UNDERSTANDING THE WORLD OF CRYPTOCURRENCY

The recent swift and sudden collapse of Sam Bankam-Fried's cryptocurrency exchange, Bahamas-headquartered FTX, valued at a reported £32 billion, stunned the cryptocurrency markets, his high-profile VC investors, FTX customers and employees, beneficiaries of his philanthropy, leaders in the "effective altruism" movement, Bahamian officials who had hoped the country would become a base for the evolving crypto industry, lobbyists, policymakers and regulators. As described in greater detail below, as a cryptocurrency exchange, FTX allowed customers to connect their cryptocurrency wallets and buy, sell or enter into derivative contracts for coins and tokens, as well as NFTs. Customers could trade digital currencies for other digital currencies or traditional currency (fiat), and vice versa.

The impact of the collapse of FTX is being felt far and wide, and this is likely only the beginning. The first high-profile casualty of the contagion appears to be the cryptocurrency lender BlockFi, which filed a Chapter 11 bankruptcy petition yesterday. Two weeks ago, BlockFi had acknowledged significant exposure to FTX and paused many of its platform activities following the collapse of FTX.

Some have likened the collapse to a "Lehman moment." It is too early to tell, but no doubt the collapse will be seen by lawmakers and regulators as unmistakeable evidence of the need to accelerate ongoing efforts to regulate the digital assets sector. The FTX collapse comes at a time when the cryptocurrency industry is struggling to gain acceptance and credibility. Investigations, as well as regulation, are sure to follow.

The cryptocurrency market got its start in the wake of the global financial crisis. Largely in response to the collapse of confidence in global financial institutions, Bitcoin was launched by the anonymous (and as-yet identified person or group) Satoshi Nakamoto to reimagine currency – a fragmented system of trust, decentralized across the internet. Since then, the market has ballooned, yet with virtually no regulation.

I set out below as an "explainer," for those less familiar with cryptocurrencies, of what the crypto market is all about and touch on recent efforts to regulate it. I note at the outset that, according to a Pew Research Center research note (November 2011), 16% of adult Americans (22% of men, and 10% of women) say they personally have invested in, traded or otherwise used cryptocurrency, including 31% of Americans aged 18-29, 43% of men aged 18-29 but only 19% of women 18-29.

What is Crypto?

Cryptocurrency, or crypto, is a digital, decentralized representation of value that functions as a medium of exchange, a unit of account and/or a store of value. In short, it is any form of "currency" that exists in a digital or virtual (rather than physical) form and uses cryptography as the means of recording, verifying and transferring ownership, including to effect secured transactions. Its most notable attribute is that it is decentralized.

The "currency" is generated through a process of solving complex cryptographic puzzles. The value of cryptocurrencies is transferred and recorded on a blockchain, with its provenance and transfer of ownership verified by cryptography – hence the "crypto" in "cryptocurrency." Cryptocurrencies have similar functions to fiat or ordinary currencies, but they do not rely on any clearing house, central bank or other bank for settlement purposes and

are not backed or issued by any government. An owner of cryptocurrency in fact owns a digital key stored in a digital wallet, nothing tangible.

To understand how this peer-to-peer digital payment system works, you need to understand the following key concepts: distributed ledgers and blockchain (on which all transactions are recorded and verified), digital keys, digital wallets (which hold the digital keys) and mining (the process using computers to solve complex mathematical problems by which units of cryptocurrency are created by crypto miners).

I set out below a glossary of relevant terms:

Bitcoin: the first cryptocurrency. It was launched in 2009 based on a 2008 white paper written by an anonymous figure or group under the pseudonym Satoshi Nakamoto. The idea behind Bitcoin was to create an electronic peer-to-peer cash system. Bitcoin is a network comprising a decentralized ledger and internet-based payment system. Non-Bitcoin currencies are known as **altcoins.**

Block: a package of digitally recorded data.

Blockchain: the technology underpinning all cryptocurrencies. It is a digital form of keeping records (a distributed ledger) with sequential blocks of data built upon one another, generating a permanent, and unchangeable, ledger of transactions. Each transaction on the blockchain is registered chronologically (time-stamped) and cryptographically linked through a series of blocks in a way that prevents previous blocks from being modified or otherwise tampered with. Each such transaction once verified is added as a "block" in the chain. Data can be added to the chain via a network of computers, but once added cannot be removed or modified.

Central Bank Digital Currencies, or CBDCs: virtual currencies created and backed by a central bank. Central banks, including the Federal Reserve, have been exploring the feasibility and viability of CBDCs. (*See, e.g.*, Fed: Money and Payments in Age of Digital Transformation and WH Office of Science & Technology Policy - CBDC).

Coin: digital value living on a blockchain or cryptocurrency network. In some cases, such as Bitcoin, blockchains have the same name for the coin and the network. It in effect is a cryptocurrency, native to the blockchain on which it was created and is traded. It should not be confused with a token.

Cold wallet, or cold storage: a method of storing cryptocurrency offline that is impervious to hacking or online theft, though it does risk being lost or stolen. Cold wallets are physical devices similar to USB drives. A **hot wallet** is a software-based wallet connected to the Internet. The wallets store public and private keys.

Cryptography: the use of cryptographic protocols to encrypt messages between parties.

dAapps, or decentralized applications: provide services similar to those on standard consumer applications, but use blockchain technology to provide users with control over their data, as there is no centralized intermediary to manage the data. The essential elements of dApps are: they are open source, decentralized, distributed on a blockchain and based on smart contracts.

DAO, or centralized autonomous organization: a cooperative based on smart contracts, where rights to vote on collective investments are tied to utility coins.

Decentralization: the cornerstone of cryptocurrency is that power over it is distributed. There is no central authority.

DeFi, or decentralized finance: activities undertaken as part of a multifaceted, open financial infrastructure without the involvement of a financial institution, government or other intermediary.

Distributed ledger, or distributed ledger technology (DLT): a database spread across several nodes in different countries that is both decentralized and transparent to those with access to the relevant network. Each node holds a full copy of the ledger and is updated for each new transaction based on consensus algorithms. A blockchain is a form of distributed ledger, but it need not be structured as blocks.

Exchange, or crypto exchange: a cryptocurrency exchange is a digital marketplace through which customers can buy or sell cryptocurrency for other digital currencies or traditional (fiat) currencies. A customer that sets up an account on an exchange can then buy and sell cryptocurrencies. These exchanges operate 24/7. Many exchanges have wallets, but these should not be confused with the wallets that the customers control. Assets in an exchange wallet are controlled by the exchange, while assets in a cold/hot wallet set up by a customer are controlled by that customer.

Fork: if the community of users of a blockchain decides to change the governing protocols, the new path is known as a fork.

ICO, or initial coin offering: an offering to raise funds for a cryptocurrency project.

Mining: an algorithm-based process by which new cryptocurrency units are made available by solving complex mathematical problems, and transactions between users are validated and logged on the blockchain. **Miners** use computing power to solve a **hash,** which is the result of a compression of data through algorithms involving trillions of possible combinations. Miners receive rewards in exchange for creating new crypto, the first miner that solves the puzzle receiving the reward. Miners in effect are the facilitators of the cryptocurrency ecosystem, and the Proof of Work process ensures its accuracy and integrity.

NFTs, or non-fungible tokens: units of value representing the ownership of a unique digital item, such as art.

Node: a connected computer that is part of the blockchain. Any node can be used to broadcast messages across a system.

PoS, proof of stake: an alternative to PoW to validate crypto transactions and add them as new blocks to the chain. This alternate consensus mechanism is based on **validators** that get the chance to validate new transactions and be rewarded by locking up their stake (crypto tokens or cryptocurrency) in a smart contract on the blockchain. If validators fail to accurately validate new data or seek to game the system, they can lose their stake.

PoW, or proof of work: the consensus mechanism (of software algorithms) involving multiple nodes used to verify the hash needed to add a block to a blockchain. It is the key element used to verify the accuracy of new transactions underlying cryptocurrencies that are

added to a blockchain. The PoW is needed to ensure the integrity of new data related to new transactions since in the decentralized world of crypto there is no central governing authority. PoW most importantly solves the so-called **double spend** problem, namely users spending the same units in different places before the system records the transaction. It solves the problem by verifying a transaction before it is added to the blockchain, through the incentives to miners to be the first. The major criticism of this process is the massive amounts of electric power is needed to mine crypto. Many but not all cryptocurrencies use the PoW process.

Private key: random characters providing access to bitcoins or other cryptocurrencies in a specific wallet, which can be used to verify ownership. An owner of a private key can generate a public key whose ownership can be verified without the identity of the owner being identified. Essentially private keys are used to send cryptocurrency from a wallet, but cannot be used to receive cryptocurrency. The **public key** functions as an account number and can be used to receive cryptocurrency from another user, but cannot be used to send cryptocurrency. These keys usually consist of 64 characters to encrypt a wallet (public key) or decrypt a wallet (private key) and generate digital signatures. The public key is also known as a wallet address.

Smart contract: a piece of code executed on the blockchain that self-executes an agreement, for example upon creation of a token, or transfer to a new owner.

Stablecoin or digital fiat: a cryptocurrency that pegs its value to a non-digital currency or commodity, such as a fiat currency. A **digital fiat** represents a **fiat** (derived from the Latin term for decree, as in currency whose value and legal status as tender flows from a government decree), which is a government-backed currency, such as the US dollar, on the blockchain. It can also be backed by US Treasuries or other cryptocurrencies. A stablecoin can also be an algorithmic stablecoin, which is backed only by code. Some refer to stablecoins that are pegged to fiat such as the US dollar (on a 1:1 basis), and are convertible on demand from the issuer for the fiat, as "**payment stablecoins**" (*see, e.g.*, Circle's Payment Stablecoin Policy Principles and the Gillibrand-Lummis Bill.)

Token: a unit of value (a piece of code comprising distinct asset references, unique properties or legal rights) on a blockchain that is managed by a smart contract and an underlying distributed ledger. A token can represent any asset, including cryptocurrencies, and is the principal way of transferring and storing value on a blockchain. Tokens can be fungible or non-fungible. In contrast to a coin, the token in effect is tied to a project that sits atop a blockchain.

Tokenization: the process by which the value of a tangible or intangible asset is converted into a token. Once tokenized, the underlying asset can be transferred, exchanged or stored on a compatible platform or marketplace. The potential of asset tokenization is potentially unlimited

Utility tokens: is a cryptocurrency on a pre-existing blockchain that allows access to a specific product or service on that blockchain ecosystem, essentially allowing users to perform specified actions on the specified network. Utility tokens have a monetary value, but are not intended to be a medium of exchange as they only function in the one ecosystem. A utility token may be used for voting on proposed changes to a dApp, in which case it is known as a "**governance token**." Utility tokens emerged on the Ethereum blockchain, when

it introduced smart contract functionality, and gained prominence during the surge of ICOs. Tokens should not be confused though with coins, as only the latter function as a medium of exchange.

How is Crypto Regulated in the United States?

The short answer is that it is lightly regulated. If you have money in a traditional bank account, it is protected up to guarantee limits. If you wire money to the wrong account from a regulated bank, you may be able to get it back. If your account at a regulated bank is hacked, you may well have protection. None of that obtains in the crypto world. If the money is gone, it is gone; there is no one to go to. Customers of crypto exchanges have the protection of neither the Federal Deposit Insurance Corporation ("FDIC") (for bank accounts) nor the Securities Investor Protection Corporation (for brokerage accounts). In addition to the cryptocurrencies themselves, there are options and futures on these currencies, and significant amounts of leverage. These have a turbocharging effect on volatility.

As is often the case, laws/regulations lag behind innovation. Think of credit default swaps, collateralized debt obligations and the plethora of other instruments that cratered the global financial markets in 2008. And just as policymakers and regulators needed a crash course (no pun initially intended) in the murky world of financial derivatives in 2008, so too should FTX be a wake-up call for lawmakers to get up to speed on the entire digital assets sector.

One challenge for regulation is that the crypto market by definition based on its antecedents is decentralized; it is in the cloud. Who can regulate it? And in the United States there is the added challenge of the bifurcation of regulatory oversight between the Commodity Futures Trading Commission ("CFTC") and the Securities and Exchange Commission (the "SEC"). Separately, the Department of Justice has the ability to prosecute fraud.

Executive Orders

In September, the White House, following submission of agency reports called for in a March Executive Order on Ensuring Responsible Development of Digital Assets, set out its Comprehensive Framework for Responsible Development of Digital Assets (*see* Fact Sheet). The reports cover a range of topics related to digital assets, including illicit finance, protection of consumers, US competitiveness, the US system of money and payments (including stablecoins and instant payments) and the policy implications of creating a CBDC, and climate. The reports released in September were:

- Commerce Department - US Competitiveness
- Justice Department - Enforcement
- Treasury Department - Future of Money and Payments
- Treasury Department Action Plan - Illicit Finance
- Treasury Department - Consumer Implications
- WH Office of Science & Technology Policy - CBDC
- WH Office of Science & Technology Policy - Climate Implications

Among other things, the Framework encourages agencies to address current and emerging risks in the digital asset ecosystem and urges regulatory and law enforcement agencies to collaborate to address acute digital assets risks facing consumers, investors and businesses, and to share data on consumer complaints regarding digital assets. The Administration is considering whether to ask Congress to amend the Bank Secrecy Act to apply explicitly to

digital asset service providers, including digital asset exchanges and NFT platforms. Treasury is to enhance dialogue with the private sector to ensure that digital asset firms understand existing obligations and illicit financing risks associated with digital assets, share information and encourage the use of emerging technologies to comply with obligations.

These additional agency reports were issued previously, over the summer:

- Justice Department - Enforcement Cooperation
- Treasury Department - Framework on International Engagement

Treasury

In May, Treasury Secretary had called for regulation of the stablecoin market following a precipitous drop in value of the algorithmic stablecoin TerraUSD (meaning it fell below its 1:1 US dollar peg), causing a drop of 50% in the value of Bitcoin from its high in November 2021, as the organization behind TerraUSD injected liquidity in the form of Bitcoin.

The President's Working Group on Financial Markets, the FDIC and the Office of the Comptroller of the Currency had issued a report in November 2021 on Stablecoins, calling on Congress to enact legislation to ensure that payment stablecoins and payment stablecoin arrangements are subject to prudential oversight. The report notes that "because payment stablecoins are an emerging and rapidly developing type of financial instrument, legislation should provide regulators flexibility to respond to future developments and adequately address risks across a variety of organizational structures." Such legislation should require specifically:

- stablecoin issuers to be insured depository institutions, which are subject to appropriate supervision and regulation, at the depository institution and the holding company level;
- custodial wallet providers to be subject to appropriate federal oversight and regulators should be empowered to require any entity that performs activities that are critical to the functioning of the stablecoin arrangement to meet appropriate risk-management standards; and
- stablecoin issuers to comply with restrictions on their activities that limit affiliation with commercial entities.

Commodity Futures Trading Commission

The CFTC regulates commodity futures and options, and has evolved into the regulator of derivatives. Industry and others have been pushing for the CFTC to have greater oversight over crypto at the expense of the SEC. To the extent that crypto is deemed a security, oversight would fall within the SEC's jurisdiction, but there is ambiguity over which components of the crypto world are securities. The White House Framework announcement did not allocate regulatory responsibility as between the CFTC and the SEC, instead calling on them both, "consistent with their mandates," to "aggressively pursue investigations and enforcement actions against unlawful practices in the digital assets space."

The CFTC has brought enforcement actions again entities clearly falling within its jurisdiction, namely commodity pool operators. (*See* Mirror Trading International Proprietary Limited.)

Securities and Exchange Commission

SEC Chair Gensler, and his predecessor Jay Clayton, have steadfastly maintained that, based on the holding in the seminal Supreme Court case (*SEC v. W.J. Howey Co.*), the vast majority of tokens in the crypto market are securities, the offer and sale of which are subject to the federal securities laws and, therefore, SEC oversight. (*See, e.g.*, 9/8/22 speech). Under the so-called *Howey* test, an instrument is deemed a security if investors are expecting profits derived from the efforts of others in a common enterprise.

In 2017, in its Report of Investigation of The DAO, the SEC cautioned that offers and sales of digital assets in the form of ICOs could be deemed to be offers and sales of securities, subject to the federal securities laws. In particular, it found that the tokens offered by The DAO in exchange for the virtual currency, Ether, were securities. In December 2017, Munchee Inc. halted the sale of digital tokens to raise capital for its blockchain-based food review service after being contacted by the SEC.

The SEC website lists 100 enforcement actions brought by the SEC in connection with crypto assets between July 2013 and November 2002. In February 2022, BlockFi agreed to pay a $100 million penalty for violating both the public offering rules as well as the Investment Company Act of 1940 in connection with a retail crypto lending product. *See also* "Framework for 'Investment Contract' Analysis of Digital Assets" issued by the SEC's Strategic Hub for Innovation and Financial Technology (modified April 2019). An SEC no-action letter, in effect finding that a token was not a security, was issued to Pocketful of Quarters.

Earlier this month, the court in *SEC v. LBRY* ruled in favor of the SEC (granting its motion for summary judgment), finding that the native digital token of the LBRY blockchain, LBC, was a security under the *Howey* test. (*See* SEC Litigation Release.) This followed a similar final judgment on consent in *SEC v. KIK Interactive Inc.* in October 2020. (*See* SEC Press Release.) In June 2020, the SEC had obtained court approval of a settlement in its case against Telegram Group and its subsidiary TON Issuer Inc. relating to an offering of digital tokens, in which the defendants agreed to return more than $1.2 billion to investors and to pay an $18.5 million civil penalty. (See Press Release.) These decisions represent the application of the *Howey* test based on "objective economic realities" of the transactions in question.

In what could be a significant development in the area, one way or the other, the SEC brought charges in December 2020 against Ripple Labs, its former CEO and Board chair, its former COO and now CEO, and various others over the sale of Ripple's cryptocurrency XRP. That case is still pending in federal court. A number of amicus briefs have been filed in support of the defendants, including on behalf of XRP holders as well as by crypto industry trade associations. Both Ripple and the SEC filed motions for summary judgment in September.

Congress

In June, Senators Kirsten Gillibrand (incidentally, a former derivatives attorney) and Cynthia Lummis introduced the Responsible Financial Innovation Act to create a comprehensive regulatory framework for digital assets. Among other things, the bill creates a definition of digital assets and distinguishes between digital assets that are securities or that are commodities by evaluating the purpose of the asset and the rights/powers it conveys the consumer. The bill gives the CFTC authority over applicable digital asset spot markets.

Digital assets that meet the definition of a commodity, such as Bitcoin and Ether, which represent more than half the digital asset market capitalization, would be regulated by the CFTC. The bill would establish 100% reserve, asset type and detailed disclosure requirements for all payment stablecoin issuers.

Concluding Thoughts

Addressing the need for regulatory oversight of digital assets may well be a bipartisan issue in Congress, but as the former head of the FDIC, Sheila Bair, noted in an interview with the Financial Times, there are authorities in place that empower regulators to act while Congress figures out what to do. Regulators, she argues, should not wait for Congress, as the current state of US regulatory oversight of the digital markets means that American investors are trading digital assets through entities headquartered offshore that are not subject to prudential requirements under US law.

There is only so much regulation can do. In part, regulation serves to put investors on notice of the risks, and there should be little mystery about the risks. The more significant question is around the internal guardrails for an industry in swift transition. Recent events over the past year are a timely reminder of the importance of board oversight, external audits, internal control, and customary corporate governance procedures, including around conflicts of interest. These elements are not limited to the markets for cryptocurrencies or other digital assets, but the absence of a comprehensive regulatory regime makes these all the more important. As technology drives new entrants seeking capital, and whether the opportunities are presented by the embrace of digital assets or climate-related green technology, or otherwise, investors should not lose sight of the basics of governance. The imperatives are not unlike the governance challenges seen in the dot.com boom and the early days of the social media platforms.

* * *

Mark S. Bergman
7Pillars Global Insights, LLC
Washington, D.C.
November 29, 2022