Cryptocurrencies Demystified and the SEC Regulatory Stance

Seoyoung Kim and Sumon Mazumdar

Background

Since the first cryptocurrency, Bitcoin, was introduced in 2009, the crypto-world has exploded. There are now over 1800 "crypto-currencies" (i.e., "digital assets", "tokens", or "coins"), many of which are traded on crypto-exchange platforms across the world, with a total market capitalization in excess of $350 billion.

A cryptocurrency is simply a set of code that is designed to serve a particular function. However, such functions differ considerably from coin to coin, and may even evolve for the same coin over time. Understanding a token's function is critical from a regulatory perspective. As Commissioner Peirce of the Securities and Exchange Commission ("SEC") recently noted, some assets may take several forms (e.g., money may come in the form of a dollar bill or as "short term, revolving loans accessible through a credit card transaction"), but all forms of money are subject to the same regulation because they serve the same function. The "inverse is also true in the financial world. A thing might seemingly have one form but in fact support many functions, each requiring a different regulatory regime. A mortgage can be a loan, but also an income stream to be used to fund a collateralized debt obligation. […] Given our federal system's considerable array of financial regulators, defining the function of a product or transaction is always essential to determining its proper regulatory regime." (Hester Peirce, "Beaches and Bitcoin: Remarks before the Medici Conference," May 2, 2018),

Some cryptocurrencies, like Bitcoin, are considered "virtual currencies," which are a "commodity" according to the Commodity Exchange Act (CEA) and subject to the Commodity Futures Trading Commission's ("CFTC") oversight. Tokens that are not considered virtual currencies are exempt from the CFTC's oversight, but may be considered "securities" and thus may be subject to securities laws as we discuss below.

In this paper we first discuss the use of distributed ledger technology, which is common to all cryptocurrencies, and the different functions (or proposed functions) of various cryptocurrencies.

A critical element of a token is that its functionality may change over time. At inception, many have no functionality because the underlying ledger (or platform) is yet to be developed. But over time, as development proceeds and more users adopt the token, its platform may become operational and decentralized. This metamorphosis in a token's functionality raises important regulatory questions: should the token be considered a security subject to federal securities law and the SEC's oversight? And if a token is deemed a security at its inception, does it remain a security forever? We discuss the SEC's views on these questions, which have garnered significant public attention recently.

Distributed ledgers: The technology underlying a cryptocurrency

Distributed ledger technology is a central characteristic common to cryptocurrencies. A distributed ledger is a record-keeping system of digital data that has no central administrator or centralized data storage. Instead the ledger is replicated, shared and synchronized across a multitude of users (the ledger's network). For example, Bitcoin was designed to be a digital currency that could serve as a substitute for fiat money. Bitcoin transactions are recorded on a decentralized electronic ledger that is replicated and maintained across all members or nodes of the decentralized Bitcoin network, which is "permissionless", *i.e.*, open to all. Using the consensus mechanism invented by Nakamoto, members of the network can verify Bitcoin transactions and get new coins for their efforts. Once verified, a block of new Bitcoin transactions are added to the existing electronic ledger (which is referred to as a "blockchain") in a virtually irreversible manner. Thus, unlike fiat money transactions that trusted intermediaries, such as banks, must record and verify, Bitcoin transactions can be verified, accessed, and stored by anyone, making the Bitcoin network a decentralized autonomous organization ("DAO").

Whether a cryptocurrency's network is truly a DAO is an important factor in assessing whether it constitutes a security under the three-pronged Howey Test, as we discuss in greater detail further below.

Different functions and types of crypto-currencies

The world of crypto-currencies is diverse and embodies varying categories with significantly different functions depending on the coin's developers.

A. Virtual currencies / electronic money

The first official cryptocurrency, Bitcoin, was designed to serve as a disintermediated, general-purpose digital currency. That is, instead of relying on fiat currency transactions that require financial intermediaries, parties can conduct peer-to-peer transactions digitally using Bitcoins. Lately, Bitcoin has been used to pay for a variety of goods and services, such as art, wine and even goats. Regulators like the CFTC consider Bitcoin a virtual currency. The SEC has also clarified that coins like Bitcoin, which is "a pure medium of exchange" and designed as a "replacement for currency", are not securities.

B. Utility tokens

Most coins developed after Bitcoin are not intended to serve as a general purpose digital currency. Instead, they are designed to allow the owner to pay for goods or services at a specific online venue (or "platform") programmed by the coin's developers, much like tokens that are required to pay for rides offered at a particular amusement park. Such coins are commonly referred to as utility tokens.

For instance, parties can pay using Ether (a token designed for use on the Ethereum platform) to set up "smart contracts." Smart contracts are simply lines of code written to automatically verify and enforce a series of pre-designated rules. For instance, a program designed to deliver an electronic document upon verification of funds is an example of a simple smart contract. Founding groups of developers often use such smart contracts to raise funds via an initial coin offering ("ICO") to pay for the development of a new crypto-currency platform. It is worth noting that as the Ethereum's popularity has risen, Ether has also become an acceptable general-purpose virtual currency.

C. Tokenized securities

Some coins are explicitly designed to provide the owner with cash-flow claims to the profits of an underlying business. For instance, venture capital funds that invest in the crypto-technology sector (e.g., Blockchain Capital and SPiCE VC) have raised investment capital by issuing coins that give investors a share of the fund's profits and are, therefore, *de-facto* tokenized shares.

D. Coins with no intended purpose

Finally, some coins are explicitly designed to provide no practical use case or value. Examples include the Jesus Coin (JC) and the GotFomo (GTFO) coin for those who may be afflicted with the fear of missing out (i.e., FOMO).

In sum, some coins, like Bitcoin, are considered virtual currencies which are regulated by the CFTC). But most coins are not virtual currencies. Tokens viewed as securities are subject to the SEC's oversight as we discuss below

The SEC's regulatory activity in the crypto-space

The majority of coins that are not virtual currencies are described as utility tokens by their founders. Because such tokens do not confer explicit cash flow rights to the owner, they are not immediately apparent as securities. However, SEC Chairman Clayton recently noted, "[m]erely calling a token a "utility" token or structuring it to provide some utility does not prevent the token from being a security. Tokens and offerings that incorporate features and marketing efforts that emphasize the potential for profits based on the entrepreneurial or managerial efforts of others continue to contain the hallmarks of a security under U.S. law." (Chairman Jay Clayton's Testimony on "Virtual Currencies: The Roles of the SEC and CFTC," United States Senate, Committee on Banking, Housing, and Urban Affairs February 6 2018).

In particular, ICOs have garnered considerable attention lately given the speed and magnitude at which developers can raise capital via an ICO compared to traditional methods of financing. In the Basic Attention Token ("BAT") ICO, developers raised $35 million in just 30 seconds. ICO investors typically pay using some existing crytpocurrency, such as Bitcoin or Ether, and (in most cases) receive a token in exchange that gives them the right to use the proposed new platform when it is developed. Thus, tokens sold in an ICO often have no immediate functionality because they only become functional if the proposed platform is actually developed and becomes operational in the future. Therefore, the token's lack of immediate functionality could result in its being considered a security subject to the SEC's oversight, even though the token may not convey any cash flows rights to the buyer like a traditional security. The SEC

may consider the sale of such a token to the general public through an ICO to be a security offering that must be appropriately registered.

The Howey Test of determining whether a token is a security

According to the Howey Test (SEC v. W.J. Howey & Co., 328 U.S. 293, 298-99 (1946)), an investment contract is any contract, transaction, or scheme involving (1) an investment of money (2) in a common enterprise (3) with the expectation that profits will be derived from the efforts of the promoter or a third party.

In SEC v. Shavers, No. 4:13-CV-00416 (E.D. Texas, Aug. 6, 2013), the court applied this three-pronged Howey Test to an alleged Bitcoin-related Ponzi scheme, determining that Shavers had sold investment contracts and, thus, was subject to federal securities laws. Specifically, Shavers had created an online entity, Bitcoin Savings and Trust ("BTCST"), through which he allegedly defrauded investors out of more than 700,000 bitcoins. Shavers had advertised a Bitcoin "investment opportunity" in BTCST investments promising investors up to 7% interest per week and claiming that the invested funds would be used for Bitcoin activities. Instead, Shavers allegedly used Bitcoins from new investors to repay earlier investors and to pay for his personal expenses.

However, Shavers argued that the BTCST investments did not qualify as securities, because Bitcoin is not actually money and does not fall under the regulatory jurisdiction of the United States. Shavers further argued that since all of his transactions were Bitcoin transactions, no money was ever exchanged. The SEC argued that the BTCST investments were both investment contracts and notes, and, thus, constituted securities under its jurisdiction. The term "security" is defined as "any note, stock, treasury stock, security future, security-based swap, bond ... [or] investment contract ..." 15 U.S.C. § 77b.

Applying the Howey Test, the court concluded that the BTCST investments were indeed investment contracts and hence securities, because the BTCST investments: (1) constituted an "investment of money" since "Bitcoin can be used as money" to pay for goods or services, and can also be exchanged for conventional currencies such as the U.S. dollar; (2) involved "a common enterprise" because the investors were dependent on Shavers' expertise in Bitcoin

markets and his local connections; and (3) were made by investors who expected profits from Shavers' trading activity.

More recently, in July 2017, the SEC issued a Section 21(a) report regarding initial coin offerings ("DAO Report") that examined the application of the federal securities laws to the offer and sale of virtual tokens that were created and distributed on the Ethereum blockchain by an entity called "The DAO" (not to be confused with the generic term DAO; i.e., a de-facto decentralized autonomous organization). The SEC's report concluded that The DAO's virtual token constituted an investment contract and, therefore, was a security subject to federal securities laws—including those relating to offers, sales, and trading—regardless of whether the security is certificated or issued on a blockchain and irrespective of whether fiat money or virtual currencies are used to purchase the security in question. Later in 2017, the SEC set up a Cyber Unit, which, among other things, focuses on violations of federal securities laws involving distributed ledger technology and initial coin offerings.

Most ICOs are securities according to the SEC, but they may not necessarily remain securities

In December 2017, SEC Chairman Clayton noted that determining whether a particular ICO constitutes a security offering depends on its particular facts and circumstances, and that "[b]y and large, the structures… [he had seen to date] involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws." (Statement on Cryptocurrencies and Initial Coin Offerings, SEC Chairman Jay Clayton, December 11, 2017).

Importantly, though, even if a token's ICO is designated a security offering, it does not necessarily remain a security forever, as William Hinman, director of the SEC's Division of Corporation Finance, recently clarified. Specifically, Director Hinman noted that a digital asset that began as a security might later be sold "in a manner that does not constitute an offering of a security" in "cases where there is no longer any central enterprise being invested in or where the digital asset is sold only to be used to purchase a good or service available through the network on which it was created." For instance, "putting aside the fundraising that accompanied the creation of Ether, based on […] the present state of Ether, the Ethereum network and its

decentralized structure, current offers and sales of Ether are not securities transactions." ("Digital Asset Transactions: When Howey Met Gary (Plastic)" William Hinman, June 14, 2018).

New regulatory questions

Thus, the SEC recognizes that as a token's platform evolves, its treatment as a security may no longer be valid. This raises several questions: How does one determine whether a platform has become sufficiently operational and decentralized so that its token is no longer deemed a security?

Absent any bright-line tests, the question will likely require further regulatory guidance in the future because even operational and decentralized platforms may rely, to some extent, on the efforts of a founding group for its further development. For instance, the Ethereum network is accepted as an operational and decentralized organization today by the SEC. Yet, Ethereum's ongoing development remains under the centralized direction of the Ethereum Foundation. The issue of whether a token is a security is likely to also result in lawsuits from private plaintiffs. For instance, three securities lawsuits have been filed against Ripple this year. The third, filed on July 5, 2018, is a securities class action filed in San Mateo county on behalf of all California purchasers of Ripple tokens ("XRP") against Ripple, XRP II and its Chief Executive Officer, that alleges Ripple's XRP token (the third largest crypto-currency by market capitalization) "had all the traditional hallmarks of a security, yet defendants failed to register them as such."

Finally, it is worth noting that to avoid the SEC's registration requirements of a securities offering to the general public, many coins are now being offered as Regulation D ("Reg D") offerings. Such offerings are exempt from full SEC registration requirements, because they are offered only to accredited investors—i.e., individuals who have a net worth of over $1 million (outside of their primary residence) or an annual income of at least $200,000, or companies that have over $5 million in assets.

Reg D offerings of tokens have become more popular since the development of an investment contract known as a SAFT ("Simple Agreement for Future Tokens"). Similar to Y-Combinator's "Simple Agreement for Future Equity" (SAFE), a popular contract used to raise funds for start-ups and promises future equity to investors contingent on subsequent venture rounds, a SAFT promises future tokens to investors in exchange for their investment capital up

front. A SAFT is considered a security that can only be sold to accredited investors if the developers wish to seek exemption from registration requirements as per Rule 506(c) under Reg D. Nonetheless, the same regulatory questions discussed earlier apply to such exempt offerings: Will the future token offered to a SAFT investor be deemed a security? Will such a token ever be re-classified and no longer deemed a security? If so, what criteria will be applied to determine whether the token's functionality has changed sufficiently to merit a re-classification?

Concluding remarks

The manner in which a crypto-currency is regulated depends on its functionality, which differs from coin to coin. Virtual currencies like Bitcoin that serve as general purpose digital money are regulated by the CFTC as a commodity. Coins that are not virtual currencies may be deemed *securities* and subject to the SEC's regulatory oversight.

The SEC applies the Howey Test to determine if a token has the traditional hallmarks of a security. If it does, then the token's sale through an ICO constitutes a security offering that must be registered if the token is offered to the general public. But a coin's functionality may change over time. Thus, even if a token is viewed as a security at inception it may no longer remain a security later if the token's platform becomes sufficiently operational and decentralized. The changing functionality of tokens raises additional regulatory questions, and the SEC has already issued "dozens of subpoenas and information requests to technology companies and advisers" in a probe of the ICO and token sales industry. The regulatory landscape concerning cryptocurrencies is likely to continue to change as the technology itself continues to evolve rapidly.