respondent: Burnside lives in California. BTC Trading Corp. is a Belize corporation and the alter ego of Burnside.

b. Allegations: Respondents operated unregistered, online, virtual currency-denominated securities exchanges and broker-dealers. Registered accountholders could buy, sell, and trade securities of businesses listed on the Respondents' websites using Bitcoin and Litecoin. The exchanges held users' funds. Users could not exchange virtual currency for fiat on the exchanges. The exchanges were not registered and were therefore in violation of Section 5 of the Exchange Act. Burnside also offered shares in unregistered transactions in exchange for bitcoins and litecoins. Burnside would down operations when contacted by the SEC. Burnside's failure to register his offerings violated Section 5 of the Securities Act.

c. Theory: The exchanges gave users the ability to create and list initial and secondary securities offerings in exchange for a flat listing fee. Users could also invest and trade in any listed security. The exchanges used a non-discretionary system to match and execute trades. The exchanges were therefore "exchanges" under Section 3(a)(1) of the Exchange Act and Exchange Act Rule 3b-16. Burnside and BTC Trading violated Section 15(a)(1) of the Exchange Act by acting as unregistered broker-dealers by soliciting the public to open accounts, which led to transaction-based compensation for Burnside (through BTC Trading). Finally, Burnside failed to register his offering of shares in two companies, which were securities, violating Sections 5(a) and (c) of the Securities Act.

d. Settlement: Respondent fully cooperated and wound down his operations. Respondents agreed to cease-and-desist from violating Section 5(a) and (c) of the Securities Act and Sections 5 and 15(a) of the Exchange Act; Burnside is barred from associating with any broker-dealer, prohibited from serving as an officer or director of a registered investment company, and barred from participating in any offering of a penny stock, with a right to apply for reentry after 2 years. Burnside to pay disgorgement of $58,387 and a civil monetary penalty of $10,000. Burnside admitted the findings of the Order.

5. *SEC v. AriseBank, Jared Rice Sr., and Stanley Ford*, 18-cv-186 (N.D.Tex. Jan. 25, 2018)

   a. Defendants: AriseBank is an unincorporated entity with its PPB in Texas. Rice, 29, is a resident of Texas. Ford, 45, purports to reside in Dubai, but also resides in Texas.

   b. Allegations: AriseBank claims to be the first decentralized bank, offering consumer-banking products and services and supporting more than 700 virtual currencies. AriseBank, through the individual defendants, offered securities in the form of tokens in an unregistered ICO. And AriseBank made false and misleading statements in connection with its ICO.

   c. Theory: each investment offered and sold was an investment contract and therefore a security as defined in the Securities Act and Exchange Act.

   d. Status: TRO granted; briefing motion for preliminary injunction

6. *SEC v. PlexCorps, Dominic LaCroix and Sabrina Paradis-Royer*, 17-cv-7007 (E.D.N.Y. Dec. 1, 2017)

   a. Defendants: PlexCorps is an unincorporated entity. LaCroix resides in Canada. Paradis-Royer resides in Canada.

   b. Allegations: PlexCorps, through the individual defendants, offered securities in the form of tokens in an unregistered ICO. And PlexCorps made false and misleading statements in connection with its ICO.

   c. Theory: each investment offered and sold was an investment contract and therefore a security as defined in the Securities Act and Exchange Act. Defendants appear to be challenging the SEC's jurisdiction over them.

   d. Status: TRO granted; Preliminary injunction granted; jurisdictional discovery ongoing

7. *SEC v. Renwick Haddow, Bar Works Inc., Bar Works, 7th Avenue, Inc., and Bitcoin Store, Inc.*, 17-cv-4950 (S.D.N.Y. June 30, 2017)

   a. Defendants: Haddow is a U.K. citizen residing in New York. Bar Works is a Delaware corporation with its PPB in New York. 7th Avenue is a New York

corporation. Bitcoin Store is a Delaware corporation with its PPB in New York.

b. Allegations: Haddow created an unregistered broker-dealer called InCrowd Equity, Inc. Using InCrowd, Haddow sold securities in Bitcoin Store, a purported platform for customers to hold and trade Bitcoin, and sold securities in Bar Works. The offering contained false and misleading statements. The SEC alleges violations of 17(a) and 10(b) and Rule 10b-5, 15(a).

c. Theory: standard securities fraud

d. Status: TRO granted; Defendants exception Haddow found in default; no answer yet from Haddow

8. *SEC v. Shavers and Bitcoin Savings and Trust*, 13-cv-00416 (E.D.Tex. July 23, 2013)

a. Defendants: Shavers, 30, resides in Texas. BitCoin Savings and Trust is an unincorporated entity with no physical presence.

b. Allegations: fraudulent offers and sales of securities by Shavers and Bitcoin Savings and Trust, a Bitcoin-denominated Ponzi scheme. The offering was not registered either.

c. Theory: the investments offered by Shavers constitute securities under the Securities Act and the Exchange Act.

d. Status: TRO granted; SEC won summary judgment, a permanent injunction, disgorgement of 180,819 bitcoins, and a civil penalty of $300,000.

e. Key ruling on subject matter jurisdiction: Magistrate Judge found that the investments meet the definition of investment contracts and are therefore securities.

9. *SEC v. Garza, Gaw Miners LLC and ZenMiner LLC d/b/a Zen Cloud*, 15-cv-1760 (D. Conn. Dec. 1, 2015)

a. Defendants: Garza, 30, lives in Vermont and Connecticut. GAW Miners, LLC and ZenMiner are Delaware LLCs with a PPB in Connecticut.

b. Allegations: Defendants sold to over 10,000 investors investment contracts representing shares in the profits they claimed would be generated from using their purported computing power to mine for virtual currency. The shares were securities, but the offering was not registered. Defendants made false and misleading statements in connection with its offering. SEC alleges violation of 10b-5, 17(a), and 5(a) and (c).

c. Theory: the investments offered constituted securities under the Securities Act and the Exchange Act.

d. Status: settled for permanent injunction from further violations; barred from further security offerings; disgorgement of $9,182,000; and interest of $742,774.

10. *SEC v. Montroll and Bitfunder*, 18-cv-1582 (S.D.N.Y. Feb. 21, 2018)

    a. Defendants: Montroll, 37, resides in Texas. Bitfunder is an unincorporated entity.

    b. Allegations: Bitfunder is an unregistered bitcoin-denominated securities exchange that defrauded investors by misappropriating funds and failing to disclose a hack. Montroll also sold unregistered securities that purported to be investments in the exchange.

    c. Theory: the investments offered constituted securities under the Securities Act and the Exchange Act.

    d. Status: awaiting responsive pleading

11. *SEC v. RECoin, DRC World, Inc., and Zaslavskiy*, 17-cv-5725 (E.D.N.Y. Sept. 29, 2017)

    a. Defendants are Maksim Zaslavsky and two companies owned by Zaslavsky, REcoin Group Foundation LLC and DRC World, Inc.

    b. Allegations: fraud and misstatements in connection with an ICO

    c. Theory: tokens are securities under the Securities Act and the Exchange Act

    d. Status: stayed pending criminal action

B. Commodity Futures Trading Commission

1. *In the matter of: BFXNA Inc. d/b/a Bitfinex*, CFTC Docket No. 16-19 (CFTC June 2, 2016)

    a. Respondent: Bitfinex is an online cryptocurrency exchange formed in BVI with a PPB in Hong Kong

    b. Allegations: violations of CEA 6(c) and (d). Bitfinex permitted users to trade bitcoins on margin without being registered with the CFTC. Bitfinex also held margin-purchased bitcoin in wallets that it controlled, failing to deliver them to the purchasers.

    c. Theory: Bitcoin and virtual currencies are commodities. In re Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29, 2015 WL 5535736 (CFTC Sept. 17, 2015). Many users on the exchange were not ECPs and Bitfinex provided margin trading, providing jurisdiction under § 2(c)(2)(D) of the Act. Bitfinex's accounting for customer interests in the bitcoin held in an omnibus settlement wallet did not constitute "actual delivery." There is therefore no applicable exception to the CFTC's jurisdiction. Bitfinex failed to register.

d. Settlement: $75,000 civil monetary penalty; C&D from further violations; does not admit or deny the allegations

2. *In the matter of Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan*, CFTC Docket No. 15-29 (CFTC Sept. 17, 2015)

   a. Respondent: Coinflip is a Delaware corporation with a PPB in San Francisco that is not registered with the CFTC. Riordan is the CEO and controlling person of Coinflip. Coinflip operated the Derivabit platform.

   b. Allegations: Derivabit is an online facility offering to connect buyer and sellers of Bitcoin options contracts. Respondents violated § § 4c(b) and 5h(a)(1) of the Act and Commission Regulations 32.2 and 37.3(a)(1) by conducting activity related to commodity options and by operating a facility for the trading of swaps without being registered as a swap execution facility or designated contract market.

   c. Theory: Virtual currencies are commodities under Section 1a(9) of the Act. Derivabit facilitated the trading of options and swaps on its platform without registering with the CFTC. Riordan is liable as Coinflip's control person.

   d. Settlement: cease and desist from further violations of Sections 4c(b) and 5h(a)(1) of the Act.

3. *CFTC v. Gelfman Blueprint, Inc. and Nicholas Gelfman*, 17-cv-7181 (S.D.N.Y. Sept. 21, 2017)

   a. Defendants: Gelfman is resident in Brooklyn and is the CEO and Head Trader of GBI. GBI is a New York corporation.

   b. Allegations: Gelfman and GBI operated a Bitcoin Ponzi scheme in which they fraudulently solicited participation in a pooled fund that purportedly employed a high-frequency, algorithmic trading strategy to trade Bitcoin. The strategy and reports were fake and the payouts to certain investors came from funds misappropriated from other investors. Gelfman staged a hack to conceal the scheme, but in fact stole virtually all of the $600,000 raised from investors. CFTC alleges fraud under Section 6(c)(1) of the Act

   c. Theory: Bitcoin and other virtual currencies are commodities under Section 1a(9) of the Act.

   d. Status: GBI defaulted; the parties are discussing settlement, but there is an ongoing criminal action: New York v. Nicholas Gelfman, Case No. 2017NY049091 (N.Y. Crim. Ct. N.Y. County).

4. *CFTC v. CabbageTech, Corp. d/b/a Coin Drop Markets and Patrick K. McDonnell*, 18-cv-0361 (E.D.N.Y. Jan. 1, 2018)

   a. Defendants: McDonnell is a New York resident. CabbageTech is a New York corporation.

b. Allegations: Defendants operated a deceptive and fraudulent virtual currency scheme to induce customers to send money and virtual currencies to Defendants in exchange for purported virtual currency trading advice concerning the trading of virtual currencies, including Bitcoin and Litecoin, and for virtual currency purchases and trading on behalf of customers. After obtaining funds, Defendants misappropriated them and stopped communicating with customers. CFTC alleges fraud under 6(c)(1) of the Act.

c. Theory: The CFTC argued that it had jurisdiction over all virtual currencies.

d. Important ruling: The court agreed with the CFTC, finding that the CFTC has jurisdiction over virtual currencies.

5. *CFTC v. My Big Coin Pay, Inc., Randall Crater and Mark Gillespie*, 18-cv-10077 (D. Mass. Jan. 16, 2018)

   a. Defendants: My Big Coin Pay, Inc. is a Nevada corporation. Crater is a New York resident. Gillespie is a Michigan resident.

   b. Allegations: fraudulent offering the virtual currency My Big Coin ("MBC"). Defendants told customers that MBC was backed by gold and any payouts were in fact misappropriated funds from other customers. The CFTC alleges fraud under 6(c)(1) of the Act.

   c. Theory: virtual currencies are commodities under the CFTC's purview

   d. Status: The court granted a TRO. Gillespie is in default. Motion to dismiss pending.

6. *CFTC v. The Entrepreneurs Headquarters Limited and Dillon Michael Dean*, 18-cv-00345 (E.D.N.Y. Jan. 18, 2018)

   a. Defendants: "TEH" is an England and Wales company. Dean is the sole founder, principal, director, and officer of TEH. His last known residence is in Colorado.

   b. Allegations: Dean, through "TEH", fraudulently solicited $1.1M in Bitcoin from the public for participation in a pooled investment vehicle for trading commodity interests. Rather than convert customers' Bitcoin to fiat and invest in binary options contracts, as promised, Defendants misappropriated customers' funds and lied to customers about their account balances. Defendants lied about a hack to conceal the scheme. CFTC brings claims for fraud under 4c(b) of the Act, 4o(1)(A)-(B) of the Act, and for failure to register as a CPO and AP of a CPO.

   c. Theory: bitcoin is a virtual currency, which is a commodity; the scheme purported to involve trading options contracts.

   d. Status: Answer due March 20.

C. U.S. Treasury's Financial Crimes Enforcement Network ("FinCEN")

1. *In the Matter of Ripple Labs Inc. and XRP II, LLC*, No. 2015-05 (FinCEN May 5, 2015)

    a. Violation of BSA for failure to register as a money services business and failure to implement AML

    b. Settlement: $700,000 civil monetary penalty

D. Federal Trade Commission

1. *FTC v. DLuca et al.*, 18-cv-60379 (S.D. Fl. February 20, 2018)

    a. Violation of Section 5(a) of the FTC Act in connection with purported money-making schemes involving cryptocurrencies including "Bitcoin Funding Team," "My7Network," and "Jetcoin." They were pyramid schemes.

II. STATES CEASE AND DESIST ACTIONS: FRAUDULENT OFFERINGS AND REGISTRATION FAILURES

A. Texas

1. Balanced Energy, LLC
2. BitConnect
3. LeadInvest
4. DavorCoin

B. North Carolina

1. BitConnect

C. South Carolina

1. Swiss Gold Global Inc. and Genesis Mining, Ltd. (registration violations only)

D. Massachusetts

1. Caviar (registration violations only)

III. CRIMINAL PROSECUTIONS

A. Federal Prosecutions

1. *BTC-E a/k/a Canton Business Corp. and Vinnik*, CR 16-00227 (N.D. Cal. Jan. 17, 2017): money laundering and unlicensed money service business
2. *Montroll*, 18-Mag-1372 (S.D.N.Y.)- perjury and obstruction of justice for false testimony to the SEC in connection with a hack of bitcoin
3. *Homero Joshua Garza*, 17-cr-158 (D. Conn. July 20, 2017)
4. *Haddow*, 17-Mag-4939 (S.D.N.Y. June 29, 2017)- wire fraud (see SEC action above)

5. *Liberty Reserve and individuals*, 13-cr-368 (S.D.N.Y. May 28, 2013)- money laundering (calling Liberty Reserve "the financial hub of the cyber-crime world")
6. *Mansy and TV Toyz, LLC*, 15-cr-198 (D. Me. Nov. 17, 2015)- failure to register a money transmitting business
7. *Zaslavskiy*, 17-cr-647 (E.D.N.Y. Nov. 21, 2017)- criminal securities fraud; see RECoin above

B. New York

1. Gelfman (see CFTC action above)

IV. PRIVATE CIVIL LITIGATION

A. DDOS attack

1. *Clark v. Payward d/b/a Kraken*, 17-cv-1623 (M.D. Fl. July 5, 2017) - case stayed pending arbitration
    a. Individual account holders bring a fraud suit against Kraken, a large crypto exchange
    b. Kraken suffered a DDoS attack that robotically forced the liquidation of the plaintiffs' margin trading accounts

B. Unregistered securities

1. *Rensel v. Centra Tech*, 17-cv-24500 (S.D. Fl. Dec. 13, 2017) - class action
2. *Balestra v. ATBCoin*, 17-cv-10001 (S.D.N.Y. Dec. 21, 2017) - class action
3. *GGCC, LLC v. Tezos*, 17-cv-6779 (N.D. Cal. Nov. 26, 2017) - class action
4. *Davy v. Paragon Coin*, 18-cv-671 (N.D. Cal. Jan. 30, 2018) - class action

C. Fraudulent offering

1. *Hodges v. Monkey Capital*, 17-cv-81370 (S.D. Fl. Dec. 19, 2017) - class action
2. *Dookeran v. Xunlei*, 18-cv-467 (S.D.N.Y. Jan. 18, 2018) - class action
3. *Greenawalt v. Riot Blockchain, Inc*., 18-cv-440 (D. Co. Feb. 22, 2018)
4. *Baker v. Tezos*, CGC-17-562144 (Sup. Ct. Cal. San Francisco Oct. 25, 2017) - class action

D. Stock manipulation

1. *Blais v. The Crypto Co*., 18-cv-1072 (C.D. Cal. Feb. 7, 2018)- derivative complaint

E. Misappropriation of funds

1. Liu v. Project Investors, Inc. d/b/a Cryptsy, (S.D. Fl. Jan. 13, 2016) - class action
2. *Faasse v. Coinbase*, 18-cv-1382 (N.D. Cal. Mar. 2, 2018) - class action

F. Breach of contract

1. *R3 v. Ripple*, 655781/2017 (Court of Chancery Del. Oct. 30, 2017)- failure to execute R3's options contract

G. Unfair trade practices

1. *Berk v. Coinbase*, 18-cv-1364 (N.D. Cal. Mar. 1, 2018)- class action; Coinbase allegedly tipped off certain exchange customers about the listing of BCH when bitcoin forked

CHAPTER V
CYBERSECURITY

I. OVERALL TAKEAWAYS

A. Cybersecurity rules for cryptocurrency and blockchain-related entities will vary depending on (i) the nature of the business activity, (ii) the services, if any, provided to customers, and (iii) the legal status of any cryptocurrencies involved in the entities' business model. Failure to follow applicable cybersecurity rules can result in regulatory enforcement actions, customer lawsuits, and reputational harm.

B. For example, entities that hold or exchange cryptocurrency on behalf of customers will need to focus on protecting the cryptocurrency in their possession from theft and their computer systems from disruption or sabotage. They will also need to protect the confidentiality of any personal and financial information they collect from their customers.

C. In general, as a best practice and to manage cybersecurity-related legal, financial, and reputational risks, entities dealing in cryptocurrency and blockchain technology should seriously consider adopting comprehensive cybersecurity compliance programs. At a minimum, these programs should address the following:

1. *Cybersecurity Risk Assessments and Testing*. What kinds of valuable data or assets does the entity maintain or possess? What are the entity's vulnerabilities, both external and internal? Is the entity keeping up with the latest cyber threats and intelligence? Is the entity testing its systems and procedures for vulnerabilities?

2. *Data and System Safeguards*. Entities should take reasonable measures to safeguard any valuable data that they possess, including trade secrets, business plans, and any personal and financial information that they possess for their customers or employees. Entities should protect any cryptocurrency in their possession from theft and their computer systems from disruption. Any safeguards adopted should be tailored to the entity's cybersecurity risk profile, the size of the entity, the nature of the entity's business, and the specific threats facing the entity.

3. *Access Controls.* Implement access controls for the entity's computer systems. Restrict access to confidential and sensitive information on those systems to only those employees and third-party vendors who need access in connection with their work for the entity. Consider using two-factor authentication and VPN services for remote connections to the entity's network. Enforce strong password policies and require employees to routinely change passwords.

4. *Data Encryption*. When feasible, encrypt customer and other sensitive data both in storage and in transit. Securely destroy customer data when there is no longer a business or legal need to retain it.

5. *Network Monitoring*. To the extent feasible, monitor networks and systems for suspicious activity. Maintain network logs and audit trails for a reasonable period of time.

6. *Backups and Contingency Plans*. Maintain backups of transaction information and sensitive data. Have contingency plans in place in the event that internal or external computer systems and networks are unavailable.

7. *Employee Training*. Provide regular cybersecurity training to staff. Ensure that any staff responsible for cybersecurity at the entity keep up to date on the latest threats and technology.

8. *Software Updates*. Promptly implement updates and patches for known software vulnerabilities and for system security software.

9. *Senior Management Engagement*. Designate someone in senior management to be responsible for the entity's cybersecurity compliance program. Ensure that regular reports on cybersecurity are provided to senior management and the board.

10. *Manage Third-Party Cybersecurity Risks*. Entities should understand whether any third-party vendors have access to their sensitive data and systems. Entities should also seek to mitigate any risks posed by third-party vendors by conducting audits and by contractually requiring vendors to safeguard the data they possess on behalf of the entity.

11. *Incident Response Plans*. Be prepared to respond quickly and appropriately to any cybersecurity incidents, including by notifying senior management and appropriate personnel immediately of the breach, retaining external counsel and appropriate cybersecurity vendors, if necessary, to investigate and remediate the breach, and promptly make required or voluntary disclosures to regulators, customers, investors, and law enforcement. If critical computer systems or networks are disrupted in an attack, or critical data is lost or held ransom, be prepared to quickly implement contingency and business continuity plans. Conduct tabletop exercises to ensure that staff understand their roles and responsibilities in the event of a breach.

D. Further, entities should ensure that any public statements or representations to customers about the steps they take to protect their computer networks, assets, and customer data are accurate. Regulators routinely sanction companies that misrepresent the level of data protection they provide to their customers.

II. SIGNIFICANT CYBERSECURITY INCIDENTS INVOLVING CRYPTOCURRENCIES AND BLOCKCHAIN

A. To date, significant cybersecurity incidents have focused almost largely on the theft or misappropriation of cryptocurrency. Major incidents include the following:

1. Mt. Gox (2011 – 2014). Mt. Gox was a bitcoin exchange based in Japan that, at one time, handled at least 70 percent of all bitcoin transactions worldwide. In early 2014, Mt. Gox filed for bankruptcy after an unknown attacker allegedly stole bitcoins that were worth, at the time of the bankruptcy, hundreds of millions of dollars. Although the attacker has never been identified, in 2017, the DOJ indicted a Russian national named Alexander Vinnik for allegedly helping to launder a significant portion of the bitcoin stolen from Mt. Gox.[1] Vinnik was arrested in Greece and faces extradition to the United States. Mt. Gox itself allegedly had inadequate security and internal controls and Mark Karpeles, the former CEO of Mt. Gox, was arrested in Japan in 2015 and charged with manipulating financial records of Mt. Gox and embezzling certain funds related to the exchange. He has denied the charges.

2. The DAO (2016). The DAO was intended to be an example of an autonomous organization in which participants would vote on the types of investments to be made by the organization and would then be entitled to a share of the profits from those investments. Between April and May of 2016, the DAO held an ICO in which investors could purchase DAO tokens in exchange for Ether cryptocurrency, raising at least $168 million. However, less than a month after the DAO ICO was closed, an unknown attacker allegedly exploited a flaw in the DAO's code to drain approximately 3.6 million Ether from the DAO to a blockchain address controlled by the attacker. One month later, the Ethereum network agreed to create a "hard fork" in the Ethereum blockchain that allowed the stolen Ether to be credited to the DAO as if nothing had happened.

3. Coincheck (2018). In January 2018, unknown hackers allegedly stole hundreds of millions of dollars in XEM tokens from Coincheck, a cryptocurrency exchange in Japan. Coincheck has agreed to pay up to $420 million to users whose XEM tokens were stolen. Coincheck, which is slowly resuming operations, is under investigation by Japan's Financial Services Agency over its data security safeguards and is the subject of a lawsuit in Japan.

B. As the cryptocurrency and blockchain industry matures, and as entities in this space begin to provide a wider array of services to customers or incorporate blockchain technology into more traditional business models, blockchain entities may become attractive to hackers not just for the cryptocurrency they hold, but also for their customer data or to disrupt the operation of financial markets.

   1. For example, cryptocurrency entities that hold a "BitLicense" from the New York Department of Financial Services are required to maintain anti-money laundering programs and collect identifying information for their customers – information that could be stolen by external or internal bad actors if not properly protected.

[1] *See United States v. Vinnik*, 16 Cr. 227 (N.D. Cal.).

III. APPLICABLE CYBERSECURITY LAWS

A. The cybersecurity rules that apply to a cryptocurrency or blockchain entity will depend on the nature of the business and how the cryptocurrency associated with the entity is classified under the law. For example, if the cryptocurrency is a "security," cybersecurity rules applicable to the securities industry may apply.

B. Federal Trade Commission

1. Section 5(a) of Federal Trade Commission Act (FTC Act) (15 U.S.C § 45(a)): Prohibits "unfair" or "deceptive" acts or practices, which the FTC has applied to businesses in situations in which either (i) the business has failed to adequately protect customer information or (ii) the business has falsely or deceptively promised customers that it has adopted certain data protection measures when, in fact, it has not.

    a. Section 5(a) of the FTC Act is the closest the U.S. has to a national data protection and data privacy law. Section 5(a) gives the FTC enforcement authority over a wide range of business activity affecting commerce in the United States.

    b. In determining whether a data protection practice is appropriate, the FTC seeks to determine whether data protection practices are reasonable: "From the outset, the FTC has recognized that there is no such thing as perfect security, and that security is a continuing process of detecting risks and adjusting one's security program and defenses. For that reason, the touchstone of the FTC's approach to data security has been reasonableness—that is, a company's data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors. Moreover, the FTC's cases focus on whether the company has undertaken a reasonable process to secure data."[2]

2. Many states have "mini-FTC acts" that contain similar provisions to the FTC Act and are used by state attorneys general and state agencies to enforce data protection standards by entities.

C. Banking Law

1. Title V of the Gramm-Leach-Bliley Act (GLB Act) (15 U.S.C. § 6801 et seq.): Requires financial institutions to protect the privacy of confidential customer information and to notify customers of their privacy policies and practices at least annually – and to allow customers to opt-out of disclosures of customer information to unaffiliated third parties in certain circumstances. Grants rulemaking and enforcement authority to agencies such as the SEC, CFTC, CFPB, and FTC with respect to financial institutions under their jurisdiction. For example, the SEC has the authority to enact and enforce rules

[2] *The NIST Cybersecurity Framework and the FTC,* FTC Business Blog (Aug. 31, 2016).

related to the GLB Act with respect to broker-dealers, investment companies, and investment advisers.

2. Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681 et seq.): Requires businesses that use consumer credit information to take certain steps to safeguard and ensure the accuracy of consumer credit information.

D. Securities and Securities Market Rules

1. SEC Regulation S-P (17 C.F.R. § 248.1 et seq.): Regulation S-P implements the privacy and customer data protection requirements of the GLB Act and the FCRA. With respect to data security, Regulation S-P requires broker-dealers, investment advisers, and investment companies to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. Among other things, the policies must be "reasonably" designed to (i) insure the security and confidentiality of customer information; (ii) protect against anticipated threats to the security and integrity of the customer information; and (iii) protect against unauthorized access to the use of customer records or information that could result in "substantial harm or inconvenience" to the customer.[3] Regulated entities are further required to take "reasonable measures" to securely dispose of customer credit and consumer reports.[4]

2. SEC Regulation S-ID (17 C.F.R. § 248.201): Requires broker-dealers, investment advisers, and investment companies to adopt written identity-theft prevention programs that are designed to detect, prevent, and mitigate identity theft in connection with customer brokerage accounts and other accounts covered under the regulation. Such programs must be appropriate to the size and complexity of the broker-dealer and the nature and scope of its activities, including reasonable policies and procedures to detect and respond to any identity theft red flags.[5]

3. SEC Rule 15c3-5 (17 C.F.R. § 240.15c3-5): Requires broker-dealers with market access to establish written risk management controls that are reasonably designed to manage the financial, regulatory, and other risks associated with market access.[6]

4. SEC Regulation SCI (17 C.F.R. § 242.1000 et seq.): Requires exchanges, alternate trading systems, and self-regulatory organizations (referred to as "SCI Entities") to adopt written policies and procedures to ensure their operational security and prevent disruptions to financial markets. Further, Regulation SCI requires that SCI entities (i) remediate data breaches or intrusions into their systems and notify the SEC and market participants regarding such events; (ii) conduct independent reviews of their systems

[3] *See* 17 C.F.R. § 248.30
[4] For more information regarding Regulation S-P, see SEC Release Nos. 34-42974 and 34-50781.
[5] For more information regarding Regulation S-ID, see SEC Release No. 34-69359.
[6] *See* SEC Release No. 34-63241.

and submit quarterly reports to the SEC; and (iii) engage in regular testing of incident response and business continuity plans.[7]

5. SEC Guidance for Public Companies on Reporting Material Cybersecurity Risks and Incidents (SEC Release Nos. 33-10459 & 34-82746): In February 2018, SEC Chair Jay Clayton issued updated guidance recommending that public companies adopt policies and procedures to ensure the timely disclosure to the investing public of (i) material cybersecurity risks facing the companies and (ii) material cyber incidents, including significant data breaches. Further, the SEC cautioned public companies that they should implement blackout periods and seek to prohibit trading by insiders prior to the time a potentially material cyber incident is disclosed to the public.

6. FINRA Rules 3110 & 3120: Obligation to adopt and test supervisory procedures to comply with securities laws and regulations.

7. FINRA Rule 4370: Obligation to adopt business continuity plans.

8. FINRA Rule 4530: Obligation to report to FINRA violations of securities rules and regulations.

E. Commodities and Commodities Market Rules

1. CFTC Rules Implementing the GLB Act and FCRA (17 CFR Part 160 & Part 162): Applies to entities regulated by the CFTC, such as futures commission merchants, commodity trading advisors, commodity pool operators, and swap dealers, and requires these entities to adopt policies and procedures that (i) address the administrative, technical, and physical safeguards for the protection of customer records and information; (ii) detect and mitigate identity theft; (iii) provide privacy notices to customers; and (iv) securely dispose of customer data.

2. CFTC System Safeguard Rules (17 C.F.R. §§ 37.1400-1401, 38.1050-1051, 39.18, 49.24): Rules requiring contract markets, swap execution facilities, swap data repositories, and derivatives clearinghouses to adopt cybersecurity programs and engage in testing to ensure their systems are reliable and secure.

3. National Futures Association ("NFA") Interpretive Notice to NFA Compliance Rules 2-9, 2-36 & 2-49: The NFA adopted guidance requiring member entities to adopt policies and procedures that are reasonably designed to supervise the risks of unauthorized access to or attack of information technology systems, and to respond appropriately should unauthorized access or attack occur.

[7] *See* SEC Release No. 34-73639.

F. FTC Rules for Financial Institutions

1. FTC Financial Privacy and Safeguards Rules (16 C.F.R. Part 313 & Part 314): Implements the GLB Act's requirements regarding consumer privacy and safeguarding of consumer information for financial institutions regulated by the FTC. These institutions include entities engaged in check-cashing, nonbank lenders and payment transfer services.

G. NY Department of Financial Services (NYDFS) Cybersecurity Rules

1. BitLicense Cybersecurity Rules (23 NYCRR Part 200) and Cybersecurity Requirements for Financial Services Companies (23 NYCRR Part 500): Among the strictest cybersecurity rules in the U.S., the NYDFS cybersecurity rules require most entities regulated by the NYDFS to adopt comprehensive cybersecurity programs to protect their data and systems. These include the follow requirements:

   a. Adopt comprehensive cybersecurity programs that (i) identify and assess internal and external cybersecurity risks; (ii) protect computer systems and confidential information from unauthorized access; (iii) detect, respond to, and recover from cybersecurity incidents; and (iv) fulfill applicable regulatory reporting requirements.

   b. Adopt written cybersecurity policies that address information security, data governance and classification, and customer data privacy.

   c. Appoint a Chief Information Security Officer ("CISO") and retain qualified cybersecurity staff.

   d. Conduct cybersecurity risk assessments that are to be used by the entity in creating appropriate cybersecurity policies and procedures.

   e. Maintain written incident response plans.

   f. Encrypt confidential data and securely dispose of confidential data.

   g. Make data security a part of the development of any internal computer applications and evaluate externally-developed applications for potential security issues.

   h. Use multi-factor authentication for outside connections to an entity's network.

   i. Maintain audit trails for financial transactions and network activity.

   j. Actively manage cybersecurity risks posed by third party vendors.

   k. Report any cyber incidents the NYDFS within 72 hours.

   l. Submit an annual certification from a senior officer regarding compliance with the NYDFS cybersecurity rules.

2. The NYDFS Cybersecurity rules for financial services entities went into effect in 2017 and compliance is now mandatory with many of their provisions.

H. U.S. Treasury Department Rules

1. Financial Crimes Enforcement Network ("FinCEN") Advisory FIN-2016-A005 (Oct. 25, 2016): This advisory instructs financial institutions that suspicious activity reports ("SARs") should be filed when a cyber incident or attack could result in suspicious transactions, such as, for example, when a computer hacker steals account credential information that could result in an attempt to steal money from a bank account. When filing cyber-related SARs, financial institutions are further instructed to include information related to the cyber incident, including a description of the method of intrusion, IP addresses used, and device identifiers.

I. State Data Breach Notification Laws

1. All fifty states plus the District of Columbia and certain U.S. territories maintain data breach notification laws that require businesses to notify their customers in those states after a data breach has compromised their personal information. Each state law varies in terms of how quickly notice must be provided; whether a breach must present a risk of financial harm to customers in order for notice to be mandatory; whether the business must also notify state regulators, law enforcement, and national credit reporting agencies; and what information must be included in the notice.