October 6, 2021

Cryptoassets at an Inflection Point

Cryptoassets and the underlying blockchain technologies are becoming increasingly mainstream, with stablecoins, decentralized finance (DeFi), and digital representation of ownership (NFTs) rapidly gaining footing. While these technologies have attractive features, and may yet prove revolutionary for our economy, this rapid growth also poses significant risks, implicating longstanding principles of prudential regulation, market integrity, and investor protection. The challenge facing U.S. regulators and lawmakers is one of balance: to protect investors and market integrity, and curb excesses that could significantly harm the economy, while preserving the technology's benefits for market participants and the U.S.'s position at the industry's vanguard. Following are some considerations which could help strike an appropriate balance on some of the most salient issues posed by cryptoassets' rapid growth.

- *Stablecoins should maintain robust and transparent reserves under regulatory oversight.* While stablecoins vary in their design, most stablecoins share hallmarks of demand deposits—specifically, they purport to be fully backed by, and redeemable on demand for, an underlying unit of fiat currency. Although a stablecoin may be backed by FDIC-insured deposits, some stablecoins hold a mix of non-FDIC-insured cash and securities, and some may have at times maintained a fractional reserve. Insofar as stablecoins represent assets other than cash, they possess hallmarks of securities—specifically money market funds. These features render stablecoins susceptible to the same liquidity and "run" risk as regulated banks and money market funds, albeit without commensurate regulatory oversight, including as to reserve requirements, and with varying levels of transparency. With institutional investors and venture capital funds increasingly participating in crypto markets, the risk of contagion from this burgeoning shadow banking system cannot be discounted. Pending possible development of a U.S. central bank digital currency (which is appealing in principle but carries daunting design challenges), the market capitalization of stablecoins can be expected to grow.

  Accordingly, it is appropriate that U.S. regulators have sounded warnings about the stablecoin ecosystem and are working towards responsive rule proposals to bring stablecoins within the regulatory perimeter. In our estimation, fiat-backed stablecoins should either be issued by banks (as permitted for national banks under OCC guidance) with the associated liquidity requirements, or, if issued by a nonbank and not regulated as a money market fund, should be fully backed by reserves consisting of insured bank deposits and/or highly liquid treasury bills. Apart from mitigating run risk, maintaining a nexus between stablecoins and traditional banking would help avoid pressures on bank lending and money creation through the pyramiding of deposits that could ensue from unchecked growth of stablecoins and functional removal of fiat currency from banking channels.

- *Deposit-like products require particular regulatory focus.* Some companies engaged in cryptocurrency lending, such as BlockFi and Celsius, are offering retail-oriented products whereby depositors of stablecoins can currently earn annual yields of 8% or more (a function of corresponding customer demand to engage in crypto-collateralized borrowing in order to participate in DeFi or to obtain liquidity in lieu of selling appreciated cryptoassets). Although these products are not, and do not purport to be, FDIC-insured, in an environment where bank deposits earn mere basis points, the appeal of these products is considerable, although we expect rate compression over time. While we express no view here as to the legal status of any particular product, there are clear policy repercussions from the growth of bank-like functions outside of the regulated banking system. Depending on their design, some of these products may indeed have hallmarks of securities and/or demand deposits. Accordingly, it is appropriate for regulators to examine these products on a case-by-case basis in the interest of investor protection. To date, BlockFi and Celsius have each been subjected to state-issued cease and desist orders in respect of interest-bearing products, and Coinbase received an SEC Wells notice in connection with its proposed interest-bearing "Lend" product. Decentralized lending and borrowing platforms pose similar challenges, but do not include a central point of failure as in the case of centralized crypto borrowing and lending, and currently lack the retail orientation of some centralized platforms.

- *Significant DeFi participation should require a "KYC" touch-point.* The scope of cryptoassets' use for criminal purposes, such as ransomware, may be significantly less than generally believed; bad actors could do better than to transact through a globally viewable (albeit pseudonymous) and immutable ledger such as bitcoin. That said, the lack of "know your customer" and anti-money laundering hurdles for swaths of crypto transactions—ranging from DeFi activity to some NFT sales at stratospheric valuations—is perceived by many as a feature, not a bug. Proposed rules promulgated by the Treasury Department at the end of the Trump Administration (and paused by the Biden Administration) would have required that licensed crypto exchanges verify the identity of recipients using unhosted wallets for transactions exceeding $3,000 in value, and draft guidance proposed by the G7's Financial Action Task Force would encompass most DeFi activity within the definition of "Virtual Asset Service Providers" subject to anti-money laundering requirements. While these rules and guidance, if adopted, would help curtail some illicit activity, they would, in the former case, impose daunting burdens on cryptocurrency exchanges and other participants in the crypto ecosystem beyond what is required of other money services businesses, and could drive transactions away from licensed exchanges, and in the latter case, could effectively criminalize development of decentralized exchanges and lending platforms. An alternative path forward could be to require that DeFi users (at least above a prescribed dollar threshold of activity) have their identity validated via a third-party KYC-check, and to reflect the fact of that validation within the blockchain, or through a wallet interface, without broadcasting the participants' identity. Relatedly, DeFi platforms could deploy code (including, if necessary, through protocol "forks") requiring such a proof of validation, or enabling validated participants to elect to only transact opposite similarly validated participants.

- *Market integrity is paramount.* To the extent that cryptocurrency markets do not include assets constituting securities, such markets are outside the purview of the SEC.

Insofar as such markets do not include derivatives, they are outside the purview of the Commodity Futures Trading Commission, which does not regulate spot markets. This poses a particular challenge in regulating decentralized exchanges. But even in the case of some centralized exchanges—whose internal protocols vary in their stringency—there are risks of market manipulation, such as front running and insider trading. And empirically, there have been numerous reported instances of increased token trading volume in the run-up to certain cryptoassets being "listed" on major platforms, or of token developers transacting in tokens while in possession of asymmetric information. Fundamentally, even if nonderivative cryptoassets are commodities and not securities, in terms of their risk profile, they bear hallmarks of securities or derivatives that are not common to, say, bushels of wheat. Consequently, we anticipate that legislators and regulators will consider measures to provide assurance of the integrity of centralized markets. Such measures are more difficult to conceive in the case of decentralized markets, but decentralized markets are comparatively open and transparent, and perhaps offer the prospect of code-based solutions. And while normally associated with the SEC, the authority to bring insider trading cases also rests with the CFTC, which might be more frequently invoked in appropriate cases.

- *Securities disclosure should take into account cyptoassets' distinctive features.* The SEC's existing disclosure regime is somewhat ill-fitting for crypto securities, being geared towards traditional equity and debt securities. For example, the financial profile of the "issuer" of a token—often a nonprofit entity—may be irrelevant to a prospective token purchaser, such that requirements for audited financial statements, MD&A and the like would not be beneficial, and the associated costs and burdens could tend to deter registration. Conversely, an independent audit of a protocol's code, including in respect of future token generation, could be of much utility. Recognizing that discrete categories of securities may necessitate alternative disclosure regimes, the SEC promulgated Regulation AB to govern tailored disclosure with respect to asset-backed securities. Such an approach could be suited to the cryptoasset space, especially if calibrated so that investors come to see such disclosure as valuable (relative to current reliance on crypto issuers' so-called "white papers," GitHub, social media and the like) and issuers come to see such disclosure as both navigable and a qualitative differentiator.

Protective features of the traditional financial system did not spring fully formed with the advent of markets, but evolved as a result of bitter experience which need not be relearned now at the expense of crypto investors and financial stability. At the same time, heavy-handed regulatory approaches risk harming a burgeoning ecosystem featuring much bottom-up wealth generation. Striking the appropriate balance will require the concerted efforts of many constituencies, which would be well served by open dialogue, inclusive of both traditional institutions shaped by past experience as well as thoughtful voices from among the digital pioneers.

David M. Adlerstein