

U.S. Department of the Treasury

# Crypto-Assets:

## Implications for Consumers, Investors, and Businesses



September 2022



## TABLE OF CONTENTS

<b>I. EXECUTIVE SUMMARY.....</b>	<b>1</b>
<i>Listening to the Public.....</i>	<i>4</i>
<b>II. OVERVIEW OF CRYPTO-ASSET MARKETS ECOSYSTEM.....</b>	<b>4</b>
<b>Descriptions of Key Terminology.....</b>	<b>4</b>
<i>Crypto-assets.....</i>	<i>4</i>
<i>Wallets, Keys, and Custody .....</i>	<i>6</i>
<b>Entities Providing Services or Products in Crypto-asset Markets .....</b>	<b>7</b>
<i>Crypto-asset Platforms.....</i>	<i>7</i>
<i>Miners and Validators .....</i>	<i>11</i>
<i>Data Aggregators.....</i>	<i>12</i>
<i>Traditional Financial Institutions.....</i>	<i>12</i>
<b>III. CRYPTO-ASSET MARKET TRENDS, USES, AND OPPORTUNITIES .....</b>	<b>13</b>
<b>Market Size .....</b>	<b>13</b>
<b>Current Uses and Opportunities in Crypto-assets for Consumers, Investors, and Businesses ...</b>	<b>15</b>
<i>Native Crypto-asset Financial Markets, Products, and Services .....</i>	<i>15</i>
<i>Financial Market and Payment System Infrastructures .....</i>	<i>19</i>
<i>Other Commercial Activities .....</i>	<i>22</i>
<b>IV. RISKS AND EXPOSURES FOR CONSUMERS, INVESTORS, AND BUSINESSES .....</b>	<b>25</b>
<b>Conduct Risks .....</b>	<b>26</b>
<i>Fraud, Theft, and Mismanagement.....</i>	<i>26</i>
<i>Information Asymmetry: Lack of Transparency .....</i>	<i>29</i>
<b>Operational Risks .....</b>	<b>33</b>
<i>General Features and Decentralized Governance .....</i>	<i>34</i>
<i>Security and Scalability Tradeoffs and De-anonymization .....</i>	<i>35</i>
<i>Peer-to-Peer Verification, Mining Pools, and Validation Incentives.....</i>	<i>35</i>
<b>Risks in Crypto-asset Intermediation .....</b>	<b>37</b>
<i>Resources and Capabilities Risks.....</i>	<i>37</i>
<i>Custody Risks.....</i>	<i>37</i>
<b>Risk Exposures: Regulatory Non-Compliance and Evolving Market Oversight .....</b>	<b>38</b>
<i>Effects of Legal and Regulatory Non-Compliance .....</i>	<i>40</i>
<i>Effects of Changes in the Scope and Application of Laws and Regulations.....</i>	<i>40</i>
<b>V. OPPORTUNITIES AND RISKS FOR POPULATIONS VULNERABLE TO DISPARATE IMPACTS .....</b>	<b>41</b>
<b>Potential Opportunities for Populations Vulnerable to Disparate Impacts.....</b>	<b>42</b>
<i>Expanded Access to Financial Services .....</i>	<i>42</i>
<i>Reduced Transaction Costs.....</i>	<i>44</i>
<i>Potential Opportunities to Build Wealth.....</i>	<i>45</i>
<b>Potential Risks to Populations Vulnerable to Disparate Impacts.....</b>	<b>46</b>
<i>Market Volatility and Inadequate Disclosures.....</i>	<i>46</i>
<i>Targeting .....</i>	<i>47</i>
<i>Privacy and Surveillance Risks.....</i>	<i>49</i>
<b>VI. RECOMMENDATIONS .....</b>	<b>50</b>



# CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES

Executive Order 14067 on Ensuring Responsible Development of Digital Assets; Section 5(b)(i)—the implications of developments and adoption of digital assets and changes in financial market and payment system infrastructures for U.S. consumers, investors, businesses, and for equitable economic growth.

## I. EXECUTIVE SUMMARY

Digital asset markets have changed and grown dramatically over the past decade based on estimates of market capitalization, transaction volumes, and the number and types of assets. Millions of people globally have some exposure to crypto-assets, including at least 12% of Americans. President Biden’s Executive Order on Ensuring Responsible Development of Digital Assets (Executive Order) observes that continued expansion of crypto-based technology could have profound implications for the users of crypto-assets—namely, consumers, investors, and businesses.

Pursuant to the Executive Order, this report reviews the current crypto-asset markets and trends that inform the potential opportunities and risks associated with their use. This report focuses on crypto-assets rather than digital assets more broadly as crypto-assets are currently at the center of the consumer and investor experience.<sup>1</sup> This report also discusses the implications of these opportunities and risks for consumers, investors, and businesses, with an eye towards those aspects affecting populations vulnerable to disparate impacts.

Despite the recent expansion in the number and type of crypto-assets and activities, crypto-asset products are primarily used to trade, lend, and borrow other crypto-assets. Their use in performing other activities is currently limited and the potential for blockchain technology to transform the provision of financial services, as espoused by developers and proponents, has yet to materialize. Nevertheless, it is possible that new products and use cases could emerge.

---

<sup>1</sup> Ensuring Responsible Development of Digital Assets, 87 Fed. Reg. 14143 Section 9(d) (Mar. 9, 2022). The term “digital assets” is defined by the Executive Order to include cryptocurrencies, stablecoins, and Central Bank Digital Currencies (CBDCs). This report uses the term “crypto-assets” to refer to all digital assets that are not CBDCs. The terms used in this report also generally reflect the meanings commonly used by the industry and market participants, with modifications and clarifications as appropriate. While labels may vary, the terms are also meant to be consistent with the meanings used in other reports mandated by the Executive Order. These are not legal definitions, unless otherwise noted, and their use in this report does not suggest the instruments, entities, concepts, or activities are subject to different legal or regulatory frameworks than their analogues in traditional financial markets. The objective behind the use of certain terminology is to emphasize the functions and activities associated with crypto-assets to facilitate an understanding of crypto-asset markets and the attendant opportunities and risks. The context in which crypto-assets are offered, sold, transferred, and otherwise used distinguishes whether a user has the characteristics of a consumer, investor, or business, or some combination of those characteristics. For example, a person engaging in self-directed trading, holding, or staking of crypto-assets with the expectation of realizing price appreciation or earning a return would be characterized as an investor. A person using crypto-assets to pay for goods and services might be characterized, at least in part, as a consumer, and a seller of those goods or services might be characterized as a business. These characterizations are meant to provide readers with a functional understanding of the ways in which the public interact with crypto-assets—they are not meant to convey any conclusions regarding the legal classification of the products, activities, or entities involved. In all cases, users may interact with different intermediaries and may experience varying degrees of exposure to crypto-asset products, services, and technology.

In addition, both the existing use cases, and potential opportunities, come with risks, including conduct and market integrity risks, operational risks, and intermediation risks (i.e., traditional financial risks that have the potential to manifest in particular ways in the crypto-asset markets). Some risks are unique to the crypto-asset ecosystem, while others are versions of those experienced in traditional financial markets that may be heightened when experienced in the crypto-asset ecosystem.

Consumers and investors are exposed to improper conduct in the crypto-asset ecosystem for a variety of reasons, including a lack of transparency as well as the fact that crypto-assets have relatively novel and rapidly developing applications. This leads to frequent instances of operational failures, market manipulation, frauds, thefts, and scams. While the data for populations vulnerable to disparate impacts remains limited, available evidence suggests that crypto-asset products may present heightened risks to these groups, and the potential financial inclusion benefits of crypto-assets largely have yet to materialize.

Consistent with the objective of protecting consumers, investors, and businesses, as well as promoting responsible development of payment innovations and digital assets, this report recommends that relevant agencies adopt a multi-part approach to address relevant risks associated with the crypto-asset sector using their existing authorities. This approach prioritizes the need for urgent action to protect consumers, investors, and businesses, even as stakeholders continue to debate legislative proposals on the subject of crypto-asset market regulation. It builds on and complements actions recommended in other reports pursuant to the Executive Order, including the report under Section 4(b) on the future of money and payments, the report under Section 6(b) on financial stability risks and regulatory gaps, and the report under Section 7(b) on illicit finance risks.

**Recommendation 1:** U.S. regulatory and law enforcement agencies should, as appropriate, vigilantly monitor the crypto-asset sector for unlawful activity, aggressively pursue investigations, and continue to bring civil and criminal actions to enforce applicable laws with a particular focus on consumer, investor, and market protection.

Frauds, thefts, and scams have emerged as an especially grave area of concern in crypto-assets, with estimates of claimed losses reaching billions of dollars and causing material harm to U.S. consumers, investors, and businesses.

**Recommendation 2:** U.S. regulatory agencies should continue using their existing authorities to issue supervisory guidance and rules, as needed, to address current and emerging risks in crypto-asset products and services for consumers, investors, and businesses. Agencies should work collaboratively to promote consistent and comprehensive oversight that addresses the risks identified in this report.

Many U.S. regulatory agencies have already issued guidance or statements related to market participants within their respective jurisdictions. Such actions benefit consumers and investors of crypto-assets and entities offering crypto-asset products and services by reducing uncertainty for business operations and raising conduct standards to facilitate responsible innovation.

The regulators should also review existing regulations and take appropriate steps to address: (i) consumer and investor confusion regarding the regulation of crypto-asset products and services and (ii) gaps in disclosures by market participants promoting crypto-asset products or services and operational and technical obligations of crypto-asset intermediaries.

Crypto-assets are a new and rapidly developing financial product and activity that can implicate the jurisdictions and interests of multiple federal and state regulatory and law enforcement authorities. As such, active collaboration and coordination is necessary to ensure that crypto-asset products, services, activities, and data are subject to, and in compliance with, appropriate supervision, oversight, regulation, collection, and disclosure requirements.

In addition to financial risks, the use of public, also known as “permissionless,” blockchains exposes users to novel forms of operational risks. It is critical that regulators work to address these risks, including through the expanded application of existing operational risk management standards, when possible, and enhanced use of supervisory guidance, as well as alerts to consumers, investors, and businesses to adopt improved diligence tactics.

**Recommendation 3:** U.S. authorities should work individually and through the Financial Literacy and Education Commission (FLEC), as appropriate, to ensure that U.S. consumers, investors, and businesses have access to trustworthy information on crypto-assets.

To help address the extensive risks associated with engagement in crypto-asset markets, as well as the prevalence of frauds, thefts, scams, and other undesirable practices in the sector, the FLEC should coordinate and promote consumer and investor education efforts for crypto-assets, ensuring that consumer- and investor-friendly, trustworthy, and consistent educational materials are accessible and inclusive.

In light of the lack of data and information on the use of crypto-assets by populations vulnerable to disparate impacts, FLEC member agencies should also explore using existing surveys to collect new or additional data that can help facilitate better understanding of the opportunities and risks facing these populations.

Finally, the FLEC should, where appropriate, engage with industry leaders, academics, and other relevant parties to promote and coordinate public and private strategies for financial education outreach to consumers.

## *Listening to the Public*

In drafting this report, Treasury benefitted from the wide-ranging insights of members of the public by issuing a request for comment (RFC). The RFC offered an opportunity for interested parties to provide input, data, and recommendations pertaining to the implications of the development and adoption of digital assets for U.S. consumers, investors, and businesses.

Through the RFC, Treasury received valuable and diverse input from members of the public across the country that reflected a strong desire for engagement. Treasury received over 260 unique responses with over 280 signatories, including over 90 organizations. The submissions were made on behalf of over 10,000 member firms and hundreds of thousands of supporters and individuals. These organizations represent a broad range of stakeholders, including communities impacted by digital asset mining, technology developers, industry stakeholders, financial institutions, consumer advocates, and academics.

The data and insights shared through the RFC demonstrated a variety of views among commenters on the responsible development of digital assets, as well as on the implications for U.S. consumers, investors, and businesses. Commenters generally expressed their desire for action with respect to digital assets and supported the coordinated government approach pursued by the Administration.

Comments submitted in response to the RFC are available at:  
[www.regulations.gov/document/TREAS-DO-2022-0014-0001](http://www.regulations.gov/document/TREAS-DO-2022-0014-0001)

## **II. OVERVIEW OF CRYPTO-ASSET MARKETS ECOSYSTEM**

As directed by the Executive Order, this report discusses the implications of developments and adoption of crypto-assets and changes in financial market and payment system infrastructures for U.S. consumers, investors, businesses, as well as implications for equitable economic growth. The crypto-asset ecosystem is complex, incorporating a number of concepts, entities, and terminology, much of which may not be entirely uniform. To facilitate and frame the subsequent discussion, this part of the report describes key terms and concepts and provides an overview of the crypto-asset markets.

### **Descriptions of Key Terminology**

#### *Crypto-assets*

The central term in this report is “crypto-assets.” Throughout this report, “crypto-assets” refer broadly and generically to all types of representations of value or claims in digital form that rely on the use of a method of distributed ledger technology (DLT),<sup>2</sup> excluding central bank digital currencies (CBDCs).<sup>3</sup>

2 The foundation of the crypto-asset ecosystem is DLT and blockchains. See Section 9(a) of the Executive Order for the relevant definition, which will be used interchangeably, unless the specific context requires a more precise distinction. Technically, a blockchain is a type of DLT, while a digital ledger may or may not be a blockchain. See, e.g., MOHAMMAD JABED MORSHED CHOWDHURY, ALAN COLMAN, MUHAMMAD ASHAD KABIR, JUN HAN & PAUL SARDA, BLOCKCHAIN VERSUS DATABASE: A CRITICAL ANALYSIS (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, 2018), <https://ieeexplore.ieee.org/abstract/document/8456055>.

3 Section 9(b) of the Executive Order defines CBDCs as “a form of digital money or monetary value, denominated in the national unit of account, that is a direct liability of the central bank.” CBDCs are not grouped with other crypto-assets for purposes of this report, and will be addressed by other reports mandated by the Executive Order. The United States currently does not have a CBDC.

Crypto-assets may be original and integral creations of an underlying distributed ledger or blockchain—sometimes referred to as being “native” to a given network. Alternatively, they may be “tokenized” representations of assets, including other crypto-assets or assets issued by traditional financial institutions or entities—such as stocks or bonds—with no initial reliance on DLT. Digital or tokenized representations of assets are also included in the term “crypto-assets.” Industry and market participants may use multiple other terms interchangeably with the term crypto-assets, including “coins” and “tokens.”<sup>4</sup> References in this report to coins and tokens should be taken to refer generically to crypto-assets.

Each type of crypto-asset may have different convertibility, fungibility, and other attributes.<sup>5</sup> While there is no universally accepted industry nomenclature, there are some common terms for various categories of crypto-assets, including what are referred to as “utility tokens” and “governance tokens.” Utility tokens purport to allow users to access products or services on a decentralized platform, discussed more below, while governance tokens claim to confer certain voting rights to holders regarding decisions to influence the operation of a decentralized autonomous organization (DAO) or to govern proposed code changes to other decentralized protocols.<sup>6</sup> Other tokens may seek to tokenize traditional financial assets.

Market participants often distinguish between “fungible” or “non-fungible” tokens, with each type being created according to a different token standard.<sup>7</sup> For fungible tokens, each token unit must be equal in character and value to other token units, and therefore indistinguishable and interchangeable. Stablecoins are an example of one type of fungible token. Stablecoins are designed with the goal of maintaining a stable value, usually in relation to a fiat currency or other assets.<sup>8</sup>

Non-fungible tokens (NFTs) are crypto-assets that are created using software code that is not fungible with other software code. NFTs purport to represent a claim or receipt on an asset or object that has inherently unique characteristics or that differs from similar assets in some distinguishable way. Although NFTs are tradeable, they are not interchangeable. Proponents of NFTs claim they have many potential applications, such as representations of collectible items (for example, art or music), digital goods, individual identification credentials, access keys, property deeds or titles, or tickets for travel or events. However, the legal rights afforded by NFTs are unclear and have been subject to litigation.<sup>9</sup>

4 Another common term is “cryptocurrency.” Section 9(c) of the Executive Order defines cryptocurrencies as referring to “a digital asset, which may be a medium of exchange, for which generation or ownership records are supported through a distributed ledger technology that relies on cryptography, such as a blockchain.” Though the term is in general use by the public, a “cryptocurrency” does not have all the attributes of “real” currency, as defined in 31 C.F.R. § 1010.100(m), including legal tender status.

5 An additional attribute of crypto-assets may be their status as legal tender. A CBDC issued by a central bank would by definition be legal tender. See the report required by Section 4(b) of the Executive Order (Section 4 Report) for additional discussion of CBDCs.

6 A DAO can be described as a system of administration that aspires to operate according to a set of encoded and transparent rules or smart contracts. A DAO governance token allows holders to vote on decisions pertaining to the underlying decentralized finance protocol. See Part IV for a discussion of the risks associated with crypto-asset investments and their governance.

7 On the Ethereum blockchain, for example, fungible tokens can be created according to the ERC-20 Token Standard. See ETHEREUM, *ERC-20 Token Standard*, (May 22, 2022), <https://ethereum.org/en/developers/docs/standards/tokens/erc-20>. Non-fungible tokens, however, can be created according to the ERC-721 Token Standard. See ETHEREUM, *ERC-721 Non-Fungible Token Standard*, (Jun. 23, 2022), <https://ethereum.org/en/developers/docs/standards/tokens/erc-721>.

8 Section 9(e) of the Executive Order defines stablecoins as “a category of cryptocurrencies with mechanisms that are aimed at maintaining a stable value, such as by pegging the value of the coin to a specific currency, asset, or pool of assets or by algorithmically controlling supply in response to changes in demand in order to stabilize value.” For more information on stablecoins, see, e.g., PRESIDENT’S WORKING GROUP ON FINANCIAL MARKETS, THE FEDERAL DEPOSIT INSURANCE CORPORATION & THE OFFICE OF THE COMPTROLLER OF THE CURRENCY, *REPORT ON STABLECOINS* (2021), [https://home.treasury.gov/system/files/136/StableCoinReport\\_Nov1\\_508.pdf](https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf).

9 Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, *FLORIDA LAW REVIEW* (Vol. 74, 2022), at 647, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3928901](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3928901).

## *Wallets, Keys, and Custody*

Another important concept in the crypto-asset ecosystem is the storage of crypto-assets in a digital wallet. A digital wallet is a software application, piece of hardware, or other device or service that stores a user's public and private cryptographic keys, which allow users to interact with one or more blockchains and, *inter alia*, to send and receive crypto-assets. A public key is the cryptographic address that a user shares with others on a blockchain to conduct crypto-asset transactions and must be paired with a user's private key to prove ownership of crypto-assets and to authorize transactions. A private key is the cryptographic password necessary to access the crypto-assets associated with a wallet address, and therefore must be kept secure.<sup>10</sup>

A user's holdings of crypto-assets are not stored in a wallet, but instead are recorded on the blockchain, and can only be controlled with the user's private key. A wallet may be compatible with one specific blockchain (a single-chain wallet), or it may support information from multiple different blockchains (a multi-chain wallet).

Wallets are central to the concept of crypto-asset custody. Custodial wallets, sometimes referred to as "hosted" wallets, are provided and maintained by an intermediary or third-party service provider. Custodial wallets generally can be used to facilitate buying, selling, or transferring of crypto-assets, and are provided by many centralized trading platforms. In contrast, with non-custodial wallets, sometimes referred to as "un-hosted" wallets, users are responsible for their own wallets and private keys.<sup>11</sup> With either type of wallet, if a user's private key is lost, forgotten, or destroyed, for example, there is typically no way to recover access to their crypto-assets.

Digital wallets generally require the use of Internet-connected hardware to receive and transmit the underlying information. While the accessibility of wallets that are directly connected to the Internet (sometimes referred to as "hot wallets") makes them more user-friendly,<sup>12</sup> they can also be more vulnerable to theft and fraud and therefore pose more risks to users. In contrast, "cold wallets" allow users to store their private keys in a physical storage device or other piece of hardware that is maintained offline, making it remote from hacking attempts, but that can be brought online to conduct transactions. Depending on how it is physically stored, a cold-storage wallet can also be vulnerable to loss, theft, damage, or destruction. Just like physical wallets can be lost or stolen, crypto-asset wallets can be hacked, or private keys can be lost or compromised, leading to a loss of funds or credentials.

A crypto-asset custodian could be a bank, broker-dealer, or other traditional financial institution, or it could be a financial technology (fintech) company. Custody involves holding the customer's private key that controls access to their crypto-asset holdings. Custodians might safekeep crypto-asset owners' keys by encrypting them or using a cold storage system (generating and keeping keys offline)

---

10 A private key is used as part of an asymmetric cryptographic algorithm such that it, when paired with another unique element of cryptographic data, is necessary to decrypt data or authorize a transaction. See, e.g., DYLAN YAGA, PETER MELL, NIK ROBY & KAREN SCARFONE, BLOCKCHAIN TECHNOLOGY OVERVIEW 11 (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Internal Report-8202, 2018), <https://nvlpubs.nist.gov/nistpubs/jr/2018/NIST.IR.8202.pdf>.

11 See Vishal Chawla, *Slope wallet provider saved user seed phrases in plain text, Solana security researchers find*, THE BLOCK (Aug. 4, 2022), <https://www.theblock.co/post/161425/slope-wallet-provider-saved-user-seed-phrases-in-plain-text-solana-security-researchers-find>.

12 Many hot wallets are free, tend to be easier for consumers and investors to use, and because they are often connected to a platform or "exchange," they may support a large number of tokens and coins.

and may provide direct custody (i.e., manage customers' crypto-assets themselves) or use a sub-custodian. As discussed more below, there are questions as to which party (the owner or custodian or sub-custodian) has ownership or control over crypto-assets held in hosted wallets, which has important implications in the event of the bankruptcy or receivership of the custodial or sub-custodial provider.<sup>13</sup>

## Entities Providing Services or Products in Crypto-asset Markets

Many types of entities in the crypto-asset ecosystem provide a variety of services or products to consumers, investors, and businesses. Many of the early movers in the space are native to the digital ecosystem and attempt to facilitate the use of services or products that rely on the operation of the underlying blockchain or distributed ledger technology. Recent entrants include more traditional financial intermediaries seeking to facilitate their customers' participation in crypto-asset markets. Some relevant crypto-asset entities are described below.

### *Crypto-asset Platforms*

Crypto-asset platforms or “exchanges” facilitate an array of activities in various types of crypto-assets, including coins, tokens, stablecoins, and NFTs.<sup>14</sup> These platforms may be, for example, facilities or systems that bring together multiple buyers and sellers of crypto-assets to trade.<sup>15</sup> The number and prevalence of crypto-asset platforms has grown along with the proliferation of coins and tokens and as more consumers and investors have entered the space.

Some registered futures or securities exchanges are offering certain types of registered and regulated crypto-asset-based products, such as futures contracts or exchange-traded funds, alongside their more traditional product offerings. Most crypto-asset platforms, however, are relatively new or recently created facilities and systems formed by technology firms focusing exclusively on crypto-assets. Such platforms may take the position that they operate outside of existing regimes of market regulation, which may not be accurate and may create risk for investors and consumers.<sup>16</sup>

**Crypto-asset platforms take two forms, “centralized” and “decentralized,” each of which implicates distinct opportunities and risks for consumers, investors, and businesses.<sup>17</sup>**

13 See Part IV, Risks and Exposures for Consumers, Investors, and Businesses, for discussions of bankruptcy, safekeeping, and custody of crypto-assets.

14 Crypto-asset platforms are commonly referred to in the media and by the industry as “exchanges.” In the context of U.S. market regulation, however, the term “exchange” is generally reserved for certain entities such as national securities exchanges (i.e., stock exchanges) or designated contract markets (i.e., futures exchanges) that are registered (or exempt from registration by rule or order) with either or both the Securities and Exchange Commission or the Commodity Futures Trading Commission. Unless explicitly noted otherwise—for example, through use of the phrase “registered exchange”—use of the term exchange in this report does not imply registration with or regulation by any regulatory authority and, for this reason, use of the more generic term “platform” is preferred. It should be noted that because an entity is referred to as a “platform” does not mean that it does not have a legal obligation to register as an exchange with the proper agency or agencies.

15 IOSCO, ISSUES, RISKS AND REGULATORY CONSIDERATIONS RELATING TO CRYPTO-ASSET TRADING PLATFORMS 4 (2020), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf>.

16 See, e.g., SEC, ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS IN THE MATTER OF BLOCKFI LENDING, LLC (2022), <https://www.sec.gov/litigation/admin/2022/33-11029.pdf>.

17 “Centralized” and “decentralized” are the terms most commonly used by the industry and market participants to distinguish types of platforms, and therefore are used in this report. However, because the true degree of a platform's claimed decentralization is often low or unclear, others have suggested distinguishing platforms as either “permissioned” or “permissionless” systems, respectively. See, e.g., David Rosenthal, *Regulating “Digital Assets,”* DSHR's BLOG (Jul. 27, 2022), <https://blog.dshr.org/2022/07/regulating-digital-assets.html>.

## Centralized Platforms (Traditional Venues and Crypto-asset Trading Platforms)

Registered exchanges and other traditional venues in the United States have begun to offer indirect exposure to crypto-asset products. Contract markets designated by the Commodity Futures Trading Commission (CFTC) (DCMs) offer crypto-asset futures and options contracts to enable investors to hedge positions in, or gain indirect exposure to, crypto-assets.<sup>18</sup> Similarly, national securities exchanges registered with the Securities and Exchange Commission (SEC) offer investors indirect exposure to crypto-assets by trading securities such as stocks of public companies whose businesses are related to crypto-assets. Other types of products trade on over-the-counter venues.<sup>19</sup>

Registered exchanges and other traditional venues carry fewer of the risks seen in other crypto-asset trading platforms and decentralized finance because they, and their members and intermediaries, are registered, regulated, overseen by relevant federal agencies, and subject to numerous regulatory requirements. The requirements for exchanges, their members and other intermediaries include, among other things:

- (I) Conducting customer identification and verification, recordkeeping and reporting obligations, and obligations to comply with requirements regarding anti-money laundering countering the financing of terrorism (AML/CFT) and the Bank Secrecy Act (BSA);
- (II) Providing secure custody of customer assets;
- (III) Ensuring trade execution and settlement;
- (IV) Maintaining and complying with rulebooks;
- (V) Reporting to regulators and the public; and
- (VI) Complying with disclosure obligations and business conduct standards.

Registered exchanges are also self-regulatory organizations (SROs) and as such have certain responsibilities for promoting market integrity by setting and enforcing industry and membership rules and standards.<sup>20</sup>

Centralized crypto-asset platforms (CEXs) facilitate, as a primary service, direct (or spot) trading of crypto-assets by users.<sup>21</sup> Some CEXs also facilitate trading in crypto-asset based derivatives, such as futures and options. CEXs may require users to undergo customer verification. They also are the only part of the crypto-asset ecosystem that allows users to deposit U.S. dollars. CEXs require users to deposit crypto-assets or fiat currency into an account on the platform before being eligible to trade, and they provide a means for consumers and investors to cash out their crypto-asset holdings back

---

18 In December 2017, the Chicago Mercantile Exchange (CME) and Chicago Board Options Exchange (CBOE) launched futures contracts on bitcoin (though CBOE stopped offering bitcoin futures contracts in 2019) and later other exchanges (e.g., ICE Futures US, and FTX US Derivatives) began offering crypto-assets futures contracts.

19 There are exchange-traded funds (ETFs), registered with the SEC, that trade in CME's bitcoin futures contracts, but to date, the SEC has not approved any of the many applications it has received for a spot crypto-asset exchange traded product.

20 Apart from the exchanges, there are industry-wide SROs, including the Financial Industry Regulatory Authority (FINRA) and the National Futures Association (NFA). Exchange members are generally subject to FINRA or NFA rules.

21 Other sources or authorities may use different labels to refer to entities that this report refers to as CEXs. For example, the IOSCO uses the term "centralized crypto-asset trading platforms." See, e.g., IOSCO, IOSCO DECENTRALIZED FINANCE REPORT (2022), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf>.

into fiat currency. As a result, CEXs are sometimes referred to as the “on-ramps” and “off-ramps” in the crypto-asset ecosystem.

Currently, U.S.-based CEXs that facilitate trading in spot crypto-asset transactions generally operate as money services businesses (MSBs) under the regulations of Treasury’s Financial Crimes Enforcement Network (FinCEN) and are therefore subject to AML/CFT obligations.<sup>22</sup> CEXs may also hold state money transmission licenses and may be subject to, among other requirements and depending on the states in which they operate, permissible investment requirements, reporting requirements, bonding requirements, and inspection by state regulatory agencies. However, the consumer and investor protections offered by these state-based jurisdictions vary and are typically fewer and less extensive than federal laws applicable to securities and derivatives markets and products or consumer financial products and services.

Simply registering with FinCEN or states as an MSB or money transmitter does not absolve a CEX of its other relevant legal obligations. Any activity with U.S. residents involving crypto-assets that are derivatives or securities falls under the jurisdiction of the CFTC or SEC. For example, if a CEX offers trading of crypto-assets that are securities and operates as an exchange, as defined under federal securities laws, then the platform must either register with the SEC as a national securities exchange or qualify for an exemption from registration.<sup>23</sup> Similarly, a CEX that offers a trading facility for U.S. customers to trade futures, options, or swaps referencing crypto-assets that are commodities must register with the CFTC as a designated contract market or swap execution facility.

Unlike registered exchanges, CEXs generally have no exchange member firms or other intermediaries and have no self-regulatory functions. A CEX itself is often the intermediary between buyers and sellers of crypto-assets and typically provides many, or all, of the services necessary to trade crypto-assets (e.g., trading, custody,<sup>24</sup> and transfers) for both crypto-assets and fiat currencies.<sup>25</sup> As discussed in Part IV, the risks associated with CEXs that are not in compliance with U.S. laws and regulations, or that may not be regulated, are significant. Whether a CEX is properly registered, and the associated risks of transacting with CEXs compared to registered exchanges, therefore carries important implications for customers using CEXs to trade crypto-assets, many of whom may be confused or misled by a CEX’s marketing and promotional materials.

---

22 FinCEN published interpretive guidance in March 2013 stating an administrator or exchanger of “convertible virtual currency” is an MSB under FinCEN’s regulations, specifically a money transmitter, with limited exceptions. See FinCEN, *Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, (Mar. 18, 2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>. CEXs are also subject to sanctions imposed by Treasury’s Office of Foreign Assets Control and other U.S. government agencies, as well as other types of government-imposed restrictions that apply to U.S. persons, such as export controls.

23 See SEC, *Statement on Potentially Unlawful Online Platforms for Trading Crypto-assets*, (Mar. 7, 2018), <https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading>. An SEC-registered trading platform would be exempt from FinCEN’s MSB regulations, pursuant to 31 CFR 1010.100(ff)(8)(ii). However, to date, no CEX or other crypto-asset platform has registered with the SEC as a national securities exchange, and some CEXs operating today might indeed be unregistered exchanges under the federal securities laws. Many CEXs claim there is “legal uncertainty” as to the registration and regulatory status of CEXs under U.S. securities and derivatives laws and are not currently registered, while relying on MSB and state money transmission licenses in order to operate in the United States.

24 Such custodial arrangements, however, do not involve the same types of customer protection rules—such as segregation and permissible investment requirements, or any type of insurance—that apply to traditional financial intermediaries.

25 For example, a CEX may offer the following services to facilitate user access and trading: trading spot and derivatives on multiple coins and tokens, including stablecoins; custody services for crypto-assets; payment, exchange, and other agent services; loan origination and trading; insurance; and access to decentralized crypto-asset platforms. In addition, some CEXs have expanded their services to include other related activities, such as crypto-asset mining.

## Decentralized Platforms (DeFi Protocols)

Decentralized crypto-asset platforms or protocols are a prominent part of the crypto-asset ecosystem. The term “decentralized” commonly refers to the provision of financial products, services, arrangements, and activities that use DLT in an effort to disintermediate and decentralize legacy ecosystems by eliminating the need for certain traditional financial intermediaries and centralized institutions.<sup>26</sup> Decentralized platforms include what are referred to as decentralized exchanges (DEXs) and other types of platforms referred to as decentralized finance (DeFi) protocols.<sup>27</sup>

Like centralized platforms (both traditional exchanges, with respect to crypto-asset derivatives and securities, and CEXs), decentralized platforms offer users the ability to trade crypto-assets and to engage in a variety of other crypto-asset-based activities, such as lending and borrowing crypto-assets. Decentralized platforms typically do not conduct customer verification on their users, nor do they implement other AML/CFT measures. Like many centralized platforms for crypto-assets, or CEXs, DeFi platforms or protocols—which are designed to enable peer-to-peer market transactions, without a centralized intermediary controlling users’ funds or access—also are not currently registered with the SEC or CFTC and therefore may be operating in non-compliance with U.S. law and regulation.

Proponents of DeFi protocols see the purported absence of intermediation as a benefit that allows users to make trades and move their assets wherever and whenever they want, without having to wait for bank transfers or pay bank fees. However, as others have observed, the miners and validators that are critical to the execution of any transaction on DeFi trading or lending platforms play an important intermediation role.<sup>28</sup> Further, a lack of industry-recognized operational control frameworks, conduct standards, or other self-policing mechanisms often leaves users exposed to a number of risks specific to DeFi protocols,<sup>29</sup> as well as some of the same risks as with unregistered or unregulated CEXs. As a result, it is important for investors, consumers, and other market participants to be made aware of the fact that they are exposed to greater risks when engaging with DEXs.<sup>30</sup> See Part IV for further discussion of risks in DeFi.

Many DeFi protocols claim not to rely on a formal centralized governance structure. Specifically, organizers of DeFi protocols aspire to operate autonomously, with little or no governance structure. In practice, many DeFi protocols adopt governance elements. For instance, the organizers of a DeFi protocol may employ a DAO in which (i) participants may have the ability to maintain direct real-time control of contributed funds and (ii) governance rules may be formalized, automated, and enforced

26 See IOSCO, *supra* note 21.

27 Currently, there is no generally accepted definition of “DeFi,” or what makes a product, service, arrangement, or activity “decentralized.” Further, as noted with respect to CEXs, other sources or authorities may use different labels for entities referred to in this report as DEXs or DeFi protocols. For example, because DeFi protocols use smart contracts in some part of the application, DeFi participants sometimes refer to such protocols as “decentralized applications” or “dApps.”

28 RAPHAEL AUER, JON FROST & JOSE MARIA VIDAL PASTOR, MINERS AS INTERMEDIARIES: EXTRACTABLE VALUE AND MARKET MANIPULATION IN CRYPTO AND DeFi (BANK FOR INTERNATIONAL SETTLEMENTS (BIS), BIS Bulletin No. 58, 2022), <https://www.bis.org/publ/bisbull58.pdf>.

29 The term “decentralized finance” should be viewed critically as it may not represent accurately the reality in decentralized markets today. See Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, BIS (BIS Quarterly Review, Dec. 2021), [https://www.bis.org/publ/qtrpdf/r\\_qt2112b.pdf](https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf). Although most activities in the decentralized crypto-assets space have corollaries in traditional finance, these activities are—for the most part—currently limited to facilitating yield-enhancing, speculative, and leveraged activities in crypto-assets. See IOSCO, *supra* note 21.

30 See Caroline Crenshaw, *DeFi Risks, Regulations, and Opportunities*, INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW (Vol. 1, 2021), at 4, 7, <https://gbbccouncil.org/wp-content/uploads/2021/11/IJBL-1.pdf>.

using smart contracts or other software.<sup>31</sup> For example, in exchange for depositing a crypto-asset, a protocol smart contract may create new tokens that are assigned to the wallet address of the person who sent the asset. The number of tokens created may be proportional to the amount of crypto-asset transferred. The new tokens representing the initial crypto-asset deposit can then be effectively rehypothecated—lent out or used as collateral on other platforms. The protocol may separately issue reward tokens on occasion for being a user of the platform, and those reward tokens in turn may be governance tokens that grant its holder certain voting and ownership rights. Holders of a sufficient number of governance tokens may be able to raise governance or procedural topics (e.g., certain changes to the code) that may be implemented if a sufficient number of users vote for the proposal. Within this framework, decentralization does not necessarily equate to wide distribution, and the ownership of voting rights and tokens many governance tokens can be highly concentrated.<sup>32</sup>

There are possibly thousands of DeFi protocols, though only a small number experience significant user activity. One frequently cited data aggregator reportedly tracks more than 1,800 different DeFi protocols across 27 different categories with a combined “total value locked” (or “TVL”) of \$86.0 billion as of August 19, 2022.<sup>33</sup> The most prominent category of DeFi protocols includes those that facilitate the trading of crypto-assets (i.e., DEXs), reportedly with 516 separate platforms with a combined \$26.3 billion in TVL.<sup>34</sup>

In contrast to the type of trade matching typically carried out on centralized platforms (such as central limit order books), some DEXs rely on liquidity pools and automated market-making enabled by smart contracts to facilitate trading and other types of services. After DEXs, lending and borrowing DeFi protocols reportedly have the greatest TVL at \$17.3 billion across 164 separate platforms; there are also reportedly 338 protocols that pay users a reward for staking crypto-assets on the platform—so-called “yield” protocols—with over \$8.4 billion TVL.<sup>35</sup>

### *Miners and Validators*

Mining is the process of using a consensus mechanism to verify and add transactions to a distributed ledger in exchange for newly minted crypto-assets that compensate participants in the consensus mechanism.<sup>36</sup> Miners or validators are a decentralized network of actors who compete to add new entries, or “blocks,” to a public ledger or blockchain. These actors typically use a consensus

---

31 See SEC, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO (2017), <https://www.sec.gov/litigation/investreport/34-81207.pdf>.

32 One recent analysis found that among several major DAOs, less than 1% of token holders controlled 90% of the voting power. See CHAINALYSIS, *Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated*, (Jun. 27, 2022), <https://blog.chainalysis.com/reports/web3-daos-2022>. Also, the amount of governance tokens a user must either own or be delegated to raise new proposals may be extremely high.

33 DEFI LLAMA, *TVL Rankings*, <https://defillama.com>. TVL, an industry reported metric, is the amount of user funds deposited or “locked” in a DeFi protocol, and is used as a measure to gauge the size of the DeFi market or the degree of adoption or acceptance by users. TVL information is not audited or verified, may double-count funds, and therefore may not be a reliable metric. See IMF, GLOBAL FINANCIAL STABILITY REPORT: COVID-19, CRYPTO, AND CLIMATE 42 (2021), <https://www.imf.org/en/Publications/GFSR/Issues/2021/10/12/global-financial-stability-report-october-2021>.

34 DEFI LLAMA, *supra* note 33.

35 *Id.*

36 While blockchains are foundational to the crypto-asset ecosystem, not every transaction in, activity relating to, or ownership of crypto-assets is reflected in a distributed ledger. Though transactions, activities, and balances may take place and be recorded on a blockchain (referred to as “on-chain”), many occur or are maintained “off-chain,” sometimes through third parties or intermediaries.

mechanism—such as proof-of-work (PoW) or proof-of-stake (PoS), depending on the design or architecture of the blockchain—to carry out the work of updating a blockchain. Miners typically are compensated for this work by receiving fees, called “gas fees” in the case of the Ethereum blockchain, and in some cases, “block rewards,” both of which are paid or issued in the blockchain’s native token.<sup>37</sup> As with DeFi ownership, mining activities may be concentrated, and indeed have become increasingly dominated in recent years by organizations with large-scale operations.<sup>38</sup> Some of the largest miners are public companies.

### *Data Aggregators*

The crypto-asset ecosystem generates a vast amount of information. Accurate and reliable data is critical to maintaining market integrity, including identifying potential money launderers and terrorist financiers, market manipulators, fraudsters, and other actors attempting to conduct illicit financial activity or take advantage of consumers, investors, and businesses. Crypto-asset and DeFi markets operate globally on a 24/7 basis, producing a constant flow of data about transactions, coin and token prices, trading volumes, and other financial metrics and activities taking place on- and off-chains. Where assets or transactions occur on public blockchains, such as through DEXs or other DeFi protocols, the information is recorded on the underlying ledger and is in theory completely open and transparent to all market participants.<sup>39</sup>

Data pertaining to off-chain activity is extremely limited and subject to voluntary disclosure by trading platforms and protocols. As a result, the quality of off-chain data is less verifiable, and coin and token prices (and other data) may differ markedly between platforms.<sup>40</sup> Unlike traditional registered exchanges, CEXs and DeFi protocols operating today either are not complying with, or are not subject to, obligations to report accurate trade information periodically to regulators or to ensure the quality, consistency, and reliability of their public trade data.

### *Traditional Financial Institutions*

Traditional financial institutions such as banking institutions, broker-dealers, investment advisers, futures commission merchants (FCMs), and clearinghouses are increasingly expressing interest to enter the crypto-asset ecosystem and seeking ways to provide crypto-asset services to consumers, investors, and businesses in response to growing demand. Traditional intermediaries are exploring a range of services relying on DLT, such as providing custody for crypto-assets, holding reserves for

---

37 “Gas” is a term associated with the Ethereum blockchain that refers to a unit of payment for the computational effort of conducting transactions or smart contract functions. Gas is measured in small bits called “gwei,” with each gwei equaling 0.000000001 (one-billionth) ETH. The “gas price” on the network at any given moment is driven by demand, transaction congestion, and other factors.

38 See, e.g., IGOR MAKAROV & ANTOINETTE SCHOAR, BLOCKCHAIN ANALYSIS OF THE BITCOIN MARKET (NATIONAL BUREAU OF ECONOMIC RESEARCH (NBER), Working Paper No. 29396, 2021), <https://www.nber.org/papers/w29396>. The report found that the top 10% of miners control 90% of the Bitcoin mining capacity, and the top 0.1%—about 50 miners—control 50% of mining capacity.

39 While this transparency benefits the entire ecosystem, ordinary consumers and investors may themselves benefit less directly depending upon whether they are technically able to access, process, and comprehend raw blockchain data.

40 As recently as 2021, researchers estimated that over 70% of all crypto-assets volumes were wash trades, with such “fabricated volumes” serving to improve exchange ranking and temporarily distorting prices. See, e.g., LIN WILLIAM CONG, XI LI, KE TANG & YANG YAN, CRYPTO WASH TRADING (SOCIAL SCIENCE RESEARCH NETWORK, 2021), <http://dx.doi.org/10.2139/ssrn.3530220>.

stablecoin issuers, facilitating payments,<sup>41</sup> and expanding credit and investments in native crypto-asset companies.<sup>42</sup> Some banking institutions are specializing in the crypto-assets space and offering clients services such as lending (providing fiat loans collateralized by crypto-assets), staking (placement of coins and tokens in protocols or pools to earn interest), and governance services (allowing participation in on-chain governance from within the institution’s user interfaces).

### III. CRYPTO-ASSET MARKET TRENDS, USES, AND OPPORTUNITIES

While features of crypto-asset projects and technologies vary significantly, a common feature attributed to the use of blockchain technology is a reduced reliance on intermediaries, including the possibility to facilitate the secure transfer of value between parties without the use of a mutually trusted third party.<sup>43</sup> The distributed model of record keeping and computing also introduces the possibility of more direct peer-to-peer and fully automated transactions, which together may produce future benefits associated with: faster settlement of financial transactions; new financial products; and direct access to asset networks by individual consumers, investors, and businesses. To date, however, competing technologies, applications, and paradigms for adoption have produced a patchwork of systems that have yet to deliver, separately or collectively, on many of the promised benefits for consumers, investors, and businesses, including complete disintermediation or satisfactorily addressing some of the drawbacks of moving away from an intermediated model of finance.<sup>44</sup> These and other rapidly evolving dynamics are likely to impact the degree to which these products and services are more widely adopted over time.

#### Market Size

On January 1, 2020, on the eve of the COVID-19 pandemic, the market capitalization of Bitcoin—the first and largest crypto-asset by price and market capitalization—was about \$130.6 billion, down from the previous high of about \$320.6 billion in December 2017.<sup>45</sup> During the pandemic, the market

---

41 The OCC has instructed that before engaging in these crypto-assets activities, a national bank or federal savings association should notify its supervisor of its intent and receive notification of its supervisor’s non-objection. See, e.g., OCC, *Chief Counsel’s Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank*, (Interpretive Letter No. 1179, Nov. 18, 2021), <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1179.pdf>. The FDIC has requested all FDIC-supervised institutions that are considering engaging in crypto-related activities to notify the FDIC of their intent and to provide all necessary information that would allow the FDIC to engage with the institution regarding related risks. See FDIC, *Notification of Engaging in Crypto-Related Activities*, (Apr. 7, 2022), <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html#letter>.

42 See Carla Mozee, *These 13 Banks Have Invested The Most In Crypto And Blockchain To Date*, MARKETS INSIDER, (Aug. 15, 2021), <https://markets.businessinsider.com/news/currencies/13-top-banks-investing-cryptocurrency-blockchain-technology-funding-blockdata-bitcoin-2021-8>.

43 See, e.g., MICHAEL CASEY, JONAH CRANE, GARY GENSLER, SIMON JOHNSON & NEHA NARULA, *THE IMPACT OF BLOCKCHAIN TECHNOLOGY ON FINANCE: A CATALYST FOR CHANGE*, (INTERNATIONAL CENTER FOR MONETARY AND BANKING STUDIES, 2018). However, others note that “a review of blockchain research suggests that true disintermediation might be possible in some finance areas but not all,” and that “despite Bitcoin’s disintermediation from conventional financial infrastructure, it is still important to build up a new infrastructure with intermediation to allow the conversion between Bitcoin and fiat currencies to occur.” See Cynthia Weiyi Cai, *Disruption of financial intermediation by FinTech: a review on crowdfunding and blockchain*, ACCOUNTING AND FINANCE (Vol. 58 Issue 4, Dec. 12, 2018), at 965-992, <https://onlinelibrary.wiley.com/doi/full/10.1111/acfi.12405>.

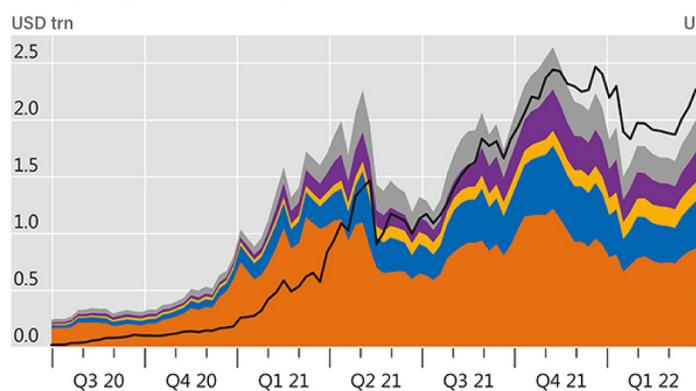
44 Cynthia Weiyi Cai, *supra* note 43. See also Moxie Marlinspike, *My first impressions of web3*, MOXIE (Jan. 7, 2022), <https://moxie.org/2022/01/07/web3-first-impressions.html>.

45 A chief concern with these market measures is the accuracy and reliability of the data available given the lack of a standardized reporting regime. See, e.g., Javier Paz, *More Than Half of All Bitcoin Trades Are Fake*, FORBES (Aug. 26, 2022), <https://www.forbes.com/sites/javierpaz/2022/08/26/more-than-half-of-all-bitcoin-trades-are-fake/?sh=fe4e626681f7>.

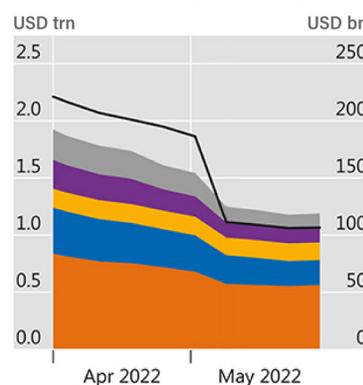
capitalization of Bitcoin increased again, reaching its all-time high of nearly \$1.3 trillion in November 2021, before declining significantly thereafter.<sup>46</sup> As of August 20, 2022, the market capitalization of Bitcoin is around \$404.8 billion.<sup>47</sup> Over the same period, there has been seemingly exponential growth in the number of coins and tokens, with an estimated handful of crypto-assets in 2013, to more than 2,800 by the end of 2019, to nearly 10,400 as of early 2022, according to one source.<sup>48</sup> The aggregate market capitalization of all crypto-assets also experienced expansive growth and volatility: from just under \$200 billion in January 2020 to approximately \$2.9 trillion in November 2021, before falling to less than \$1.0 trillion in June 2022.<sup>49</sup> The chart below illustrates this trend.

## Market size of cryptocurrencies and DeFi

A. Rapid growth in crypto and DeFi...



B. ...Followed by a collapse



Market cap (lhs): Bitcoin Stablecoins Others  
Ether DeFi coins

Total value locked (rhs): — DeFi

Sources: CoinGecko; DeFi Llama; BIS.

At the same time, the number of centralized and decentralized platforms available to consumers, investors, and businesses has proliferated, offering the possibility to engage in an ever-changing variety of financial, as well as non-financial, activities. Different types of crypto-assets, including cryptocurrencies and other native fungible coins and tokens, NFTs, and tokenized forms of traditional assets, have developed at different rates.

46 COINMARKETCAP, *Bitcoin: Historical Data for Bitcoin*, <https://coinmarketcap.com/currencies/bitcoin/historical-data>.

47 *Id.*

48 STATISTA, *Number of cryptocurrencies worldwide from 2013 to February 2022*, (Mar. 22, 2022), <https://www.statista.com/statistics/863917/number-crypto-coins-tokens>. Other sources identify many more coins and tokens. For example, Etherscan lists over 500,000 ERC-20 tokens, though most may not trade and do not have meaningful market values. See ETHERSCAN, *Token Tracker*, <https://etherscan.io/tokens>. Another source estimates that in DeFi there are over 1.7 million tokens, of which approximately 10% have been identified by the source to be scams. See TOKENSNIFFER, <https://tokensniffer.com>.

49 COINMARKETCAP, *Global Cryptocurrency Charts: Total Cryptocurrency Market Cap*, <https://coinmarketcap.com/charts>. See also Josh Zumbrun, *Why Crypto's Market Cap Never Booms, or Busts, as Much as You Think*, THE WALL STREET JOURNAL (Aug. 5, 2022), <https://www.wsj.com/articles/why-cryptos-market-cap-never-booms-or-busts-as-much-as-you-think-11659691802>. The article suggests that most market capitalization measures are overestimates because they include crypto-assets that are unrecoverable due to loss of keys and other factors.

## Current Uses and Opportunities in Crypto-assets for Consumers, Investors, and Businesses

The current uses of native crypto-assets and tokenized traditional assets are limited. These can be grouped into three broad categories, including: (i) crypto-asset-based alternatives to traditional financial products and services; (ii) financial market and payment system infrastructures; and (iii) potential cases for other consumer and commercial uses by individuals and businesses (e.g., NFTs, gaming, records, identity, supply chain management). Specific uses, which are in various stages of development or implementation, include:

- Financial markets, products, and services that use native crypto-assets consist primarily of trading, lending, and collateral activities of other crypto-assets and are generally speculative in nature;
- Limited instances of use as a medium of exchange for goods and services;
- Market and payment system infrastructures for traditional assets using permissioned blockchains; and
- Technological innovations to transform commercial activities to attract more significant adoption, most of which are at the pilot stage and face obstacles.

The following discussion addresses relevant issues with both native and tokenized use cases, as well as potential opportunities, including the role of technological innovation. While the discussion contains examples of potential opportunities using blockchain technology, crypto-asset transactions using CEXs at present generally occur off-chain rather than on-chain.<sup>50</sup> It should also be noted that technologists disagree about the value of certain use cases, and the potential utility of blockchains more generally.<sup>51</sup>

### *Native Crypto-asset Financial Markets, Products, and Services*

Native crypto-asset activities take a variety of forms. As with other crypto-asset-related activities, the form of the activity may be less relevant than its underlying function.<sup>52</sup> As noted above, the most predominant use cases to date consist of trading, lending, and investing, although there are efforts underway to increase the scale of other consumer use cases. Adoption by U.S. adults of cryptocurrency to-date—which has been growing—has primarily been for investing purposes, with the adoption for payments or remittances remaining limited. According to the Survey of Household Economics and Decisionmaking (SHED) conducted by the Federal Reserve in October and November 2021, 12% of adults in the United States held or used cryptocurrencies in the prior year,<sup>53</sup> substantially

---

50 See Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *supra* note 29, at 26.

51 See Letter in Support of Responsible Fintech Policy, dated Jun. 1, 2022, <https://concerned.tech>.

52 See Jay Clayton, Chairman, SEC, Statement on “Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission” at 5 (Feb. 6, 2018), <https://www.banking.senate.gov/imo/media/doc/Clayton%20Testimony%202-6-18.pdf>. Former Chairman Clayton noted that “simply calling something a ‘currency’ or a currency-based product does not mean that it is not a security.”

53 BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, ECONOMIC WELL-BEING OF U.S. HOUSEHOLDS IN 2021 45 (2022) <https://www.federalreserve.gov/publications/files/2021-report-economic-well-being-us-households-202205.pdf>.

higher than results from 2015, when a private survey found that 1% of U.S. adults said they had ever collected, traded, or used the individual cryptocurrency Bitcoin.<sup>54</sup>

## Trading

Trading is currently the most common activity in the crypto-asset ecosystem. For example, as with traditional trading markets, crypto-asset trading markets include short-term traders, arbitrageurs, and “buy and hold” investors hoping to profit from long-term price appreciation. A large share of trading volume is in stablecoins, which are used as collateral on crypto-asset platforms and protocols, and which facilitate trading and lending of other crypto-assets, borrowing, and other activities. Traders engage both in spot market trading of crypto-assets, as well as crypto-asset-based derivatives such as futures and options. Since 2020, the market for crypto-asset-based derivatives has grown significantly and now accounts for 69% of total crypto-asset volumes, outpacing the spot market.<sup>55</sup> According to reports, institutional investors, rather than retail investors, comprise a majority of the trading activity in crypto-asset markets.<sup>56</sup>

Both CEXs and DEXs generate revenues through trading fees, which can vary significantly among different platforms. Further, trading on DEXs generally includes gas fees to compensate miners and validators for contributing the computing and storage resources necessary to verify and write transactions to a blockchain. Gas fees add to the costs of transacting and can vary widely depending on the complexity of a transaction and the congestion on the blockchain.

Participation in DEX and DeFi protocols’ liquidity pools, whereby users pool and lock their assets in the platform’s smart contract, relies on a profit-sharing model.<sup>57</sup> The assessment of fees, the transparency of trading standards on platforms, liquidity pools’ operations, sufficiency of cybersecurity protections, and adequacy of disclosures all subject users to significant risks. These risks are discussed in more detail in Part IV.

## Lending, Borrowing, Staking, and Collateral

CEXs or DEXs may also offer other yield-generating activities, including lending and borrowing and staking services, sometimes referred to by platforms and users as “yield farming.” Numerous

---

54 Andrew Perrin, *16% of Americans say they have ever invested in, traded or used cryptocurrency*, PEW RESEARCH CENTER (Nov. 11, 2021), <https://www.pewresearch.org/fact-tank/2021/11/11/16-of-americans-say-they-have-ever-invested-in-traded-or-used-cryptocurrency>. This Pew Research Center survey, conducted in September 2021, found that 16% of U.S. adults say they personally have invested in, traded or otherwise used crypto-assets like Bitcoin or Ether. An updated survey carried out in July 2022 shows that this finding is unchanged from September 2021. See Michelle Faverio & Navid Massarat, *46% of Americans who have invested in cryptocurrency say it’s done worse than expected*, PEW RESEARCH CENTER (Aug. 23, 2022), <https://www.pewresearch.org/fact-tank/2022/08/23/46-of-americans-who-have-invested-in-cryptocurrency-say-its-done-worse-than-expected>.

55 See CRYPTOCOMPARE, EXCHANGE REVIEW 13 (2022), [https://www.cryptocompare.com/media/40485073/exchange\\_review\\_july\\_vf-1.pdf](https://www.cryptocompare.com/media/40485073/exchange_review_july_vf-1.pdf). Most of this activity currently is taking place on non-U.S. CEXs and DeFi protocols. Nevertheless, derivatives trading typically involves the use of leverage—i.e., the practice of placing outside bets with only a small amount of money upfront, often involving margin or borrowed funds—to amplify returns. But leverage can also work against traders when prices decline, by leading to rapid liquidation of their positions and collateral.

56 See George Steer, *Did Institutional Investors Crash the Crypto Party?*, FINANCIAL TIMES (May 13, 2022), <https://www.ft.com/content/12b80e7f-047d-4273-8766-226b5d91a1fc>.

57 Liquidity pools in turn rely on automated market-maker (AMM) protocols which use preset mathematical equations (e.g.,  $x*y=k$ , where  $x$  and  $y$  represent the values of tokens in a liquidity pair and  $k$  is a constant) to ensure the ratio of assets in the liquidity pools remains balanced and determine prices based on trading volumes. For a discussion of AMMs, including certain features of AMMs that may expose liquidity-takers to market manipulation on DEXs, see Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *supra* note 29, at 34-35.

centralized crypto-asset lending platforms offer products that are marketed as forms of high-yield savings or deposit-like products in different forms under which users can lend out their crypto-assets. In these scenarios, crypto-assets serve as the sole source of collateral used to facilitate transactions involving other crypto-assets.<sup>58</sup> Platforms may attract users by promising to pay returns that are far greater than those offered by traditional banks, and inappropriately use bank-like terms such as “savings account,” “deposit,” or annual percentage yield (APY) and other promotional tactics that can obscure the associated risks.

The source of the high yields on these types of products is not entirely clear, but crypto-asset firms purport to generate them using some combination of (i) interest earned by the platforms on short-term loans of these crypto-assets; (ii) returns gained by investing customers’ crypto-assets in other crypto-assets, in traditional financial instruments, such as securities, or in other centralized or decentralized yield-generating projects; (iii) staking fees or rewards granted to those staking crypto-assets in order to be used toward validation in Proof-of-Stake consensus mechanisms used on certain blockchain protocols; or (iv) other income generated through holding certain crypto-assets (e.g., initial holders of new coins).

Users may also borrow through centralized platforms, where loans of U.S. dollars or crypto-assets are available without credit checks and collateralized by users’ holdings of crypto-assets.<sup>59</sup> Users are often borrowing to exploit pricing disparities among the various crypto-assets and trading platforms. Lending platforms generally limit the amount that users can borrow to some fraction—e.g., 50%—of the value of their collateral. While there is little transparency into the activity in the form of verifiable reporting on the number of borrowers, the sizes of loans, and the frequency of margin calls and liquidations, lending and borrowing activity appeared to have been growing through the end of 2021. Activity has appeared to decline through the first half of 2022.<sup>60</sup>

Investors and consumers may also engage in lending and staking through decentralized markets and intermediaries. According to one estimate, DeFi protocols developed for lending and other yield farming activities appear to account for a little over one-third of the TVL in all DeFi platforms.<sup>61</sup> Lending participants expect to receive new tokens issued by a DeFi protocol, representing their *pro rata* claim on the protocol’s lending pool, which they are able to redeem later for the assets originally placed plus accrued interest. Lending participants also may earn reward tokens for providing liquidity, which are often governance tokens issued by the protocol that may increase the expected return beyond accrued interest.

58 Because loans generally are disbursed in digital coins or tokens and are secured by other crypto-assets, the self-referential nature of these activities may present wrong-way risks, meaning that a party’s credit risk is correlated with the value of the underlying asset. See, e.g., SIRIO ARAMONTE, SEBASTIAN DOERR, WENQIAN HUANG & ANDREAS SCHRIMPF, DEFI LENDING: INTERMEDIATION WITHOUT INFORMATION? 1-2 (BIS, BIS Bulletin No. 57, 2022), <https://www.bis.org/publ/bisbull57.pdf>.

59 Though credit assessments typically are not required for borrower loan approvals, more and more centralized crypto-asset lending platforms are carrying out certain “know your customer” or KYC diligence on customers to comply with anti-money laundering and other illicit financial activities laws.

60 This may be due, at least in part, to the fact that several prominent platforms were faced with enforcement actions from state or federal regulators, while others experienced liquidity strains due to a broad decline in crypto-asset prices, leading more than one platform to place limits on or altogether suspend customer withdrawals. See, e.g., SEC, *BlockFi Agrees to Pay \$100 Million in Penalties and Pursue Registration of its Crypto Lending Product*, (Feb. 14, 2022), <https://www.sec.gov/news/press-release/2022-26>; MacKenzie Sigalos, *From \$25 billion to \$167 million: How a major crypto lender collapsed and dragged many investors down with it*, CNBC (Jul. 18, 2022), <https://www.cnbc.com/2022/07/17/how-the-fall-of-celsius-dragged-down-crypto-investors.html>.

61 DeFi DEXs currently account for just over a quarter of all TVL in DeFi, while all other protocol categories combined make up the rest. See DEFI LLAMA, *Protocol Categories*, <https://defillama.com/categories>.

Participants may also borrow crypto-assets from DeFi lending protocols. Like centralized lending platforms, DeFi lending protocols generally permit users to borrow only a fraction of their crypto-asset collateral (i.e., the loans are “over-collateralized,” in some cases up to 150% of the loan), users who can provide the required collateral can participate in transactions on the platform, and there is no credit assessment on borrowers. Borrowers are typically subject to a collateralization ratio (sometimes called a “health factor”<sup>62</sup>) which, if breached, will lead to their loan being liquidated and a portion of their collateral being seized, inclusive of a liquidation fee. These liquidation fees are often not disclosed to the user in loan documentation, but may instead be incorporated by reference to the protocol’s documentation or frequently asked questions.<sup>63</sup>

Investors in crypto-assets can also earn returns on their holdings through staking,<sup>64</sup> which is the process of “locking up”—or committing—crypto-assets to support the operation of the underlying blockchain in exchange for rewards. Like crypto-assets generally, staking reward estimates are volatile and can change unpredictably over time, but as of August 2022, one data aggregator estimated that the top 206 staked assets generated an average annual return of 8.82%.<sup>65</sup>

### Raising Capital (e.g., ICOs)

Startup companies, developers, and other participants in the crypto-asset ecosystem have raised funds from investors and other users to create blockchain projects, establish DAOs or DeFi protocols, or simply to create a new coin or token. Such funds have been raised through so-called “initial coin offerings,” or ICOs, which have been compared to crowdfunding and initial public offerings (IPOs) in traditional regulated securities markets.<sup>66</sup>

A typical ICO starts with the developer or project owner issuing a white paper that provides some information on the goals of the project and other details.<sup>67</sup> Tokens offered through the project are often labeled as “utility tokens,” which purport to provide investors a means to later obtain access to certain products or services in exchange for the tokens. Alternatively, tokens may purport to represent an ownership stake in the project or a proportional right to earn certain rewards. Tokens are often then sold in secondary markets to other investors, either through centralized or decentralized crypto-asset platforms or other intermediaries.

62 See AAVE, *Risk Parameters*, <https://docs.aave.com/risk/asset-risk/risk-parameters#health-factor>.

63 See, e.g., Alexis Goldstein, Director of Financial Policy, Open Markets Institute, Written Testimony before the United States Congress Joint Economic Committee (Nov. 17, 2021), at 20, [https://www.jec.senate.gov/public/\\_cache/files/aa387917-9456-4b1f-a948-f086594c4d15/alexis-goldstein-jec-crypto-hearing-testimony.pdf](https://www.jec.senate.gov/public/_cache/files/aa387917-9456-4b1f-a948-f086594c4d15/alexis-goldstein-jec-crypto-hearing-testimony.pdf).

64 Staking returns are only applicable in crypto-assets native to blockchains that use the proof-of-stake (PoS) consensus mechanism. In PoS blockchains, validators are selected to verify new blocks of data to be added to the network based on the quantity of native coins they have staked. Some investors pool assets to meet staking requirements, which increases the validator’s chances of being selected to verify blocks and generates rewards—usually in the form of fees paid in new native blockchain coins—that typically are distributed to pool contributors on a pro-rata basis. “Staking” is also sometimes loosely referred to by certain DeFi protocols as a synonym for simply locking assets into a smart contract on the protocol.

65 STAKING REWARDS, *Top 10 Crypto Assets by Staking Marketcap*, <https://www.stakingrewards.com>. As with other data sources regarding crypto assets noted above, such figures may not be entirely reliable, as evidenced by this site’s disclaimer regarding the accuracy of information. See STAKING REWARDS, *Disclaimer*, <https://www.stakingrewards.com/disclaimer>.

66 Whether or not a particular ICO entails an offering of securities will depend on consideration and evaluation of the facts and circumstances. See SEC, *supra* note 31, at 10, 17; *SEC v. Kik Interactive Inc.*, 19 Civ. 5244 (S.D.N.Y. 2020); *SEC v. Telegram Group Inc.*, 448 F. Supp. 3d, 352 (S.D.N.Y. 2020) (granting preliminary injunction under the securities laws).

67 Initial crypto-asset offerings may bear different labels more specific to the type of entity or purpose of the capital raise or may be structured and executed slightly differently, but the general concept is the same.

## Opportunities in Native Crypto-asset Financial Markets, Products, and Services

The capability offered by blockchain technology to transact in “trustless” environments with reduced number of intermediaries creates a number of potential opportunities, many of which are yet to be realized. Proponents have long claimed that new financial products and services could be created to operate in an automated and distributed environment with potentially lower operating costs and enabled by faster crypto-asset payment settlement activity. There could also be more widely available financial products and services with direct-to-consumer and consumer-to-consumer features of crypto-asset technologies and business models. For example, specialized assets with novel features appealing to discrete types of purchasers may emerge.<sup>68</sup> This may offer some an alternative to traditional markets where the creation of financial and non-financial products is subject to different degrees of intermediation that create variations in the benefits that entrepreneurs, businesses, investors, and consumers realize from capital investments.<sup>69</sup>

The degree to which consumers, investors, and businesses may or may not benefit from current practices for the creation and trading of crypto-assets depends upon a range of factors. Many of these factors are similar to those that are present in traditional financial markets, albeit with unique applications in the crypto-asset context. For example, search costs in crypto-asset markets are high because of the increasing variation in and lack of definitive information about crypto-assets, which may make them more difficult to value, combined with the sheer number of crypto-assets and markets, which means investors must devote more resources to identify attractive investments and avoid resource misallocations as well as scams.<sup>70</sup> Crypto-asset markets may also lack liquidity and be prone to bubbles<sup>71</sup> as a result of 24/7 trading and faster settlement, similar to the dynamics present in traditional financial markets.<sup>72</sup> Finally, credit risk associated with the underlying leveraged trading in crypto-asset markets may not be controlled fully by collateralization and automated liquidation practices used with many crypto-asset loans.<sup>73</sup> Further, in order for these markets to reach their full potential, they must be operated in compliance with applicable laws and regulations.

### *Financial Market and Payment System Infrastructures*

To date, the primary use cases, and accompanying future opportunities, of crypto-assets for financial markets and payments depend upon their potential for faster and less expensive payment and transaction settlement.

---

68 See JOSEPH ABADI & MARCUS BRUNNERMEIER, BLOCKCHAIN ECONOMICS (NBER, Working Paper 25407, 2018), [https://www.nber.org/system/files/working\\_papers/w25407/w25407.pdf](https://www.nber.org/system/files/working_papers/w25407/w25407.pdf); Hugo Benedetti & Ehsan Nikbakht, *Returns and Network Growth of Digital Tokens After Cross Listings*, JOURNAL OF CORPORATE FINANCE (Vol. 66 Issue 101853, Feb. 2021), <https://www.sciencedirect.com/science/article/pii/S0929119920302972?via%3Dihub>; and PAUL P. MOMTAZ, IS DECENTRALIZED FINANCE (DEFI) EFFICIENT? (THE ANDERSON SCHOOL AT UCLA, 2022), [https://www.researchgate.net/publication/360226953\\_IS\\_DECENTRALIZED\\_FINANCE\\_DEFI\\_EFFICIENT](https://www.researchgate.net/publication/360226953_IS_DECENTRALIZED_FINANCE_DEFI_EFFICIENT).

69 See PAUL P. MOMTAZ, *supra* note 68.

70 *Id.*, at 8-10.

71 F.A. Enoksen, Ch.J. Landsnes, K. Lučivjanská, and P. Molnár, *Understanding Risk of Bubbles in Cryptocurrencies*, JOURNAL OF ECONOMIC BEHAVIOR AND ORGANIZATION (Vol. 176, Aug. 2020), at 129-144, <https://www.sciencedirect.com/science/article/pii/S0167268120301505?via%3Dihub>.

72 Wei Xiong & Jialin Yu, *The Chinese Warrants Bubble*, AMERICAN ECONOMIC REVIEW (Vol. 101 No. 6, Oct. 2011), at 2723-2753, <https://www.aeaweb.org/articles?id=10.1257/aer.101.6.2723>; OLIVIER J. BLANCHARD & MARK W. WATSON, BUBBLES, RATIONAL EXPECTATIONS AND FINANCIAL MARKETS (NBER, Working Paper 0945, 1982), <https://www.nber.org/papers/w0945>; and J. Michael Harrison & David M. Kreps, *Speculative Investor Behavior in a Stock Market with Heterogeneous Expectations*, QUARTERLY JOURNAL OF ECONOMICS (Vol. 92 No 2, 1978), at 323-336, <https://www.jstor.org/stable/1884166?seq=1>.

73 SIRIO ARAMONTE, SEBASTIAN DOERR, WENQIAN HUANG & ANDREAS SCHRIMPF, *supra* note 58, at 2. See also Eli Tan, *Many Bored Ape NFTs Are in Danger of Getting Liquidated as Borrowed Money Comes Back to Bite*, COINDESK (Aug. 19, 2022), <https://www.coindesk.com/business/2022/08/19/many-bored-ape-nfts-are-in-danger-of-getting-liquidated-as-borrowed-money-comes-back-to-bite>.

## Payments

Increased competition associated with the development and introduction of crypto-asset-based faster payment systems may prompt the existing fiat-based payment systems to respond with more competitive, innovative, and inclusive offerings. The degree to which these benefits will be realized depends on the extent and permanence of the adoption of faster crypto-asset-based payment systems.<sup>74</sup>

While crypto-assets have not become widely adopted as a medium of exchange in the real economy, which limits their viability as a payment mechanism, some versions of peer-to-peer faster payments functionality exist within the crypto-asset ecosystem, and payment services are available to businesses and consumers directly through crypto-asset platforms and some payment platforms.<sup>75</sup> Though such services are generally not yet significantly scaled or interoperable, they do represent working examples of practical uses of crypto-asset payment systems for individual businesses, investors, and consumers. For example:<sup>76</sup>

- Crypto-asset service providers and blockchain technologies could improve efficiency in international payments and remittances for businesses and individual customers.<sup>77</sup> These and similar alternatives could help address the lack of interoperability across the payment infrastructures of different countries and the absence of a single global banking network or service that enables faster international funds settlement. These changes could provide an alternative to the current system of time consuming and expensive correspondent banking processes to complete international payments and remittances.<sup>78</sup>
- Applications of crypto-assets and DLT technologies could improve trade credit provision and other administrative processes related to trade in physical goods. Common problems in the sector include the lack of visibility in physical supply chain processes, inefficient manual paperwork requirements, regulatory and compliance costs, fraud risks, and high transaction costs. DLT applications in trade finance could create a single source of reference information to help participants synchronize the movement of physical goods, information, and financing, at times paired with smart contract and foreign exchange functions that may eliminate the need for correspondent banks and additional transaction fees.<sup>79</sup>

---

74 See the report required by Section 4(b) of the Executive Order for additional discussion of payments.

75 It is important to note that, since sending crypto-assets from one wallet to another typically requires an on-chain transaction, there is a non-deterministic fee that these platforms will pass on to users, to pay the miner or the validator a gas fee; these fees can be high in times of peak congestion.

76 Note that these projects are referenced here only as examples, and this report does not endorse or recommend the use of any specific asset, product, platform, or intermediary. The mention of, or absence of reference to, any particular project or application also does not reflect a view on viability, operational soundness, or legal status of such project or application.

77 See INTER-AMERICAN DEVELOPMENT BANK, CROSS BORDER PAYMENTS WITH BLOCKCHAIN 38 (2020), <https://publications.iadb.org/publications/english/document/Cross-Border-Payments-with-Blockchain.pdf>. See also FRIEDERIKE RÜHMANN, SAI AASHIRVAD KONDA, PAUL HORROCKS & NINA TAKA, CAN BLOCKCHAIN TECHNOLOGIES REDUCE THE COST OF REMITTANCES? 4 (ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD), 2020), <https://www.oecd-ilibrary.org/docserver/d4d6ac8f-en.pdf?expires=1661626664&id=id&accname=guest&checksum=0B50ED298A2B06C0625EB90BF9EBB569>.

78 JASON EKBERG, MICHAEL HO, TEK YEW CHIA, LAURA LIU, NAVEEN MALLELA, HARSHIKA PATEL & SUKRIT KHATRI, UNLOCKING \$120 BILLION VALUE IN CROSS-BORDER PAYMENTS 5 (OLIVER WYMAN, 2021), <https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2021/nov/unlocking-120-billion-value-in-cross-border-payments.pdf>.

79 Ilias Ioannou & Guven Demirel, *Blockchain and supply chain finance: a critical literature review at the intersection of operations, finance and law*, JOURNAL OF BANKING AND FINANCIAL TECHNOLOGY (Vol. 6, May 9, 2022), at 83–107, <https://doi.org/10.1007/s42786-022-00040-1>.

- Crypto-asset platforms, protocols, and applications have also introduced services that may allow users to create payment streams for employees, contractors, suppliers, and other beneficiaries. Such systems may provide faster access to funds and act as a close substitute for cash. These services could be particularly useful for gig workers, lower income populations, and those who are unbanked or underbanked.
- Finally, stablecoins purport to provide features that make them both more stable than non-asset-backed crypto-assets as a means of payment or settlement for crypto-asset-based transactions, and potentially, more broadly useful.

### Clearing and Settlement Uses and Related Opportunities

Crypto-asset technologies aspire to make real-time settlement standard practice, potentially reducing risks and expenses of trading compared to secondary markets for most traditional non-derivative financial products.<sup>80</sup> Current plans to shorten the settlement cycle for U.S. securities markets do not set a goal of real-time settlement, so in the absence of broader adoption of real-time settlement, crypto-asset technologies may present an opportunity.<sup>81</sup>

Tokenization, the process of digitally representing an existing real asset (e.g., securities, real estate, commodities, art) on a distributed ledger,<sup>82</sup> involves a public or private ledger that links the economic value and rights derived from these real assets with digital tokens. The act of tokenizing any asset, including intangible assets (e.g., intellectual property), introduces the technological benefits of DLT to the related clearing and settlement processes by processing transaction details and automating all other transaction related events through settlement.<sup>83</sup> Such application may create innovative methods for settling and clearing transactions, an area of finance with potential for growth—with several financial institutions exploring methods to improve the clearing or settlement of traditional securities transactions using blockchain technology.<sup>84</sup> These applications generally are using a private permissioned blockchain environment rather than a public, permissionless environment that helps improve the integrity of the system.<sup>85</sup> The scope of future tokenized crypto-asset activities on permissioned blockchains is potentially very large, with proxies for the estimated market capitalization of financial products in this segment including the value of securities held in custody by the Depository

80 BIS, STRENGTHENING REPO CLEARING AND SETTLEMENT ARRANGEMENTS 19 (2010), <https://www.bis.org/cpmi/publ/d91.pdf>. See also George Jia, *Implications of Diverging Settlement Standards*, DTCC (Aug. 6, 2020), <https://www.dtcc.com/dtcc-connection/articles/2020/august/06/implications-of-diverging-settlement-standards>.

81 Shortening the Securities Transaction Settlement Cycle, 87 Fed. Reg. 10436 (Feb. 24, 2022).

82 The Financial Stability Board (FSB) defines tokenization as “the representation of traditional assets – e.g., financial instruments, a basket of collateral or real assets – on DLT.” See FSB, DECENTRALISED FINANCIAL TECHNOLOGIES: REPORT ON FINANCIAL STABILITY, REGULATORY AND GOVERNANCE IMPLICATIONS 13 (2019), <https://www.fsb.org/2019/06/decentralised-financial-technologies-report-on-financial-stability-regulatory-and-governance-implications>.

83 Ben St. Clair, *Repo by the minute’ could reshape lending – but not quite yet*, RISK.NET (Aug. 4, 2022), <https://www.risk.net/derivatives/7952356/repo-by-the-minute-could-reshape-lending-but-not-quite-yet>.

84 See, e.g., Matthew Leising, *Goldman Begins Trading on JPMorgan’s Repo Blockchain Network*, BLOOMBERG (Jun. 22, 2021), <https://www.bloomberg.com/news/articles/2021-06-22/goldman-sachs-begins-trading-on-jpmorgan-repo-blockchain-network#xj4y7vzkg>. The article reports on new technology related activities of JP Morgan, Bank of New York Mellon Corp., Goldman Sachs Group Inc., Paxos Trust Co., and Arca.

85 IOTA KAOUSAR NASSR, THE TOKENISATION OF ASSETS AND POTENTIAL IMPLICATIONS FOR FINANCIAL MARKETS (OECD, 2020), <https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm>.

Trust and Clearing Corporation (over \$70 trillion),<sup>86</sup> and assets under management across asset classes in private markets (\$9.8 trillion).<sup>87</sup>

The integration of blockchain technologies and crypto-assets into clearing and settlement of traditional securities processes may allow for faster and cheaper transactions, increased transparency of asset positions, and increased liquidity through fractionalization.<sup>88</sup> Technology investments made by many incumbent firms in banking, insurance, asset management, and other sectors may also help to enable a transition towards increasing digitization of assets. Examples of pilot projects using blockchain technology and crypto-assets in financial market infrastructure services include:<sup>89</sup>

- A platform for clearing members that digitalizes pre-IPO equity securities, throughout issuance, distribution, and secondary transfer, and is designed to expand into other markets such as funds, debt, real estate, and loans. The platform is designed to be blockchain agnostic but will initially support issuance of securities on the public Ethereum network.
- A private permissioned distributed ledger system that records changes in ownership of securities and cash resulting from the settlement of securities transactions between participants using a digitized security entitlement—a digital representation of the security. The system is designed to conduct real-time delivery-versus-payment settlement of securities and cash for trades.
- A blockchain-based commodities settlement platform that settles transactions across gold, silver, platinum, and palladium that allows customers to pre-fund settlements and net multilaterally, creating a single platform where settlement occurs for both metals and cash positions.

### *Other Commercial Activities*

The activities, predominantly trading and other forms of speculation, discussed above currently comprise most of the transactions involving crypto-assets or occurring in the crypto-asset ecosystem. Nevertheless, consumers and other users of crypto-assets are engaging in a few different types of activities that have ostensibly non-financial aims, including social clubs and data storage built around crypto-assets and decentralized protocols. A recent report by the U.S. Government Accountability Office (GAO) found that blockchain has a wide range of potential non-financial uses, including applications to organize supply chains, create less hierarchical organizations, and document title registries for real estate.<sup>90</sup>

---

86 DTCC, *DTCC to Launch Platform to Digitalize and Modernize Private Markets*, (Nov. 9, 2021), <https://www.dtcc.com/news/2021/november/09/dtcc-to-launch-platform-to-digitalize-and-modernize-private-markets>.

87 MCKINSEY & COMPANY, *PRIVATE MARKETS RALLY TO NEW HEIGHTS: MCKINSEY GLOBAL PRIVATE MARKETS REVIEW 2022 2* (2022), <https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/mckinseys-private-markets-annual-review>.

88 IOTA KAOUSAR NASSR, *supra* note 85, at 7.

89 Note that these projects are referenced here only as examples, and this report does not endorse or recommend the use of any specific asset, product, platform, or intermediary. The mention of, or absence of reference to, any particular project or application also does not reflect a view on viability, operational soundness, or legal status of such project or application.

90 U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *BLOCKCHAIN: EMERGING TECHNOLOGY OFFERS BENEFITS FOR SOME APPLICATIONS BUT FACES CHALLENGES 1* (2022), <https://www.gao.gov/assets/gao-22-104625.pdf>.

Most such efforts are still in the pilot stage, and some prominent non-financial use cases have encountered challenges or made significant misrepresentations.<sup>91</sup> For example, the GAO found that most blockchain networks are not designed to be interoperable and cannot communicate with other blockchains.<sup>92</sup> Organizations that want to use blockchain also face legal and regulatory uncertainties and have found it difficult to find skilled workers to implement their blockchain projects.

### Non-Fungible Tokens

Whereas some activities involving crypto-assets rely on fungible coins and tokens that are interchangeable with one another, a class of crypto-assets (NFTs) has developed that allows the tokenization of distinct characteristics such that each token is unique and distinguishable from any other. NFTs have a range of potential uses, including establishing a record of purchase and potentially ownership and authenticity of a digital work or asset through a unique cryptographic code that cannot be replicated. The primary uses of NFTs currently may be non-financial in nature, such as digital art and other digital collectibles, akin to collecting trading cards or other collections, including “virtual real estate.”<sup>93</sup> In practice, however, they can be highly speculative investments—many of which have been marketed as such by the issuers of NFTs and their agents. Among consumers and investors, NFTs have become one of the most used segments of the crypto-asset ecosystem. However, the legal rights conveyed by NFTs are often unclear, raising issues that courts may have to resolve.<sup>94</sup>

NFTs may enable new methods for artists or others to sell their works in digital form, but may also introduce new risks for artists.<sup>95</sup> An NFT can be designed to include an in-built royalty system such that the content creator (or others) can earn a profit each time the NFT is resold.<sup>96</sup> Participants in the NFT space include content creators,<sup>97</sup> consumers, investors or users, and miners/validators. They also include platforms that facilitate the creation, distribution, offer and sale of NFTs.

NFT projects often center around “collections,” which consist of multiple digital works—e.g., up to 10,000 NFTs in so-called “10K projects”—created around a single theme but each with slight variation, often created algorithmically. Consumers, investors, or other users seek to own NFTs and engage in primary and secondary transactions. They include collectors and fans, who may be buying for reasons other than material value or an expected return, but also include speculators and so-called flippers hoping to make quick gains. The vast majority of NFT transactions are at the retail level, defined as

---

91 See, e.g., Matt Binder, *Web3 darling Helium has bragged about Lime being a client for years. Lime says it isn't true.*, MASHABLE (Jul. 29, 2022), <https://mashable.com/article/helium-lime-web3-crypto>.

92 For more background on blockchain interoperability, see RAFAEL BELCHIOR, ANDRE VASCONCELOS, SERGIO GUERRERO & MIGUEL CORREIA, A SURVEY ON BLOCKCHAIN INTEROPERABILITY: PAST, PRESENT, AND FUTURE TRENDS (ARXIV, 2021), <https://arxiv.org/abs/2005.14282>.

93 In a famous example, in March 2021, an NFT representing a digital work by an artist sold through an auction for over \$69 million. See Scott Reyburn, *JPG File Sells for \$69 Million, as 'NFT Mania' Gathers Pace*, THE NEW YORK TIMES (Mar. 25, 2021), <https://www.nytimes.com/2021/03/11/arts/design/nft-auction-christies-beeple.html>.

94 See Julie M. Moringiello & Christopher K. Odinet, *supra* note 9, at 7.

95 See, e.g., Kevin Collier, *NFT art sales are booming. Just without some artists' permission.*, NBC NEWS (Jan. 10, 2022), <https://www.nbcnews.com/tech/security/nft-art-sales-are-booming-just-artists-permission-rcna10798>.

96 Rosanna McLaughlin, *'I went from having to borrow money to making \$4m in a day': how NFTs are shaking up the art world*, THE GUARDIAN (Nov. 6, 2021), [www.theguardian.com/artanddesign/2021/nov/06/how-nfts-non-fungible-tokens-are-shaking-up-the-art-world](http://www.theguardian.com/artanddesign/2021/nov/06/how-nfts-non-fungible-tokens-are-shaking-up-the-art-world).

97 Content creators include individual artists, celebrities, NFT project teams (groups that plan and initiate NFT projects), and others.

trades worth less than \$10,000, making the NFT space more retail-driven than overall crypto-asset markets.<sup>98</sup>

NFTs are commonly transacted on centralized marketplaces, specialized websites where users can buy, sell, and trade NFTs similar to how users might trade other coins and tokens. Approximately \$40 billion worth of crypto-assets are estimated to have been sent to major NFT marketplaces in 2021, and more than \$37 billion as of May 1, 2022;<sup>99</sup> however, more recent industry figures suggest that NFT transaction volumes are declining.<sup>100</sup> While some NFT marketplaces may provide custody services for users' NFTs, many marketplaces do not and—as with other crypto-assets—users may need their own blockchain-secured wallets to store and access their NFTs.

NFTs are created, or minted, according to “non-fungible” token standards such that ownership can be demonstrated and verified through entries in a blockchain ledger.<sup>101</sup> Minting refers to the process whereby an NFT is created and transferred to its initial owner and requires a transaction with the smart contract of the NFT project or marketplace hosted on the blockchain. Minting NFTs can be a competitive process, with buyers frequently competing on the basis of the gas fees they are willing to pay to record a transaction on a blockchain. As with other crypto-assets, miners or validators are needed to execute the computational and validation work necessary to record NFTs to the blockchain. Because miners and validators determine the order in which they will validate pending transactions and are incentivized to prioritize transactions based on the fees they can earn, they can benefit from “gas wars” between buyers in fast-moving markets.<sup>102</sup>

## Gaming and Entertainment

The growing role of NFTs in video games and other online entertainment systems is another use case. While traditional video games have long enabled users to make in-game purchases of content and premium features, for example, to enhance their game playing experience, such transactions have generally been one-way flows of payments from players to game developers. But the integration of NFTs

---

98 Chainalysis groups NFT transaction into three categories: (i) Retail—transactions for less than \$10,000 in cryptocurrency; (ii) NFT Collectors—transactions between \$10,000 and \$100,000; and (iii) Institutional—transactions for more than \$100,000. By this classification, as of October 31, 2021, about 80% of NFT transactions—by transaction count—were at the retail level, 19% were at the NFT collector level, and less than 1% were institutional. However, in terms of transaction volume, retail NFT transactions are quite small, accounting for just 11% of trading volume during the period studied, while NFT collector-sized and institutional-sized transactions accounted for 63% and 26%, respectively, of NFT transaction volume. See CHAINALYSIS, *THE 2021 NFT MARKET REPORT 5-6* (2021), <https://go.chainalysis.com/nft-market-report.html>.

99 CHAINALYSIS, *NFT Transaction Activity Stabilizing in 2022 After Explosive Growth in 2021*, (May 5, 2022), <https://blog.chainalysis.com/reports/chainalysis-web3-report-preview-nfts>.

100 See Raphael Minter, *NFT Global Sales Hit 2022 Low, Sinking More Than \$4 Billion*, BE[IN]CRYPTO (Aug. 4, 2022), <https://beincrypto.com/nft-global-sales-hit-2022-low-sinking-more-than-4-billion>.

101 On the Ethereum blockchain, for example, whereas most “fungible” tokens are created according to the ERC-20 token standard, NFTs are created according to the “non-fungible” ERC-721 token standard.

102 In periods of volatility, a buyer may not only lose the opportunity to mint the NFT at the offered price altogether, but they may also incur losses in spent fees attempting to do so. That is, miners still collect transaction fees for failed mints, and these amounts can be quite substantial, and in some cases may exceed what goes to the content creators. Many blockchain transactions, including the minting of NFTs, involve multiple execution steps, and the gas price is applied to each separate step. Buyers attempting to mint NFTs will indicate what they are willing to pay per execution step, as well as set a capped aggregate amount. Miners will choose transactions with higher gas prices, but if the number of execution steps—which is often not known before initiating the transaction—is sufficient to exhaust the user's fee-spending cap, the user will “run out of gas,” resulting in a failed mint. The miner, however, retains the gas collected for execution steps performed up to that point. These costs may not always be transparent to those attempting to mint an NFT, especially new users.

into popular games, as well as the development of blockchain-native games, means that players can purchase tokenized game features and attributes which they own and are able to transfer.<sup>103</sup> In addition, online or blockchain-enabled “metaverses”—digital worlds where participants can interact virtually with other users and purchase tokenized digital real estate and other “merchandise”—have grown in popularity as form of entertainment. With an estimated 215 million, or 66% of, Americans playing video games at least once per week, the potential market for such so-called “play-to-earn” games is substantial.<sup>104</sup>

### Potential Opportunities in NFTs

NFTs have a number of potential future applications, including: (i) enabling the recording and verification of transfers of real estate ownership; (ii) facilitating automatic royalty payments for music and film; (iii) preventing duplication and counterfeits in the titling of other property and consumer goods; (iv) enabling more digital credentials, including identification, licensing, certification; and (v) facilitating financial industry legal compliance.

NFTs have the potential to function across both digital spaces and the physical world. As a result, NFTs can include features that serve as membership cards or tickets, providing access to events, exclusive merchandise, and special discounts.<sup>105</sup> However, many of the potential NFT use cases are still materializing, in part due to evolving technological and legal landscape, including with respect to licensing, contracts, copyright and intellectual property, anti-money laundering, and data protection.<sup>106</sup>

## **IV. RISKS AND EXPOSURES FOR CONSUMERS, INVESTORS, AND BUSINESSES**

Having considered the potential opportunities presented by crypto-asset products and services, this part of the report reviews the risks posed by crypto-assets. These risks are divided into three categories: (i) conduct risks, including product, and investor, consumer, and business protection (e.g., theft, fraud) risks; (ii) operational risks, including the technology-specific risks of crypto-assets and systems; and (iii) risks arising from crypto-asset intermediation. Some of the risks discussed in this part are unique to the crypto-asset ecosystem, as a result of the features of crypto-assets. Others are simply a form of risk already present in traditional finance markets, but which is heightened due to the specific attributes of the crypto-asset ecosystem.

103 Though tokenized game features and attributes are, on the surface, intended to enhance players’ experiences within the gaming environment, to the extent these NFTs have tradable value there is a possibility that some players will become incentivized to use them predominantly as speculative assets, purchasing in-game NFTs primarily with the aim of selling them for a future profit. Indeed, players both in the U.S. and abroad have taken to playing certain games as a way to earn a living, and some games have deployed design features and incentives in order to create an “investor mindset” among new players. In addition, the increased prevalence of “gamification” of investment activities more generally has come under greater scrutiny in recent years. See James Fallows Tierney, *Investment Games*, DUKE LAW JOURNAL (Vol. 72, Forthcoming 2022-23), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3916407](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916407).

104 ENTERTAINMENT SOFTWARE ASSOCIATION, ESSENTIAL FACTS ABOUT THE VIDEO GAME INDUSTRY (2022), <https://www.theesa.com/resource/2022-essential-facts-about-the-video-game-industry>.

105 Steve Kaczynski & Scott Duke Kominers, *How NFTs Create Value*, Harvard Business Review (Nov. 10, 2021), <https://hbr.org/2021/11/how-nfts-create-value>.

106 For example, since NFTs essentially represent the original and unique cryptographic code or on-chain token linked to the off-chain digital work or real-world asset, ownership of an NFT may not translate to ownership of an underlying asset or the associated rights (such as copyright and licensing rights). See, e.g., Stuart Levi, Mana Ghaemmaghami & Gabriel Mohr, *Skadden Discusses the Growing Complexity of Commercial Rights Issues In NFTs*, THE CLS BLUE SKY BLOG (Jun. 1, 2022), <https://clsbluesky.law.columbia.edu/2022/06/01/skadden-discusses-the-growing-complexity-of-commercial-rights-issues-in-nfts>. NFTs can also be used to facilitate money laundering and terror financing; digital art assets are inherently easier than traditional art for such purposes. See U.S. DEPARTMENT OF THE TREASURY, STUDY OF THE FACILITATION OF MONEY LAUNDERING AND TERROR FINANCE THROUGH THE TRADE IN THE WORKS OF ART (2022), [https://home.treasury.gov/system/files/136/Treasury\\_Study\\_WoA.pdf](https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf).

This part then considers factors affecting the relative exposure of consumers, investors, and businesses to these risks, including due to market participants' non-compliance with current laws and regulations, and ongoing changes related to the scope and application of those legal requirements.

## Conduct Risks

Consumers, investors, and businesses using or investing in crypto-assets are exposed to a variety of conduct risks in the crypto-asset ecosystem. Investing is often at the core of crypto-asset activity; accordingly, the conduct risks below largely focus on risks associated with investing activities.

Crypto-assets and markets that operate out of compliance with applicable laws and regulations, or are unregulated, can breed fraud, abusive market practices, and disclosure gaps.<sup>107</sup> Certain practices in the crypto-asset ecosystem have resulted in financial harm to consumers, investors, and businesses; unfair and inequitable outcomes; and damage to the integrity of the market. Some notable conduct risks are described below, but risks are likely to continue to evolve as crypto-asset markets change and therefore require vigilant and robust regulatory supervision and oversight.<sup>108</sup>

### *Fraud, Theft, and Mismanagement*

As the crypto-asset market has grown, so has the volume of fraud, scams, and theft in the ecosystem; indeed, unlawful transaction activity globally reached an all-time high in value in 2021.<sup>109</sup>

Criminals often take advantage of innovations and new technologies to perpetrate fraudulent activities, including promises or guarantees of high returns. Moreover, the crypto-asset ecosystem has unique features that make it an increasingly attractive target for unlawful activity, including the ongoing evolution of the underlying technology, pseudonymity, irreversibility of transactions, and the current asymmetry of information between issuers of crypto-assets and consumers and investors.

Multiple U.S. government agencies track and publish crypto-asset related complaints reported by the public, which have indicated a sharp increase in losses related to crypto-assets. They have also issued warnings related to their findings, including noting a material increase in crypto-assets as a payment method for all types of scams, including investment scams, romance scams, and business and government impersonation scams.<sup>110</sup>

- The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) has warned against the scams leveraging cryptocurrency ATMs,<sup>111</sup> cryptocurrency customer support impersonators, as well as romance scams that involve investment opportunities. In 2021, the IC3 received 34,202

---

107 IOSCO, *supra* note 21, at 36.

108 *Id.*, at 5.

109 At the same time, transaction activity associated with unlawful applications reached an all-time low as a share of all crypto-asset activity, reflecting the growth in overall transaction volume. See CHAINALYSIS, THE 2022 CRYPTO CRIME REPORT 3-4 (2022), <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>.

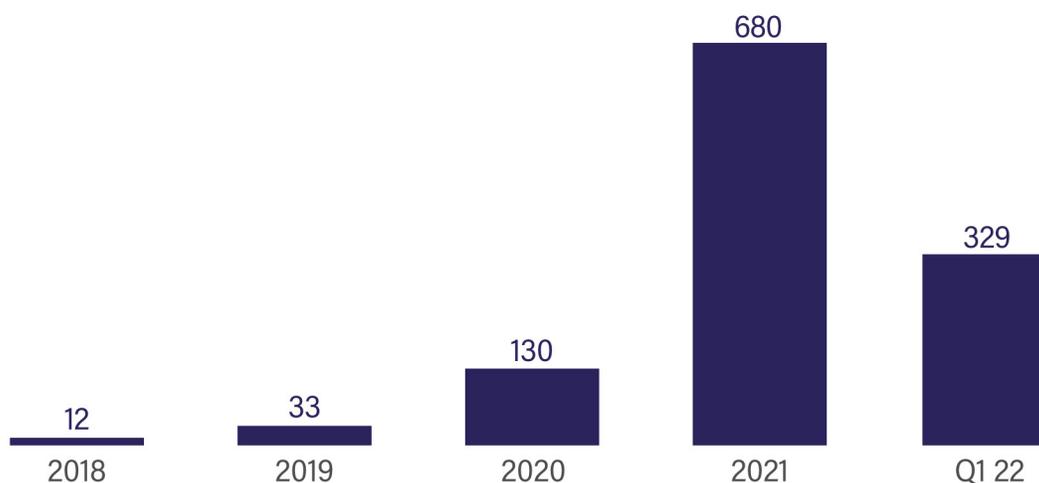
110 For more information on crypto-asset scams, see FTC, *Reports show scammers cashing in on crypto craze*, (Jun. 2022), [www.ftc.gov/system/files/ftc\\_gov/pdf/Crypto%20Spotlight%20FINAL%20June%202022.pdf](http://www.ftc.gov/system/files/ftc_gov/pdf/Crypto%20Spotlight%20FINAL%20June%202022.pdf).

111 Criminal actors, in various fraudulent schemes, maliciously leverage physical cryptocurrency ATMs to receive payments from victims. See, e.g., FBI, *The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment*, (Nov. 4, 2021), <https://www.ic3.gov/Media/Y2021/PSA211104>.

complaints involving the use of some type of crypto-asset. While the number of complaints decreased by approximately 3% in 2021 year-over-year, the loss amount reported in IC3 complaints increased by nearly 600%, from \$246 million in 2020 to more than \$1.6 billion in 2021.<sup>112</sup>

- The Consumer Financial Protection Bureau (CFPB) had 2,404 published crypto-asset consumer complaints in 2021 compared to 983 in 2020, amounting an increase of over 140%. As of July 15, 2022, the CFPB had 906 complaints year-to-date and 1,870 published complaints in the prior 12 months.<sup>113</sup>
- The Federal Trade Commission (FTC) had more than 46,000 reported incidents of fraud between January 1, 2021, and March 31, 2022, with people claiming losses that exceeded \$1 billion worth of cryptocurrencies. Cryptocurrencies represented 24% of all fraud-related losses reported to the FTC during that period—more than any other payment method.<sup>114</sup> The median individual reported loss was \$2,600.<sup>115</sup>

### Reported Cryptocurrency Fraud Losses by Year (USD MM)



Source: FTC, (Jun. 2022)

Measuring or estimating the volume of crime involving crypto-assets, or any criminal activity, can be challenging as it relies on self-reporting by victims and thus is likely to be underreported. However, given the public nature of blockchains, several private firms have been able to use proprietary methodologies to track losses from known thefts, scams, and frauds. According to one private sector estimate, there was \$14 billion worth of crypto-asset-based crime, globally, in 2021, up from \$7.8 billion in 2020; the breakdown is as follows:

- **Scams:** Scams were the largest form of crypto-asset-based crime by transaction volume in 2021. The number of scams in 2021 rose by over 60% year-over-year, while the value of stolen crypto-

112 FBI, 2021 INTERNET CRIME REPORT 13 (2021), [https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

113 CFPB, CFPB Complaint Database, <https://www.consumerfinance.gov/data-research/consumer-complaints/search>.

114 FTC, *supra* note 110.

115 *Id.*

assets rose by over 80% in 2021 to \$7.8 billion. \$2.8 billion of this total came from a relatively new but increasingly common scheme known as a “rug pull,” in which developers build out what appears to be legitimate crypto-asset projects, misleading investors into purchasing tokens associated with a project, before ultimately draining the funds provided by those investors and disappearing, typically driving the token’s value to zero.<sup>116</sup>

- *Thefts*: Of the \$14 billion in crypto-asset-based crime in 2021, theft rose by over 500% year-over-year to \$3.2 billion in total.<sup>117</sup> Thefts include security breaches that target individuals’ private keys, which can be obtained through phishing, key logging, or social engineering, code exploits, and flash loan attacks.<sup>118</sup> 2021 also marked the first year when the level of theft in DeFi surpassed theft on centralized exchanges; out of \$3.2 billion of total stolen funds, \$2.3 billion was stolen from DeFi protocols, as opposed to centralized platforms, which represented a year-over-year increase of over 1,300%.<sup>119</sup>

Analysts believe that most instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds, or promoters exploit flaws in their operating code that can lead to erroneous transactions, similar to the errors that allow rug pulls to occur. Users, who often lack the ability to read the code, must rely on a developer’s word—offered, for example, through a protocol’s white paper—that a smart contract will perform as described. Still, even auditing of the code may be insufficient to prevent theft as nearly 30% of code exploits and over 70% of flash loan attacks occurred on platforms audited within the prior year.<sup>120</sup> Sophisticated hacks, especially hacks perpetrated by nation state actors, have also emerged as an area of concern.<sup>121</sup>

- *Other*: Of the remaining \$3 billion of crypto-asset-based crime in 2021, nearly \$2 billion was associated with drug trafficking. Other activity can be traced to sales of stolen logins or credit cards, ransomware, malware, terrorism financing, and child abuse material.

---

116 CHAINALYSIS, *supra* note 109, at 3, 5, 24, and 81-84. Note that the definition of rug pulls is evolving, particularly as an innovation in scamming. Another form of a rug pull would include limiting sell orders, where tokens are coded only to be bought but unable to be sold. See Valerio Puggioni, *Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it*, COINTELEGRAPH (Feb. 6, 2022), <https://cointelegraph.com/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it>. See also KOINLY, *Rug Pulls: Your Complete Guide*, (Mar. 31, 2022), <https://koinly.io/blog/crypto-rug-pulls-guide>.

117 *Id.*, at 6.

118 In an innovation unique to DeFi lending, some protocols may support “flash loans,” which enable users to borrow, use, and repay crypto-assets in a single transaction that is recorded on the blockchain in the same data block. Because there is no default risk associated with flash loans, users can borrow without posting collateral and without risk of being liquidated. A “flash loan attack” can occur when the temporary surge of funds obtained in a flash loan is used to manipulate prices of crypto-assets, often through the interaction of multiple DeFi services, enabling attackers to take over the governance of a protocol, change the code, and drain the treasury. See, e.g., WORLD ECONOMIC FORUM, *DECENTRALIZED FINANCE (DeFi) POLICY-MAKER TOOLKIT 18* (2021), [https://www3.weforum.org/docs/WEF\\_DeFi\\_Policy\\_Maker\\_Toolkit\\_2021.pdf](https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf). See also Shaurya Malwa, *Solana DeFi Protocol Nirvana Drained of Liquidity After Flash Loan Exploit*, COINDESK (Jul. 28, 2022), <https://www.coindesk.com/tech/2022/07/28/solana-defi-protocol-nirvana-drained-of-liquidity-after-flash-loan-exploit>.

119 CHAINALYSIS, *supra* note 109, at 70.

120 *Id.*, at 73.

121 Hacks linked to nation state actors, responsible for some of the unlawful activity discussed in this section, have advanced to become persistent threats in the crypto-asset industry. One example was in the play-to-earn crypto-asset segment of the ecosystem, where the game Axie Infinity collapsed following a \$620 million hack of its Ronin Network side-chain, which was attributed to hackers affiliated with Democratic People’s Republic of Korea. See CHAINALYSIS, *supra* note 109, at 120. See also Aaron Schaffer, *North Korean hackers linked to \$260 million Axie Infinity crypto heist*, THE WASHINGTON POST (Apr. 14, 2022), <https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea>.

As discussed in more detail in Part VI, Recommendations, U.S. regulatory and law enforcement authorities should aggressively pursue investigations and enforcement actions, and pursue vigilant monitoring of the crypto-asset sector for unlawful activity.

### *Information Asymmetry: Lack of Transparency*

The traditional capital markets have statutes and regulations that create a robust disclosure regime, providing consumers and investors with material information, including with respect to conflicts of interest, so that users can better understand the risks of participation and make more informed decisions regarding their investment risks.<sup>122</sup> In the crypto-asset ecosystem, issuers and platforms may be acting in non-compliance with these statutes and regulations and, thus, do not maintain the same protocols to protect investors. Further, disclosures in the crypto-asset ecosystem that are provided may lack standardization and may not disclose material information integral to assessing risk.

### Crypto-asset Investments and Governance

Absent compliance with comprehensive, mandatory disclosure requirements, including with respect to conflicts of interest, information asymmetries will likely advantage insiders at the expense of the smallest investors and those with the least access to information. Currently, investors may lack material information necessary to assess the risk of crypto-asset investments, including with respect to the probability and severity of the loss on the investment; instead, promoters of crypto-asset investments may at best be providing investors with only broad details or superficial disclosures.<sup>123</sup>

This lack of disclosure and transparency has been prevalent in the ICO market, and instances of outright deception are not uncommon. One review of documents produced for 1,450 digital coin offerings found 271 with red flags that include plagiarized investor documents, promises of guaranteed returns, and missing or fake executive teams.<sup>124</sup> ICOs were growing in popularity when, in 2017, the SEC issued an investigative report concluding that a token issued through such an offering in 2016 was a securities offering requiring either registration or an exemption under federal securities laws.<sup>125</sup> Even before that report, the SEC was cautioning investors—many of whom are retail investors—and market professionals about investing in crypto-assets, including ICOs, warning that such investments may be securities, may be required to be registered with the SEC, and pose substantial risks. Risks in ICOs include not only their high susceptibility to volatility, information asymmetry, and price depreciation, but also a substantial risk of loss through fraud and market manipulation. The SEC has brought a number of civil actions to enforce the federal securities registration requirements and other applicable laws and regulations.<sup>126</sup> More resources may be necessary, however, to address the evolving and growing rate of frauds, manipulations, and other misconduct.

122 Rostin Behnam, Chair, CFTC, Keynote Address of Chairman Rostin Behnam at the Brookings Institution Webcast of The Future of Crypto Regulation (Jul. 25, 2022), <https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam24>. See also Gary Gensler, Chair, SEC, Testimony Before the United States House of Representatives Committee on Financial Services (Oct. 5, 2021), <https://www.sec.gov/news/testimony/gensler-2021-10-05>.

123 Caroline Crenshaw, *supra* note 30, at 5-6.

124 Shane Shifflett & Coulter Jones, *Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud*, THE WALL STREET JOURNAL (May 17, 2018), [www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115](http://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115).

125 See SEC, *supra* note 31.

126 See SEC, *Crypto Assets and Cyber Enforcement Actions*, <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions>.

The NFT market has similar disclosure and integrity gaps, where, for example, consumers can unknowingly buy NFTs that may contain copyright infringements.<sup>127</sup> The industry has seen a significant increase in the number of lawsuits filed, with claims related to deceitful marketing tactics or for sales made under false pretenses.<sup>128</sup> However, investors often suffer from a lack of recourse because there is insufficient information on whom to hold accountable or because accountable parties may be outside the jurisdiction of the U.S. courts.<sup>129</sup>

Crypto-asset investment arrangements also often fail to provide disclosures with respect to conflicts of interest, which is a cornerstone of investor protection in traditional financial markets. Much of DeFi is funded by venture capital and other professional investors. The underlying funding deals often grant professional investors equity, options, advisory roles, access to project team management, formal or informal say on governance and operations, anti-dilution rights, and the ability to distribute controlling interests to allies, among other benefits, which present opportunities for conflicts of interest. These arrangements are rarely disclosed to retail investors, but they can have a significant impact on investment values and outcomes.<sup>130</sup>

For example, one common form of governance, used broadly in DeFi applications, is the issuance of “governance tokens,” which purport to allow disparate participants to introduce and vote on proposals determining the function of a blockchain or overlying protocols. One key risk that, due to inadequate disclosure, may not be apparent to consumers and investors is the concentration of governance tokens or voting rights among a limited number of actors. Developers and early investors in a crypto-asset project may keep control of the platform by allocating significant shares of governance tokens to themselves or otherwise maintaining de facto control.<sup>131</sup> Consumers and investors should understand that the extent to which true decentralization exists in crypto-asset markets is questionable, and claims of decentralization may be exaggerated.<sup>132</sup>

### Crypto-asset Platforms

Compared to registered financial market intermediaries—which are subject to rules and laws that promote market integrity and govern risks and business conduct, including identifying, disclosing, and mitigating conflicts of interest<sup>133</sup> and adhering to AML/CFT requirements—many crypto-asset platforms may either not yet be in compliance with, or may actively claim not to be subject to, existing applicable U.S. laws and regulations, including registration requirements.<sup>134</sup> Consumers, investors,

127 Cristina Criddle, *Hermes Clashes with Artist Who Created MetaBirkins NFT*, FINANCIAL TIMES (Dec. 10, 2021), <https://www.ft.com/content/7953d195-53f6-48d2-8514-460a0ebd9aee>.

128 James Fanelli, *Crypto Industry Sees Surge in Lawsuits as Investor Losses Pile Up*, THE WALL STREET JOURNAL (Jun. 1, 2022), [www.wsj.com/articles/as-crypto-losses-hit-investors-litigation-picks-up-11654084801](http://www.wsj.com/articles/as-crypto-losses-hit-investors-litigation-picks-up-11654084801).

129 Samantha Hissong, *NFT Scams Are Everywhere. Here's How to Avoid Them*, ROLLING STONE (Jan. 24, 2022), <https://www.rollingstone.com/culture/culture-features/nft-crypto-scams-how-to-not-get-scammed-1286614>.

130 Caroline Crenshaw, *supra* note 30, at 9.

131 See, e.g., Danny Nelson & Tracy Wang, *Master of Anons: How a Crypto Developer Faked a DeFi Ecosystem*, COINDESK (Aug. 4, 2022), <https://www.coindesk.com/layer2/2022/08/04/master-of-anons-how-a-crypto-developer-faked-a-defi-ecosystem>. For further discussion of governance in decentralized finance, see Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *supra* note 29, at 27-29. See also IGOR MAKAROV & ANTOINETTE SCHOAR, CRYPTOCURRENCIES AND DECENTRALIZED FINANCE (DeFi) (THE BROOKINGS INSTITUTION, 2022), [https://www.brookings.edu/wp-content/uploads/2022/03/SP22\\_BPEA\\_MakarovSchoar\\_conf-draft.pdf](https://www.brookings.edu/wp-content/uploads/2022/03/SP22_BPEA_MakarovSchoar_conf-draft.pdf).

132 See, e.g., Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *supra* note 29.

133 FINRA, *Conflicts of Interest*, <https://www.finra.org/rules-guidance/key-topics/conflicts-of-interest>.

134 See the report required by Section 7(b) of the Executive Order for additional information on illicit finance risks.

and businesses using centralized and decentralized crypto-asset platforms are subject to a variety of risks and inconsistent practices, including the fact that crypto-assets and crypto-asset intermediaries may be unregistered or otherwise not in compliance with applicable law and that guidance and supervision of crypto-assets is still developing.

#### Access to Platforms and Illegal Activity

Access criteria for registered financial markets helps ensure that access to the systems or exchanges and to associated products is transparent and objective and may support a “gatekeeping” role that assists in preventing criminal or illegal activity. But access criteria can be varied and inconsistent among crypto-asset platforms. When the onboarding process used by platforms is limited or opaque, the risks that the platform may be used for illegal activities increases. Indeed, certain digital platforms have been charged with violating anti-money laundering laws and failing to implement adequate required anti-money laundering programs.<sup>135</sup>

#### Suitability

Registered financial market intermediaries also seek to protect consumers and investors on platforms by limiting participation on the platform to investors that are transacting in assets that match their individual financial situations or risk tolerance levels. Crypto-asset platforms that displace registered intermediaries can also leave retail investors without access to professional financial advisors or other intermediaries who help screen potential investments for quality and legitimacy or who are required by fiduciary standards to act in the best financial interest of their clients.<sup>136</sup> Further, crypto-asset platforms may not be conducting suitability assessments or providing adequate risk disclosures to investors, increasing the likelihood of investor harm.<sup>137</sup>

#### Conflicts of Interest

Crypto-asset platforms often do not disclose activities or aspects of their structure (e.g., common ownership; market making; proprietary trading; and settlement, custody, and advisory services) that may lead to conflicts of interest or that, if the platforms were registered, would be prohibited by statute or regulation. Many trading platforms are themselves heavily invested in crypto-assets and conduct proprietary trading out of compliance with laws to which they are subject or without oversight.

The conflicts of interests in crypto-asset platforms are many and varied. Platforms may be able to hide conflicted relationships through affiliates in other jurisdictions.<sup>138</sup> Some platforms have multiple affiliates, including proprietary trading funds, that are wholly owned or controlled by the platform or its related parties. Some platforms provide large investors with favorable treatment, such as free distributions of coins or tokens, known as “airdrops,” or private cash-outs away from the market.<sup>139</sup>

---

135 See, e.g., CFTC, *Federal Court Orders BitMEX to Pay \$100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations*, (Aug. 10, 2021), <https://www.cftc.gov/PressRoom/PressReleases/8412-21>.

136 Caroline Crenshaw, *supra* note 30, at 9. See also Kat Tretina, *How Fiduciary Duty Impacts Financial Advisors*, FORBES (Jul. 15, 2022), <https://www.forbes.com/advisor/investing/financial-advisor/what-is-fiduciary-duty>.

137 IOSCO, *supra* note 15, at 10.

138 Sam Reynolds, *Crypto Trading Firm TPS Capital Denied Ties to Insolvent Three Arrows. Court Documents Indicate a Connection*, COINDESK (Jul. 19, 2022), <https://www.coindesk.com/business/2022/07/19/crypto-trading-firm-tps-capital-denied-ties-to-insolvent-three-arrows-court-documents-indicate-a-connection>.

139 NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL, *INVESTOR ALERT: Attorney General James Warns New Yorkers About Cryptocurrency Investment Risks*, (Jun. 2, 2022), <https://ag.ny.gov/press-release/2022/investor-alert-attorney-general-james-warns-new-yorkers-about-cryptocurrency>.

Platforms may also engage in steering, with preferential fees for using the specific stablecoins associated with their platforms. Insider trading can also occur in crypto-asset markets, including on some of the largest crypto-asset platforms.<sup>140</sup>

#### Price Discovery and Market Manipulation

U.S. laws and regulations are designed to safeguard market integrity and protect against price manipulation and other abusive trading practices. Market manipulation and misleading or fraudulent and deceptive market conduct is prohibited and distorts the price discovery process, or prices themselves, and unfairly disadvantages investors. Currently, crypto-asset platforms may be out of compliance with applicable laws and regulations designed to protect investors and may maintain varied and inconsistent practices around trade settlement, data reporting, surveillance, and enforcement of price manipulation, creating serious risk for investors.<sup>141</sup>

In the crypto-asset ecosystem, the visibility of transactions on a blockchain is also limited by pseudonymity; without an efficient method for determining the identity of market participants, it is difficult to ascertain if asset prices and trading volumes reflect organic interest or are the product of manipulative trading, including by using bots to operate multiple wallets or a group of people trading collusively.<sup>142</sup> As a result, the values of coins and tokens may be propped up by automated trading or bots that are engaged in wash trading, or platforms may report misleading or inaccurate price information, including transactions based on self-trading.<sup>143</sup>

Bots also may be programmed to spot when another investor is trying to make a purchase and then buy ahead of the trade. Such front-running is a form of value extraction from natural traders and hinders the ability of investors to obtain reliable information before making an investment decision.

As detailed in Part VI, this report recommends a variety of actions to combat market manipulation and information asymmetry and their related risks, including increased investigation and enforcement to bring more crypto-assets and intermediaries into compliance with applicable laws and regulations and their associated disclosure requirements.

#### Problematic Terms of Service

Some users of crypto-assets are subject to problematic terms of service. For example, users staking their crypto-assets face a number of other potential risks, including insufficiently disclosed lock-up periods during which staked assets cannot be withdrawn, waiting periods for honoring withdrawal requests, exposure to the performance and integrity of a staking pool operator, and the risk of the pool

140 See SEC, *SEC Charges Former Coinbase Manager, Two Others in Crypto Asset Insider Trading Action*, (Jul. 21, 2022), <https://www.sec.gov/news/press-release/2022-127>. See also ESTER FÉLEZ-VIÑAS, LUKE JOHNSON & TALIS J. PUTNINS, *INSIDER TRADING IN CRYPTOCURRENCY MARKETS* (2022), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4184367](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4184367). See also Alexis Goldstein, *supra* note 63.

141 Rostin Behnam, *supra* note 122.

142 See Self-Regulatory Organizations; Bats BZX Exchange, Inc.; Order Setting Aside Action by Delegated Authority and Disapproving a Proposed Rule Change, as Modified by Amendments No. 1 and 2, To List and Trade Shares of the Winklevoss Bitcoin Trust, 83 Fed. Reg. 37579 (Aug. 1, 2018). See also SEC, Self-Regulatory Organizations; Cboe BZX Exchange, Inc.; Order Disapproving a Proposed Rule Change, as Modified by Amendment No. 1, To List and Trade Shares of the ARK 21 Shares Bitcoin ETF Under BZX Rule 14.11E(4), Commodity-Based Trust Shares, 87 Fed. Reg. 20014 (Mar. 31, 2022), at 20017.

143 See, e.g., BITWISE ASSET MANAGEMENT, *PRESENTATION TO THE U.S. SECURITIES AND EXCHANGE COMMISSION* (2019), <https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf>. See also CFTC, *CFTC Orders Coinbase Inc. to Pay \$6.5 Million for False, Misleading, or Inaccurate Reporting and Wash Trading*, (Release No. 8369-21, Mar. 19, 2021), <https://www.cftc.gov/PressRoom/PressReleases/8369-21>.

being hacked, which could result in the total loss of funds. Further, some stablecoins do not grant U.S. retail users any redemption rights, leaving them reliant on trading their stablecoins for U.S. dollars on digital asset trading platforms.

DeFi borrowers are at risk of having their collateral liquidated and a loan terminated at any time should the value of their collateral fall below a pre-determined liquidation threshold.<sup>144</sup> Often, liquidation may involve third-party liquidators that are incentivized to repay insufficiently collateralized loans—however briefly—in exchange for acquiring some or all of borrowers’ collateral at a discount.<sup>145</sup> Users of platforms that recently entered bankruptcy have also reported that marketing of certain crypto-asset platforms did not match the reality of the safety of their assets.<sup>146</sup>

Finally, many crypto-asset intermediaries and product contracts employ dispute resolution mechanisms—such as arbitration clauses and class action bans—also utilized by traditional finance companies, that inhibit consumers’ and investors’ ability to pursue legal claims.<sup>147</sup>

## Operational Risks

Operational risk is defined generally as the risk of loss caused by flawed or failed processes, policies, systems, or events.<sup>148</sup> In the context of multilateral systems for settling and recording financial transactions, this includes the risk that deficiencies in information systems or internal processes, human errors, governance and management failures, or disruptions from external events will reduce, deteriorate, or cause a breakdown in services provided. Such deficiencies in information systems or processes also include errors or delays in processing, system outages, information security threats, such as cyberattacks, insufficient capacity, fraud, data loss, and leakage (e.g., calculation errors, omissions, and inaccuracies).<sup>149</sup>

When assets with substantial value reside and trade on permissioned or permissionless blockchains, asset owners are reliant upon the blockchain systems for access to their digital property. Further, crypto-asset systems use different technologies, transaction processes, and distributed governance structures with novel features that may not be as robust as standards for mitigating operational risk in registered markets.<sup>150</sup> These characteristics of crypto-asset technology and products expose users to unique operational risks. Some examples include the absence of reversal mechanisms or other fail-safes for accidental or erroneous transactions, issues associated with the lack of blockchain

144 Liquidation of insufficiently collateralized DeFi loans usually happens automatically in real-time. For this reason, borrowers are incentivized to post more collateral than the minimum required to avoid forced liquidation. See, e.g., SIRIO ARAMONTE, SEBASTIAN DOERR, WENQIAN HUANG & ANDREAS SCHRIMPF, *supra* note 58, at 2-3.

145 WORLD ECONOMIC FORUM, *supra* note 118, at 18.

146 See, e.g., Molly White, *Excerpts from letters to the judge in the Voyager Digital bankruptcy case*, MOLLYWHITE.NET, (Jul. 23, 2022), <https://blog.mollywhite.net/voyager-letters>. See also Molly White, *Excerpts from letters to the judge in the Celsius Network bankruptcy case*, MOLLYWHITE.NET, (Jul. 22, 2022), <https://blog.mollywhite.net/celsius-letters>.

147 See Alexis Goldstein, *supra* note 63, at 3. See also Tamar Meshel & Moin A. Yahya, *Crypto Dispute Resolution: An Empirical Study*, JOURNAL OF LAW, TECHNOLOGY AND POLICY (Oct. 5, 2021), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3975500](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3975500); Julie M. Moringiello & Christopher K. Odinet, *supra* note 9, at 61-63.

148 See, e.g., BIS, INTERNATIONAL CONVERGENCE OF CAPITAL MEASUREMENT AND CAPITAL STANDARDS: A REVISED FRAMEWORK 140 (2005), <https://www.bis.org/publ/bcbs118.html>. See also 12 C.F.R. § 217.101.

149 BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, FEDERAL RESERVE POLICY ON PAYMENT SYSTEM RISK (2021), [https://www.federalreserve.gov/paymentsystems/files/psr\\_policy.pdf](https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf).

150 BIS & OICU-IOSCO, PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES (2012), <https://www.bis.org/cpmi/publ/d101a.pdf>.

interoperability – including those arising from flaws with cross-chain bridges, vulnerabilities associated with private keys, and difficulties integrating blockchains with traditional or legacy systems. Therefore, consumers, investors, and businesses should be aware that increasing use of public blockchains as they currently exist exposes them to these new forms of risk.

### *General Features and Decentralized Governance*

Public permissionless blockchains are ultimately forms of computer software and are subject to software vulnerabilities.<sup>151</sup> Among other things, blockchains may have software bugs and the software may need to be continually updated to address such bugs and add features.<sup>152</sup> Software is also vulnerable to attack by hackers. While certain security features of the largest public blockchains such as Bitcoin and Ethereum are considered strong, as the technology becomes more widely used, the incentives for attacks may increase.<sup>153</sup> Thus, cybersecurity practices and protections will need to keep pace with the scale of adoption.

Public permissionless blockchains also are generally based on open-source software, meaning software that allows for the inspection and modification of source code, is freely distributed, is technologically neutral, and grants free subsidiary licensing rights.<sup>154</sup> While this arrangement increases the number of parties who may contribute to the continued development of the blockchain's source code, it may reduce incentives for timely critical fixes to the software. Solutions to strengthen incentives for improved software development, such as core groups of developers that guide development or compensation for developers that devote more time to the shared project, may also introduce new problems such as conflicts of interest between the users of the network and the core group of developers or sources of funding.<sup>155</sup> In addition, alternative governance structures designed to better align the interests of different constituencies may be subject to other vulnerabilities rooted in their design.<sup>156</sup>

Smart contracts, which are widely used by many permissionless blockchains, also present risks as they combine the features of generally being immutable and publicly viewable. Taken together, these attributes pose several vulnerabilities that may be exploited by illicit actors to steal customer funds: once an attacker finds a bug in a smart contract and exploits it, immutable smart contract protocols limit developers' ability to patch the exploited vulnerability, giving attackers more time to exploit the vulnerability and steal assets.

Concerns with public permissionless blockchains are specific forms of the more general tension between decentralized and centralized features of decision-making associated with public

---

151 Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, NYU JOURNAL OF LEGISLATION AND PUBLIC POLICY (Vol. 18, 2015), at 855, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2579482](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579482).

152 See, e.g., GITHUB, *Bitcoin*, <https://github.com/bitcoin/bitcoin/labels/Bug>.

153 Angela Walch, *supra* note 151, at 863. For a more recent description of blockchain vulnerabilities and attack incentives, see, for example, Huashan Chen, Marcus Pendleton, Laurent Njilla, & Shouhuai Xu, *A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses*, ACM COMPUTING SURVEYS (Vol. 53 Issue 3, 2021), <https://doi.org/10.1145/3391195>.

154 CHRIS DiBONA, SAM OCKMAN, & MARK STONE OPEN SOURCES: VOICES FROM THE REVOLUTION 171-188 (O'Reilly, 1999). See also OPEN SOURCE INITIATIVE, *The Open Source Definition (Annotated)*, <https://opensource.org/osd-annotated>.

155 Angela Walch, *supra* note 151, at 879.

156 Wulf A. Kaal, *Blockchain-Based Corporate Governance*, STANFORD JOURNAL OF BLOCKCHAIN LAW & POLICY (Vol. 4 Issue 1, Aug. 23, 2019), [https://papers.ssrn.com/sol3/Papers.cfm?abstract\\_id=3441904](https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3441904).

blockchains. While a more decentralized system may strengthen public blockchain projects by spreading the benefits of consensus more widely once achieved, the costs of consensus increase with decentralization and reduce the likelihood of it being achieved, creating a significant vulnerability that limits the system's suitability as a core operational feature or channel of a financial system.<sup>157</sup>

### *Security and Scalability Tradeoffs and De-anonymization*

A distributed ledger may be more secure because of its reduced centrality, but as more copies of the ledger are distributed to new nodes, and more computational resources are required to reach protocol consensus, transaction rates on the network slow down. This, in turn, reduces scale (unless a degree of centralization arises to improve validation efficiency), which reduces security.<sup>158</sup> While solutions are emerging that seek to address scalability issues without sacrificing security, the main externality of the computationally heavy process of storing and processing transactions on a blockchain remains.<sup>159</sup>

Issues with scalability of public blockchains manifest in unpredictable, volatile, and regressive fees that are imposed on users. For example, high transaction demand and an increase in the Ethereum gas price in May 2022 led to average daily transaction fees spiking to \$196.68 versus a previous peak of \$69.92 in May 2021.<sup>160</sup> Such high fees not only reduce utility of the public blockchain but also have a regressive impact on users since high fees can make lower value transactions economically unfeasible. Similarly, blockchain congestion can also cause transaction times to vary widely and reduce reliability and utility for users.

One of the attractions of crypto-assets for users is the ability to perform transactions pseudonymously. However, data analysis techniques have been developed that allow pseudonyms (hashes of public keys) to be linked to the IP address where a transaction originates, potentially fatally undermining the privacy of transactions on many public blockchains.<sup>161</sup> Once a user's wallet address is known, every transaction related to that wallet is publicly visible, and attempts to obscure such transactions are often easily unobscured with chain analysis tools. Even if one attempts to regain anonymity through a separate wallet, significant efforts and precautions would need to be taken to maintain that anonymity, including technological acumen that the average consumer may not possess.<sup>162</sup>

### *Peer-to-Peer Verification, Mining Pools, and Validation Incentives*

Peer-to-peer verification protocols mean that, regardless of a blockchain's transaction speed, there are delays in processing transactions that can be on the order of tens of minutes between the execution of

157 Angela Walch, *supra* note 151, at 880.

158 See JOSEPH ABADI & MARKUS K. BRUNNERMEIER, BLOCKCHAIN ECONOMICS (FEDERAL RESERVE BANK PHILADELPHIA, Working Paper No. 22-15, 2022), <https://ssrn.com/abstract=4100197>.

159 NIC CARTER & LINDA JENG, DEFI PROTOCOL RISKS: THE PARADOX OF DEFI (RISKBOOKS, 2021), <https://ssrn.com/abstract=3866699>.

160 BITINFOCHARTS, *Ethereum Avg. Transaction Fee Historical Chart*, <https://bitinfocharts.com/comparison/ethereum-transactionfees.html#3y>.

161 Since all transactions stored on the blockchain are immutable, the entire history of actions done with an address can be traced and observed, although the identity of the person might be unknown. Should an address be linked with a person's identity—for example, by accidental disclosure or through the use of data analytics tools—there would be significant implications for that user's privacy. See ALEX BIRYUKOV, DMITRY KHOVRATOVICH & IVAN PUSTOGAROV, DEANONYMISATION OF CLIENTS IN BITCOIN P2P NETWORK (ARXIV, 2014), <https://arxiv.org/pdf/1405.7418.pdf>. See also FERENC BÉRES, ISTVÁN ANDRÁS SERES, ANDRÁS A. BENCZÜR, & MIKERAH QUINTYNE-COLLINS, BLOCKCHAIN IS WATCHING YOU: PROFILING AND DEANONYMIZING ETHEREUM USERS (ARXIV, 2020), <https://arxiv.org/pdf/2005.14051.pdf>.

162 Molly White, *Abuse and harassment on the blockchain*, MOLLYWHITE.NET (Jan. 22, 2022), <https://blog.mollywhite.net/abuse-and-harassment-on-the-blockchain>.

a transaction and its publication to the network. These network delays in updating ledgers can cause a mismatched ledger to be generated and result in possible losses by fraud, system attacks, double spending, and fake transactions.<sup>163</sup>

Mining has become a specialized industry with a significant concentration of players in mining pools.<sup>164</sup> If a mining pool were to control more than half of the total hash rate, it could lead to a 51% attack on the network.<sup>165</sup> Such attacks may arise from misaligned incentives of miners.<sup>166</sup> Further, decisions relating to the operation of a distributed ledger are made by the “core developers” of the software for that ledger and by validators of transactions on the ledger who determine the definitive record of ownership of crypto-assets on that ledger.<sup>167</sup>

In a PoS environment, the power to validate and assemble transactions into blocks is a function of one’s share of all protocol tokens held, which can create incentives to collude. Such consolidation of power may allow a validator to control which transactions can be included in the final ledger. Because validators are typically rewarded with newly issued tokens, the consolidation of power through vote-buying has been observed in some PoS blockchains.<sup>168</sup> In PoW systems, miners also select, order, and propose transactions to be added to the blockchain record, meaning miners can profit, for example, from selling off earlier processing slots. This may affect the profitability of transactions and trigger or delay transfers of ownership governed by smart contracts.<sup>169</sup>

Further, whether the consensus mechanism is PoS or PoW, miners are able to observe, select, and reorganize transactions during the verification process, and routinely include, exclude, or re-order transactions within the blocks they produce, therefore prioritizing transactions that pay higher fees. This discretionary practice, referred to as “miner extractable value” (MEV), is both opaque and potentially disadvantageous to users in the crypto-asset ecosystem. Indeed, some have observed that activities that generate MEV can resemble front-running or other market manipulation that is harmful to consumers and investors and have called for regulators to establish whether value extraction by miners constitutes illegal activity.<sup>170</sup>

---

163 GARETH W. PETERS, ARIANE CHAPELLE & EFSTATHIOS PANAYI, OPENING DISCUSSION ON BANKING SECTOR RISK EXPOSURES AND VULNERABILITIES FROM VIRTUAL CURRENCIES: AN OPERATIONAL RISK PERSPECTIVE (ARXIV, 2014), <http://arxiv.org/pdf/1409.1451.pdf>.

164 BLOCKCHAIN.COM, *Hashrate Distribution*, <https://www.blockchain.com/charts/pools>.

165 “Hash rate” is a measure of computational power and refers to the number of cryptographic hash functions a processor can calculate in a given time, usually denominated as hashes per second. See, e.g., DYLAN YAGA, PETER MELL, NIK ROBY & KAREN SCARFONE, BLOCKCHAIN TECHNOLOGY OVERVIEW (NIST, 2018), <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>.

166 See MILES CARLSTEN, HARRY KALODNER, MATT WEINBERG & ARVIND NARAYANAN, ON THE INSTABILITY OF BITCOIN WITHOUT THE BLOCK REWARD (PRINCETON UNIVERSITY DEPARTMENT OF ECONOMICS, 2016), <https://economics.princeton.edu/working-papers/on-the-instability-of-bitcoin-without-the-block-reward>. See also ERIC BUDISH, THE ECONOMIC LIMITS OF BITCOIN AND THE BLOCKCHAIN (NBER, Working Paper No. 24717, 2018), [https://ericbudish.org/wp-content/uploads/2022/03/economic\\_limits\\_bitcoin\\_blockchain.pdf](https://ericbudish.org/wp-content/uploads/2022/03/economic_limits_bitcoin_blockchain.pdf). See also ANTONIO FATAS, THE ECONOMICS OF FINTECH AND DIGITAL CURRENCIES 39-45 (CEPR PRESS, 2019), [https://cepr.org/sites/default/files/publication-files/60138-the\\_economics\\_of\\_fintech\\_and\\_digital\\_currencies.pdf](https://cepr.org/sites/default/files/publication-files/60138-the_economics_of_fintech_and_digital_currencies.pdf).

167 Hilary J. Allen, *DeFi: Shadow Banking 2.0?*, WILLIAM & MARY LAW REVIEW (Feb. 18, 2022), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4038788](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038788).

168 Brady Dale, *Vote Buying Scandal Stokes Fears of EOS Governance Failure*, COINDESK, (Oct. 3, 2018), <https://www.coindesk.com/vitalik-called-it-vote-buying-scandal-stokes-fears-of-eos-failure>.

169 Angela Walch, Professor of Law, St. Mary’s University School of Law, Written Testimony before the United States Senate Committee on Banking, Housing, and Urban Affairs, (Jul. 27, 2021), <https://www.banking.senate.gov/imo/media/doc/Walch%20Testimony%2027-27-21.pdf>. See also Hilary J. Allen, *supra* note 167.

170 RAPHAEL AUER, ET AL., *supra* note 28, at 4.

The increasing use of public blockchains exposes users to new forms of risks. As detailed in Part VI, this report recommends a multi-part approach to addressing these risks, including through the expanded application of existing operational risk management standards, when possible, enhanced use of supervisory guidance, as well as alerts to consumers, investors, and businesses to adopt improved diligence tactics, and actions to ensure financial literacy on crypto-assets, including with respect to operational risks that are unique to the crypto-asset ecosystem.

## Risks in Crypto-asset Intermediation

In addition to conduct risks in the crypto-asset ecosystem and novel operational risks, there are also traditional financial risks that have the potential to manifest in crypto-asset markets, with specific implications given the dynamics of such markets. Crypto-assets, regardless of the range of financial and non-financial characteristics they may have, are often created, marketed, traded, and custodied using the same technology systems, security protocols, and financial and operational controls. The unique exposures between crypto-asset entities and products may create a basis for heightened concern. Namely, the firms acting as intermediaries, systems administrators, and other parties in crypto-asset markets may not sufficiently account for the negative externalities that could affect these interconnected assets, firms, or activities, as compared to traditional financial firms whose non-financial activities are often limited or subject to significant controls.

Consumers, investors, and businesses using crypto-assets are exposed to risks, as crypto-asset intermediaries may lack—or have chosen not to dedicate or develop—adequate resources or capabilities to perform their obligations, leading to a loss of value for the users, disruptions of the affected customers’ businesses, and reduced confidence in the crypto-asset sector generally. The resulting loss of confidence may also produce a local or generalized withdrawal of resources from affected firms or activities, increasing the impact of the initial effects.<sup>171</sup> The potential risks associated with crypto-asset firms and market practices include those described below.

### *Resources and Capabilities Risks*

The high volatility in the price of crypto-assets, including those used in lending and staking activities, may increase the risk of margin calls on crypto-asset intermediaries, as well as follow-on collateral liquidations if margin calls are not met. While some states regulate the safety and soundness of crypto-asset firms licensed as non-banks, state laws do not address the national and international scope of activities of these firms.<sup>172</sup> As a result, capital and liquidity buffers to absorb and limit the effects of financial shocks and imbalances may be insufficient to address the increasing risk of firm failures and disruptions that may negatively impact consumers, investors, and businesses, particularly for the many development-stage crypto-asset firms and projects.

### *Custody Risks*

While crypto-asset third-party custody is a dynamic and rapidly developing field, there is currently no comprehensive regime that protects consumers, investors, and businesses in the event of a

---

171 MICHAEL TAYLOR, “TWIN PEAKS”: A REGULATORY STRUCTURE FOR THE NEW CENTURY (CENTRE FOR THE STUDY OF FINANCIAL INNOVATION, 1995).

172 Benjamin T. Seymour, *The New Fintech Federalism*, YALE JOURNAL OF LAW & TECHNOLOGY (VOL. 24, 2022), at 1, [https://yjolt.org/sites/default/files/seymour\\_-\\_the\\_new\\_fintech\\_federalism.pdf](https://yjolt.org/sites/default/files/seymour_-_the_new_fintech_federalism.pdf).

crypto-asset custodian’s insolvency and failure. Among other things, while many of the platform models involve custody, the concept of “custody” for crypto-assets is different than for traditional financial assets with which a customer may be familiar. Crypto-asset firms that appear to share characteristics of traditional financial firms but whose operating companies take the position that, or operate as if, they are unregulated may not qualify under provisions of the Bankruptcy Code,<sup>173</sup> the Uniform Commercial Code, and the Securities Investor Protection Act that provide legal certainty for the treatment for traditional financial firms and financial contracts (e.g., commodity and securities contracts involving brokers, financial institutions, and clearing agencies).<sup>174</sup> Thus, if a crypto-asset platform or other firm that custodies crypto-assets enters bankruptcy, customers may not be able to access or liquidate their crypto-assets for months or years, if at all.<sup>175</sup> Such risks are particularly pronounced when an insolvent firm’s estate is concentrated in crypto-assets with volatile prices, which may complicate the administration of the bankruptcy proceeding.

Crypto-asset third-party custodians may also hold customers’ keys in a centralized manner, comingling customers’ funds with the custodian’s own crypto-asset funds and creating a dependency of the customer on the custodian different than in more traditional financial custody relationships. If a custody provider were to be reorganized or liquidated under the Bankruptcy Code, a bankruptcy court may treat customers of the custodian as unsecured creditors who stand to lose some or all of their investment.<sup>176</sup> Custodians may also use sub-custodians, which further compounds risks to customers by introducing a second layer of credit risk.<sup>177</sup>

## Risk Exposures: Regulatory Non-Compliance and Evolving Market Oversight

Since the creation of crypto-assets, regulators and lawmakers have been applying existing financial market regulatory frameworks to crypto-assets. Although there is no simple, one-sized approach to all crypto-assets and related products and services, regulators have taken steps—through the issuance of guidance and enforcement actions—that respond to questions, and further action is needed to ensure a cohesive regulatory coverage.

---

173 Banking institutions and other depositories are subject to special resolution regimes in case of insolvency.

174 See, e.g., Philip D. Anker & George W. Shuster, Jr., *Exceptional Insolvencies: Provisions of the Bankruptcy Code and SIPA Regarding Broker-Dealers and Other Financial Market Participants and Contracts*, WILMERHALE (Sep. 17, 2008), <https://www.wilmerhale.com/en/insights/publications/exceptional-insolvencies-provisions-of-the-bankruptcy-code-and-sipa-regarding-broker-dealers-and-other-financial-market-participants-and-contracts>. See also Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, UNIVERSITY OF MIAMI BUSINESS LAW REVIEW (Vol. 24 Issue 1, Jun. 1, 2016), <https://repository.law.miami.edu/umblr/vol24/iss3/3>.

175 Vicky Ge Huang, *Celsius Customers Are Losing Hope for Their Locked-Up Crypto*, THE WALL STREET JOURNAL (Jul. 3, 2022), [www.wsj.com/articles/celsius-customers-are-losing-hope-for-their-locked-up-crypto-11656840601?mod=series\\_cryptobitcoinandogecoin](http://www.wsj.com/articles/celsius-customers-are-losing-hope-for-their-locked-up-crypto-11656840601?mod=series_cryptobitcoinandogecoin). See also Eliot Brown & Yifan Wang, *Crypto Broker Voyager Digital Files for Bankruptcy Protection*, THE WALL STREET JOURNAL (Jul. 6, 2022), [https://www.wsj.com/articles/crypto-broker-voyager-digital-files-for-bankruptcy-protection-11657098630?mod=hp\\_lead\\_pos4](https://www.wsj.com/articles/crypto-broker-voyager-digital-files-for-bankruptcy-protection-11657098630?mod=hp_lead_pos4).

176 Sidney P. Levinson, Caroline N. Swett, Alison M. Hashmall & Elie J. Worenklein, *Recent Disclosure Guidance Highlights Growing Concern Surrounding the Risks of User Assets Held by Various Crypto Custodians*, DEBEVOISE & PLIMPTON (Jun. 6, 2022), <https://www.debevoise.com/insights/publications/2022/06/recent-disclosure-guidance-highlights>. Banks are subject to a distinct irresolution regime, as the Bankruptcy Code precludes “banks” from being debtors. See Adam J. Levitin, *Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency*, TEXAS LAW REVIEW (Vol. 101, 2022), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4107019](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4107019).

177 The use of smart contracts and distributed applications in DeFi also means that even non-custodied holdings of crypto-assets may be subject to new forms of intermediation risks and inefficiencies, such as those produced by the technical features of the software programs themselves and ones resulting from actions taken by DAOs, validators, miners and other parties that influence outcomes produced by smart contracts and distributed applications. See MICHAEL CASEY, ET AL., *supra* note 43, at 4-5.

Questions around regulation and supervision of crypto-assets are complicated by the fact that some actors within the crypto-asset ecosystem attempt to design markets, products, and services such that they fall outside of the regulatory perimeter and actively dispute the application of existing laws and regulations. At the same time, other intermediaries have sought guidance on the structure, delivery, and reporting of crypto-asset activities to provide more regulatory certainty. This unique landscape affects the relative exposure of consumers, investors, and businesses to the risks of digital assets, markets, and technologies.

#### *Current Legal and Regulatory Landscape for Crypto-assets*

The current regulatory treatment of crypto-assets depends on the facts and circumstances of the crypto-asset, the nature of the activities, and the classification of entities or service providers. U.S. federal financial regulatory agencies with authority to address violations arising from the conduct risks associated with crypto-assets may include market regulators, banking regulators, agencies responsible for safeguarding the financial system from illicit use, and agencies with authority to enforce consumer protection laws. In addition, state agencies, including state securities and banking regulators often have authorities under state laws that apply to aspects of the crypto-asset ecosystem.<sup>178</sup>

The financial regulation, supervision, and enforcement framework is generally based upon the following criteria:

- (i) The product and service that is being provided. The CFTC primarily oversees commodity derivatives and associated markets and intermediaries and maintains anti-fraud and anti-manipulation enforcement over commodities that are not securities; the SEC oversees securities and securities derivatives and their associated markets and intermediaries; and the Department of Labor oversees the investment activities of retirement plan fiduciaries;
- (ii) The entity providing the service. For example, the Federal Reserve oversees activities of bank holding companies and state-chartered banks and savings associations that are members of the Federal Reserve System; the OCC supervises national banks and federal savings associations; and the FDIC is the federal supervisor for state-chartered banks and savings associations that are not members of the Federal Reserve System; and
- (iii) Whether an activity violates a civil or criminal statute. For example, the Department of Justice prosecutes various types of securities, commodities, and crypto-asset-related criminal activities, including various types of financial fraud.

The CFPB also regulates the offering of consumer financial products and services—which, depending on the facts and circumstances, may include a variety of crypto-asset related offerings—under the federal consumer financial laws, including (among others) the Dodd-Frank Act’s prohibition against unfair, deceptive, or abusive acts or practices for consumer financial products and services. Notably, no federal regulator currently has the authority to comprehensively oversee spot markets for crypto-assets that are not securities and to issue regulations over those markets to ensure market integrity.<sup>179</sup>

---

178 See NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, *NASAA Updates Coordinated Crypto Crackdown*, (Aug. 7, 2019), <https://www.nasaa.org/52027/nasaa-updates-coordinated-crypto-crackdown-2/?qoid=current-headlines>.

179 A more detailed discussion of the regulatory treatment of crypto-assets and potential gaps, especially regarding financial stability, may be found in the forthcoming report of the Financial Stability Oversight Council in response to the Section 6 of the Executive Order.

## *Effects of Legal and Regulatory Non-Compliance*

Notwithstanding the efforts of these legal and regulatory authorities, consumers, investors, and businesses remain exposed to risks, some of which arise from misconduct by bad actors, while others occur when products and services are not in compliance with regulatory requirements, regardless of intent. In particular, risks arise from non-compliance with (i) the extensive disclosure requirements for registered exchanges, products, and intermediaries that are designed to provide investors and customers with material and relevant information and (ii) the requirements around market conduct that are designed to provide fair, orderly, and efficient markets.

Some traditional financial activities and consumer financial products and services, as well as native crypto-asset firms also may view themselves—and thus operate as if—their crypto-asset activities are not subject to federal laws and regulations. This could result in crypto-asset-based activities that are economically, but not necessarily legally, equivalent to traditional financial activities exposing consumers, investors, and businesses to significant economic risks because they are not regulated in an equivalent manner. For example, despite the apparent analogy to traditional savings and deposit accounts, crypto-asset platforms may restrict withdrawals and are not covered by deposit insurance.<sup>180</sup>

Users of these crypto-asset products may be unaware of such differences and therefore be less likely to take actions that could reduce their risk exposures. Further, crypto-asset users — or those who use intermediaries—that are out of compliance with laws and regulations generally are not receiving required disclosures regarding issues such as conflicts of interests, risks, and fees.

## *Effects of Changes in the Scope and Application of Laws and Regulations*

Crypto-assets are rapidly developing, and the extent to which crypto-asset products, services, and technologies are, or should be, subject to certain U.S. laws and regulations covering conduct, operational, and intermediation risks is being actively debated. To some proponents of crypto-assets, a key goal underlying the creation and development of the crypto-asset ecosystem is the establishment of a peer-to-peer financial system that would eliminate the reliance on large incumbent intermediaries, such as banks and other traditional centralized institutions. Some extend that goal to avoiding the oversight associated with those traditional institutions.

While these perspectives are animating the public discourse regarding crypto-assets, consumers, investors, and businesses may be exposed to heightened risk from unproven features and design flaws in crypto-asset products and services. The regulatory regimes for these products and services are also still evolving.

As described in more detail in Part VI, Recommendations, regulatory agencies should use their existing authorities to address current and emerging risks in crypto-asset intermediation to the extent that such activities fall within their jurisdictions. Examples include the OCC's interpretive letters to clarify

---

180 The SEC has brought an enforcement action against a crypto-lending product for failure to properly register. See SEC, *BlockFi Agrees to Pay \$100 Million in Penalties and Pursue Registration of its Crypto Lending Product*, (Feb.14, 2022), <https://www.sec.gov/news/press-release/2022-26>. The FDIC has also issued cease and desist orders against crypto-asset companies for misstating whether their products or services are covered by federal deposit insurance. See FDIC, *FDIC Issues Cease and Desist Letters to Five Companies For Making Crypto-Related False or Misleading Representations about Deposit Insurance*, (Aug. 19, 2022), <https://www.fdic.gov/news/press-releases/2022/pr22060.html>.

the expectations of its regulated entities regarding the safeguarding of crypto-assets for customers; the SEC's special purpose broker-dealer statement on digital asset custody, which lays out certain circumstances in which the SEC will not take certain enforcement action against broker-dealers with respect to digital asset securities; and the Department of Labor's compliance assistance release cautioning retirement plan fiduciaries to be mindful of their stringent obligations of prudence and loyalty in connection with investments in cryptocurrencies.

## **V. OPPORTUNITIES AND RISKS FOR POPULATIONS VULNERABLE TO DISPARATE IMPACTS**

As discussed above, crypto-assets present a variety of potential opportunities and known and emerging risks for consumers, investors, and businesses. The nature and intensity of these risks and opportunities varies across populations and communities. This is due both to underlying social and economic factors (for example, wealth disparities, historic exclusion from the financial system, and uneven digital access), as well as crypto-asset-specific behaviors, including marketing practices that may be inappropriately targeting specific communities, potentially in an unfair or abusive manner. This part of the report identifies some of the benefits and opportunities that populations most vulnerable to disparate impacts may experience from the growth of the crypto-asset ecosystem. This part also discusses the unique risks that crypto-assets may present to these communities and notes risks identified elsewhere in this report that are likely to impact certain populations in disparate ways.

For the purposes of this analysis, we consider populations most vulnerable to disparate impacts to include the low-income population, communities that have been historically excluded from the financial system or subject to discrimination in accessing financial services or wealth-building opportunities, including Black, Indigenous, and People of Color (BIPOC) communities, as well as unbanked and underbanked populations,<sup>181</sup> the elderly, and children. Not all populations vulnerable to disparate impacts are alike, and there is substantial variation both within and across communities and individuals. Certain individuals might be considered vulnerable to disparate impact due to high exposure relative to disposable income, such as low-income individuals. Others may have an increased likelihood of encountering bias and discrimination, such as BIPOC individuals. Some elderly individuals may have less familiarity with digital offerings and may be more susceptible to fraud and scams. Children may be more impressionable and thus less prone to question targeted marketing. Disparate impacts are also likely to vary by crypto-asset offering, with different products and services potentially posing different opportunities and risks for users.

Some market participants have been promoting crypto-assets to those who lack access as a means to advance financial inclusion and build wealth, with the stated promise to serve as an alternative, or an entry point, to the banking system and traditional financial services. Specifically, some advocates have argued that crypto-assets can facilitate broader access to investment opportunities and potentially lower-cost, more accessible, financial products. There is limited data on the crypto-asset use and experience of populations vulnerable to disparate impacts. However, available

---

181 As used in this report, "unbanked" refers to individuals without a bank account; "underbanked" refers to individuals with a bank account who make use of alternative financial services offered by non-bank firms, such as money orders, bill payments services, and check cashing.

evidence to date suggests that potential financial inclusion benefits of crypto-assets largely have yet to materialize, and crypto-asset products may present increased risks to populations vulnerable to disparate impacts.

Populations vulnerable to disparate impact are engaging with crypto-assets. Survey data from the Federal Reserve Board finds that 29% of respondents who held crypto-assets for investment purposes had an annual household income of less than \$50,000.<sup>182</sup> Additionally, certain BIPOC communities may be over-represented in crypto-asset ownership or may be more likely than white individuals to own crypto-assets.<sup>183</sup> As explored below, elderly individuals have been targeted in fraud schemes and scams, and children have been targeted in marketing campaigns. Given these current risks, greater urgency in examining and responding to the potential disparate impacts of crypto-asset activities is warranted.

## Potential Opportunities for Populations Vulnerable to Disparate Impacts

Some proponents argue that crypto-assets present opportunities to expand access to financial services, improve upon existing services by reducing transaction costs, and build wealth. However, evidence currently available indicates that realization of such benefits has been limited to date.

### *Expanded Access to Financial Services*

There have long been gaps in access to financial services, resulting both from logistical and cost challenges in reaching consumers with affordable access to the products they need, and from a history of institutional discrimination through racist policies and practices that have had lasting systemic impacts that have limited access to financial services and wealth building opportunities for many BIPOC individuals.<sup>184</sup> To this day, unbanked and underbanked rates are higher among lower-income and Black and Hispanic adults.<sup>185</sup> Within this context, some market observers highlight the potential for crypto-assets to address financial inequities and provide more inclusive access to financial services.<sup>186</sup>

---

182 BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 53, at 45.

183 Andrew Perrin, *supra* note 54; and MORNING CONSULT, *The State of Consumer Banking & Payments*, (2022), [https://go.morningconsult.com/rs/850-TAA-511/images/220120\\_State\\_of\\_Consumer\\_Banking.pdf](https://go.morningconsult.com/rs/850-TAA-511/images/220120_State_of_Consumer_Banking.pdf). See also Terri Bradford, *The Cryptic Nature of Black Consumer Cryptocurrency Ownership*, FEDERAL RESERVE BANK OF KANSAS CITY (Jun. 1, 2022), <https://www.kansascityfed.org/research/payments-system-research-briefings/the-cryptic-nature-of-black-consumer-cryptocurrency-ownership>.

184 See Rocio Sanchez-Moyano and Bina Patel Shrimali, *The Racialized Roots of Financial Exclusion*, FEDERAL RESERVE BANK OF SAN FRANCISCO (Aug. 19, 2021), <https://www.frbsf.org/community-development/publications/community-development-investment-review/2021/august/the-racialized-roots-of-financial-exclusion>. See also Kristen Broady, Mac McComas & Amine Ouazad, *An Analysis of Financial Institutions in Black-Majority Communities: Black Borrowers and Depositors Face Considerable Challenges in Accessing Banking Services*, BROOKINGS INSTITUTION (Nov. 2, 2021), <https://www.brookings.edu/research/an-analysis-of-financial-institutions-in-black-majority-communities-black-borrowers-and-depositors-face-considerable-challenges-in-accessing-banking-services>. See also Kevin Fox Gotham, *Race, Mortgage Lending and Loan Rejections in a U.S. City*, SOCIOLOGICAL FOCUS (Vol. 31 No. 4, 1998), at 392-94, <https://www.jstor.org/stable/20832008>. See also Jung Hyun Choi and Peter J. Mattingly, *What Different Denial Rates Can Tell Us About Racial Disparities in the Mortgage Market*, URBAN INSTITUTE (Jan. 13, 2022), <https://www.urban.org/urban-wire/what-different-denial-rates-can-tell-us-about-racial-disparities-mortgage-market>. See also PEW CHARITABLE TRUSTS, WHO BORROWS, WHERE THEY BORROW, AND WHY 9 (2012), [https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pew\\_assets/2012/pewpaydaylendingreportpdf.pdf](https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pew_assets/2012/pewpaydaylendingreportpdf.pdf); and PEW CHARITABLE TRUSTS, THE COMPLEX STORY OF AMERICAN DEBT 4-5 (2015), [https://www.pewtrusts.org/-/media/assets/2015/07/reach-of-debt-report\\_artfinal.pdf](https://www.pewtrusts.org/-/media/assets/2015/07/reach-of-debt-report_artfinal.pdf).

185 Unbanked and underbanked rates are also higher among adults with less education. See BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 53, at 43-44.

186 See, e.g., WORLD ECONOMIC FORUM, WHAT IS THE VALUE PROPOSITION OF STABLECOINS FOR FINANCIAL INCLUSION? 11-12 (2021), [https://www3.weforum.org/docs/WEF\\_Value\\_Proposition\\_of\\_Stablecoins\\_for\\_Financial\\_Inclusion\\_2021.pdf](https://www3.weforum.org/docs/WEF_Value_Proposition_of_Stablecoins_for_Financial_Inclusion_2021.pdf).

According to data from one survey, a greater share of unbanked and underbanked individuals may own crypto-assets than individuals considered “fully banked.”<sup>187</sup> Early evidence also suggests that unbanked individuals may be more inclined to use crypto-assets for transactions, indicating they may be interested in crypto-assets as an alternative means to accessing basic financial services.<sup>188</sup> Most individuals who have owned crypto-assets have done so for investment purposes, and 99% of those who invested in crypto-assets—but did not use it for transactions—had a bank account.<sup>189</sup> Of the small percentage of adults who had used crypto-assets for transactions, 13% were unbanked, compared to 6% of adults who had not used crypto-assets.<sup>190</sup>

These findings suggest an over-representation of unbanked individuals using crypto-assets for transactions; they also indicate that 87% of the small percentage of adults who are using crypto-assets for transactions have a bank account. The motivations for individuals—particularly banked individuals—to use crypto-assets for transactions are unclear, particularly given transaction costs and market volatility may limit the utility of crypto-assets as a medium of exchange. Transaction usage by both banked and unbanked individuals is very limited, yet it appears that some small portion of individuals who are underserved by the mainstream financial system may be using crypto-assets to engage in transactions.

To understand the broader opportunity for crypto-assets to expand access to financial services, it is important to consider the reasons some individuals remain outside of the banking system. According to data from the FDIC, the top five reasons for individuals being unbanked—ranking in order of most commonly cited—are: (i) insufficient funds to meet minimum balance requirements, (ii) lack of trust in banks, (iii) privacy concerns, (iv) high bank account fees, and (v) lack of predictability of bank account fees.<sup>191</sup> It is still unclear to what degree crypto-asset based financial solutions might address these concerns and expand access for unbanked individuals.

To a certain degree, broader economic disparities underlie the specific disparities in access to, and use of, financial services.<sup>192</sup> Financial needs, such as the lack of sufficient resources to meet minimum balance requirements, cannot be addressed through financial services offerings—crypto-asset-based or otherwise. Instead, they require solutions that directly address the underlying economic issues.<sup>193</sup>

With regard to issues of trust and privacy concerns, some crypto-asset proponents argue that consumers and businesses may be more inclined to trust crypto-assets due to the decentralized and

---

187 Charlotte Principato, *Banking the Unbanked Requires Raising Trust and Awareness. For the Underbanked, Better Service Means Payments Innovation*, MORNING CONSULT (Aug. 17, 2021), <https://morningconsult.com/2021/08/17/trust-awareness-payments-unbanked-underbanked>. The survey found that 37% of underbanked and 12% of unbanked individuals owned cryptocurrency, compared to 10% of individuals considered fully banked. See also BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 53, at 45-46.

188 BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 53, at 45-46.

189 *Id.* In total, the survey found that 12% of adults had held or used cryptocurrencies in the past 12 months; 11% of adults had held cryptocurrency as an investment, while just 2% had used cryptocurrency to buy something or make a payment and 1% to send money to friends or family.

190 *Id.*

191 FDIC, *HOW AMERICA BANKS: HOUSEHOLD USE OF BANKING AND FINANCIAL SERVICES 17* (2019), <https://www.fdic.gov/analysis/household-survey/2019report.pdf>.

192 See BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 53, at 43.

193 Abbye Atkinson, *Rethinking Credit as Social Provision*, STANFORD LAW REVIEW (May 2019), at 1093-1162, <https://review.law.stanford.edu/wp-content/uploads/sites/3/2019/05/Atkinson-71-Stan.-L.-Rev.-1093-2019.pdf>.

pseudonymous nature of transactions and distribution and lack of traditional intermediaries. Trust in crypto-assets may be undermined by the risks related to operational issues, market volatility, targeting for fraud and scams, and privacy.<sup>194</sup> Additionally, many crypto-asset systems increasingly rely on centralized intermediaries and traditional financial institutions to carry out their functions or at a minimum to convert between crypto-assets and fiat currency. This may weaken the appeal of crypto-assets as an alternative for those who remain unbanked due to a lack of trust in such financial institutions, and more broadly inhibit unbanked individuals from accessing crypto-assets.<sup>195</sup>

Another challenge to the opportunity for crypto-assets to expand access is the “digital divide,” the gap between those who have ready access to computers, smartphones, and the internet, and those who do not. Underbanked individuals and individuals more broadly who face barriers to mainstream financial services, including those with lower income and those who identify as BIPOC, are often more likely to lack access to certain technology services and infrastructure.<sup>196</sup>

It is certainly the case that most, if not all, financial market intermediaries could improve reach and access to affordable financial products and services that meet the needs of consumers and businesses. To date, it appears that little progress has been accomplished through the use of crypto-asset based offerings as a means of greater financial inclusion. Only an estimated 1% of adults use crypto-assets exclusively for non-investment purposes,<sup>197</sup> and just 12% of unbanked individuals own crypto-assets at all.<sup>198</sup> Additionally, the ability of crypto-asset based financial services to address the concerns currently inhibiting individuals’ use of mainstream financial services remains unclear, and the digital divide remains a challenge.

### *Reduced Transaction Costs*

Crypto-assets may offer a means to provide users with lower-cost payment mechanisms, reducing bank fees, transfer fees and other costs. While this could prove a benefit to all users, individuals for whom such fees have been economically burdensome, or have inhibited their access to financial services, could particularly stand to benefit.<sup>199</sup> As noted, high and unpredictable costs are among

---

194 See WORLD ECONOMIC FORUM, *supra* note 186, at 16, 22.

195 Kristin N. Johnson, *Decentralized Finance: Regulating Cryptocurrency Exchanges*, WILLIAM & MARY LAW REVIEW (Vol. 62 Issue 6, 2021), at 1911, 1921, <https://scholarship.law.wm.edu/wmlr/vol62/iss6/4>. See WORLD ECONOMIC FORUM, *supra* note 186, at 13 (noting the “[l]ack of first- and last-mile infrastructure for conversions between physical cash and digital money” as a limitation on stablecoins’ financial inclusion prospects). Suggested alternatives to banks for storing crypto-assets include the use of gift cards, a credit card, or crypto-ATMs. See Kat Tretina, *How to Buy Cryptocurrency*, FORBES ADVISOR (May 15, 2022), <https://www.forbes.com/advisor/investing/cryptocurrency/how-to-buy-cryptocurrency>.

196 As of 2019, just 33.8% of unbanked households had home internet access, compared to 82.6% of banked households. See FDIC, HOW AMERICA BANKS: HOUSEHOLD USE OF BANKING AND FINANCIAL SERVICES APPENDIX TABLES 48 (2019), <https://www.fdic.gov/analysis/household-survey/2019appendix.pdf>. See also Sara Atske & Andrew Perrin, *Home broadband adoption, computer ownership vary by race, ethnicity in the U.S.*, PEW RESEARCH CENTER (Jul. 16, 2021), <https://www.pewresearch.org/fact-tank/2021/07/16/home-broadband-adoption-computer-ownership-vary-by-race-ethnicity-in-the-u-s>. See also WORLD ECONOMIC FORUM, *supra* note 186, at 13, 16.

197 BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 53, at 45-46.

198 Charlotte Principato, *supra* note 187.

199 See Ying Lei Toh, *When Paying Bills, Low-Income Consumers Incur Higher Costs*, FEDERAL RESERVE BANK OF KANSAS CITY (Nov. 23, 2021), <https://www.kansascityfed.org/research/payments-system-research-briefings/when-paying-bills-low-income-consumers-incur-higher-costs>. See also Aaron Klein, Senior Fellow, Brookings Institution, Opening statement of Aaron Klein at roundtable on America’s unbanked and underbanked (Dec. 15, 2021), <https://www.brookings.edu/opinions/opening-statement-of-aaron-klein-at-roundtable-on-americas-unbanked-and-underbanked>.

the most significant reasons individuals cited for being unbanked.<sup>200</sup> Thus the potential for reduced transaction costs presents a significant opportunity to increase financial inclusion.

While there is not currently sufficient data to comprehensively evaluate whether the crypto-asset ecosystem generally provides lower-fee financial services than traditional banking, international financial transactions provide an example that may be instructive. Costs for these transactions tend to be high; the average cost of remittances under \$200—which is often typical for low-income migrants—are on average 7% for a money transfer and can be as high as 15–20% of the principal in smaller migration corridors.<sup>201</sup> In addition, despite arguments that crypto-assets could facilitate cheaper and faster remittance payments, evidence suggests that many international crypto-asset transfers are not currently cost-effective, faster, or easier alternatives to cash, especially given the complexity of converting crypto-assets to and from local currencies.<sup>202</sup> The additional costs related to exchanging between fiat and cryptocurrencies alone can make such transactions more expensive than non-crypto-asset alternatives.<sup>203</sup> These fees are often compounded by fees paid to miners to validate transactions, and fees for matching buy and sell orders, which can be prohibitively expensive, particularly for small transactions.<sup>204</sup> According to analysts at crypto-asset platforms, the typical transaction price, or gas, on the Ethereum network can fluctuate widely depending on network congestion.<sup>205</sup> This limited evidence suggests that the potential benefits of reduced transaction prices on crypto-asset based payments systems have yet to be realized.

### *Potential Opportunities to Build Wealth*

As noted earlier, the majority of individuals who own crypto-assets do so for investment purposes.<sup>206</sup> Some members of communities historically excluded from wealth-building opportunities, including many BIPOC individuals, perceive crypto-assets as an opportunity to build wealth and narrow the racial wealth gap.<sup>207</sup> The view that crypto-assets can help build wealth has been particularly attractive to members of historically excluded communities who have some amount of financial stability but may lack access to the range of wealth-building investment products that come with being an accredited investor or accessing professional investment advice.

200 FDIC, *supra* note 191, at 17. See also CITIES FOR FINANCIAL EMPOWERMENT FUND, CFE FUND BANK ON COALITION PLAYBOOK (2021), [https://issuu.com/cfefund/docs/bank\\_on\\_playbook\\_jan\\_2017](https://issuu.com/cfefund/docs/bank_on_playbook_jan_2017). The report finds that prevalent reasons given cited by unbanked people for not having a bank account are “not having enough money to keep in an account” (43%) and “bank fees are too high” (32%).

201 Dilip Ratha, *Remittances: Funds for the Folks Back Home*, INTERNATIONAL MONETARY FUND (Feb. 24, 2020), <https://www.imf.org/external/pubs/ft/fandd/basics/remitt.htm>.

202 See, e.g., Dirk G. Baur & Thomas Dimpfl, *The Volatility of Bitcoin and Its Role as a Medium of Exchange and a Store of Value*, EMPIRICAL ECONOMICS (Vol. 61, Jan. 5, 2021), at 2663–2683, <https://doi.org/10.1007/s00181-020-01990-5>.

203 See Alexis Goldstein, Director of Financial Policy, Open Markets Institute, Written Testimony before the Committee on Banking, Housing, and Urban Affairs (Dec. 14, 2021), at 10, <https://www.banking.senate.gov/imo/media/doc/Goldstein%20Testimony%202012-14-21.pdf>. Moving into and out of stablecoins can add to the foreign exchange transaction fees involved in remitting money. When accounting for these “double-hop” costs, total fees incurred by utilizing stablecoins and digital exchanges (ranging from \$5.98 to \$86.44) can be more expensive than fees associated a payment system like Western Union (\$4.88).

204 Paul Vigna, *Crypto and Its Many Fees: What to Know About the Hidden Costs of Digital Currency*, THE WALL STREET JOURNAL (Dec. 18, 2021), <https://www.wsj.com/articles/crypto-and-its-many-fees-what-to-know-about-the-hidden-costs-of-digital-currency-11639825202>.

205 *Id.*

206 BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 53, at 45-46. In total, the survey found that 12% of adults had held or used cryptocurrencies in the past 12 months; 11% of adults had held cryptocurrency as an investment, while just 2% had used cryptocurrency to buy something or make a payment and 1% to send money to friends or family.

207 Taylor Nicole Rogers, *Crypto collapse reverberates widely among black American investors*, FINANCIAL TIMES (Jul. 4, 2022), <https://www.ft.com/content/47d338e2-3d3c-40ce-8a09-abfa25c16a7f>.

However, such communities may be inappropriately targeted by crypto-asset marketing, as well as fraud schemes, as explored in the part below exploring potential risks. Ultimately, the wealth-building potential of crypto-assets is highly uncertain, and some have expressed concern that disproportionate exposure by BIPOC communities could further exacerbate the racial wealth gap when crypto-asset markets decline.<sup>208</sup> Additionally, these markets have been highly volatile, which could pose concerns particularly for individuals with lower incomes. These risks are explored below.

## Potential Risks to Populations Vulnerable to Disparate Impacts

Different populations and individuals vulnerable to disparate impacts may be subject to greater harms depending on the nature of the particular risks of engaging with crypto-assets. Some may be more exposed to the volatility and risk of crypto-asset investing; others may be at greater risk of being preyed upon by targeted marketing, fraud, and scams; and still others may be more limited in their capacity to recover from financial harm.

### *Market Volatility and Inadequate Disclosures*

Crypto-assets are subject to large price fluctuations, and consumer advocacy groups have warned of the lack of adequate consumer protection.<sup>209</sup> In many ways, the risks associated with owning crypto-assets are the same for everyone. However, individuals with less resources, including lower-income individuals, may have greater exposure in relation to their disposable income, meaning incurred losses could have an outsized negative impact on their financial well-being. As noted above, 29% of respondents who held crypto-assets for investment purposes had an annual household income of less than \$50,000.<sup>210</sup>

Market volatility and a lack of protections or sufficient risk disclosures could also undermine trust in crypto-assets, particularly among populations vulnerable to disparate impacts, some of whom may be particularly wary of financial markets and institutions. Unexpected losses due to market movements and a lack of understanding of potential exposure could undermine consumer trust and confidence in the crypto-asset ecosystem.<sup>211</sup> This deterioration in trust may have the potential to drive further negative impact on the asset's price. These dynamics are analogous to those experienced in the U.S. banking system prior to the development of the modern regime of banking law and regulation.<sup>212</sup> During Reconstruction, many Black Americans were led to believe that their deposits in the Freedman's Savings Bank were guaranteed by the federal government. Black Americans' trust in financial institutions was affected by the deposits they lost when the bank collapsed and depositors'

---

208 Paulina Cachero, *Crypto Collapse Threatens to Leave Black, Hispanic Investors Further Behind*, BLOOMBERG LAW (Jul. 7, 2022), <https://news.bloomberglaw.com/banking-law/crypto-collapse-threatens-to-leave-black-hispanic-investors-further-behind>.

209 See, e.g., National Consumer Law Center, Comments to Department of the Treasury Office of the Comptroller of the Currency on the Advance notice of proposed rulemaking on National Bank and Federal savings Association Digital Activities (Aug. 3, 2020), at 19-20, <https://www.nclc.org/images/pdf/rulemaking/2020-OCC-fintech-NCLC-comments.pdf>.

210 BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 53, at 45.

211 WORLD ECONOMIC FORUM, *supra* note 186. See also Joe Weisenthal, *Mark Cuban Calls for Stablecoin Regulation After Trading Token That Crashed to Zero*, BLOOMBERG (Jun. 17, 2021), <https://www.bloomberg.com/news/articles/2021-06-17/mark-cuban-defi-iron-finance-crashed-100?sref=M8H6LjUF#xj4y7vzkg>; Elizabeth Lopatto, *The Tether Controversy, Explained*, THE VERGE (Aug. 16, 2021), <https://www.theverge.com/22620464/tether-backing-cryptocurrency-stablecoin>.

212 Gary B. Gorton & Jeffrey Zhang, *Taming Wildcat Stablecoins*, UNIVERSITY OF CHICAGO LAW REVIEW (Vol. 90, Forthcoming 2022), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3888752](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3888752).

funds were lost.<sup>213</sup> Researchers at the Federal Reserve Bank of Kansas City have argued that the collapse of a crypto-asset platform, and the resulting loss of customer funds, could be comparable to “a 21st century version of Freedman’s Savings Bank.”<sup>214</sup>

## Targeting

## Marketing

In the past, vulnerable communities, especially low-income communities and communities of color, have been specifically targeted by financial services companies using deceptive sales tactics and marketing.<sup>215</sup> There are several examples where crypto-asset companies are conducting similar marketing practices to particular populations, including those most vulnerable to disparate impact.

Targeted advertising and brand partnerships with prominent athletes and celebrities have been used to attract new customers to crypto-assets, with a particular focus on underserved and racial minority communities.<sup>216</sup> Recent surveys suggest that market participants believe that crypto-asset advertisements have been effective at raising awareness of, and encouraging more people to trade in, crypto-assets.<sup>217</sup> Another example is the prevalence of crypto-asset ATMs (predominantly Bitcoin ATMs, or BTMs) in lower-income neighborhoods that lack bank branches.<sup>218</sup>

Crypto-asset products may be marketed in ways that obscure their level of risk, which could exacerbate the impact of targeted marketing on vulnerable communities. As discussed in Parts II and IV, some crypto-assets and related products market themselves as safe and deposit-like, when they are actually volatile and lack protections including deposit insurance. As a result, consumers, especially those heavily targeted by crypto-asset marketing, might be at risk of viewing crypto-assets as stable consumer financial products, rather than as speculative financial assets, and therefore investing money they are not expecting, and may not be able to afford, to lose.<sup>219</sup> In the case of BTMs, concerns have also been raised regarding high fees and lack of adequate regulation.<sup>220</sup>

Recent studies have also shown that children are being exposed to crypto-assets at an early age and are often more familiar with them than their parents. One such study noted that 57% of kids surveyed

---

213 Terri Bradford, *supra* note 183, at 3.

214 *Id.*, at 4.

215 Examples include the prevalence of subprime mortgage originations and refinancing in communities of color prior to the financial crisis in 2008. See Linda E. Fisher, *Target Marketing of Subprime Loans: Racialized Consumer Fraud & Reverse Redlining*, JOURNAL OF LAW AND POLICY, (Vol. 18, 2009), <https://brooklynworks.brooklaw.edu/jlp/vol18/iss1/3>.

216 See Taylor Nicole Rogers, *Crypto Collapse Reverberates Widely Among Black American Investors*, FINANCIAL TIMES, July 5, 2022, <https://www.ft.com/content/47d338e2-3d3c-40ce-8a09-abfa25c16a7f>.

217 See Terri Bradford, *supra* note 183, at 4.

218 See Susannah Luthi, *Why Bitcoin ATMs are Vexing Rulemakers*, POLITICO (Jul. 6, 2022), <https://www.politico.com/news/magazine/2022/07/06/bitcoin-atms-regulations-00035083>; see also Susan Tompor, *Bitcoin ATMs Showing Up In Odd Spots Across Metro Detroit*, DETROIT FREE PRESS (Jun. 2018), <https://www.freep.com/story/money/personal-finance/susan-tompor/2018/06/28/bitcoin-atm-stock-cryptocurrency-value/629133002>; see also Andy Peters, *Bitcoin ATMs Start To Spread — And To Draw Scrutiny*, ATLANTA JOURNAL-CONSTITUTION (Feb. 14, 2020), <https://www.ajc.com/business/personal-finance/bitcoin-atms-start-spread-and-draw-scrutiny/ZTbMPUOoc0LB1bgC4CLJoI>.

219 This concern could extend, for example, to messaging that equates machines that enable consumer to buy and sell crypto assets to ATMs that allow them to deposit funds into a bank account.

220 See Susannah Luthi, *supra* note 218.

were familiar with crypto-assets (compared to 47% of their parents) and if given \$100, 57% of kids said they would invest their money in crypto-assets (compared to 38% who would invest in stocks).<sup>221</sup> Some high schools have begun to incorporate study of crypto-assets into their financial literacy efforts and there are crypto-focused kids camps that provide children with a laptop, cellphone, and a digital wallet.<sup>222</sup> The marketing of crypto-assets has extended to the launch of a children's show that uses NFTs to cast the shows stars,<sup>223</sup> NFT collections that are designed for children,<sup>224</sup> and a kids-based crypto-asset piggybank app and debit card.<sup>225</sup>

## Fraud and Scams

While data is limited regarding specific victims of fraud or scams, it is clear that at least one population vulnerable to disparate impacts, the elderly, are being targeted.

At just over 34% of the U.S. population, older Americans are becoming an ever-increasing target for online fraud and scams (including cryptocurrency scams).<sup>226</sup> Older Americans are generally at or past their peak of their wealth accumulation, are more likely to be isolated and emotionally vulnerable, may not understand current technologies, and therefore may be targets of frauds and scams.<sup>227</sup> Additionally, financially vulnerable older Americans that lack financial and housing security are generally more likely to take unnecessary risks and fall prey to frauds and scams in the hope of improving their financial condition.<sup>228</sup> In 2021, the FBI received more than 5,100 complaints involving some form of crypto-assets, with losses totaling over \$241 million, from persons over the age of 60.<sup>229</sup> Recent data also suggests that older Americans that are victims of typical online scams (e.g., tech support and romance scams) are increasingly being asked to pay in cryptocurrencies, which are traded through private wallets using public exchanges and can be difficult to trace.<sup>230</sup>

There are also indications that servicemembers are being targeted. Consumer complaints to the CFPB show that crypto-assets are rising as a preferred payment method for scams targeting servicemembers through identity theft or romance scams. Hundreds of published servicemember complaints to the

---

221 T. ROWE PRICE, *Families' Excitement for Cryptocurrency Brings Risks and Opportunities*, (Apr. 5, 2022), [https://www.troweprice.com/content/dam/trowecorp/Press%20Release%20-%20PKM22\\_release\\_FINAL%2004052022.pdf](https://www.troweprice.com/content/dam/trowecorp/Press%20Release%20-%20PKM22_release_FINAL%2004052022.pdf).

222 Sophie Bearman, *The Crypto Craze is Here to Stay – Now it's Even Being Taught in High School*, CNBC, (Feb. 2018), <https://www.cnbc.com/2018/02/07/bitcoin-education-at-high-schools-and-colleges.html>. See also CRYPTO KIDS CAMP, *Educating Future Leaders*, <https://www.cryptokidscamp.org>; LAVNER EDUCATION, *Crypto Camps & Courses for Kids*, <https://www.lavnercampsandprograms.com/crypto-camps-and-courses-for-kids>.

223 Cactus World, *Cactus World to Launch First NFT Kids TV Show*, (Jan. 4, 2022), [https://www.einnews.com/pr\\_news/559611329/cactus-world-to-launch-first-nft-kids-tv-show](https://www.einnews.com/pr_news/559611329/cactus-world-to-launch-first-nft-kids-tv-show).

224 ZIGAZOO, *Zigazoo NFT Guide*, <https://www.zigazoo.com/nft-guide>.

225 PIGZBE App, <https://www.finh.cc/pigzbe-app>.

226 Karen Kali, *Age-Friendly Banking & Low- To Moderate-Income Older Adults*, NATIONAL COMMUNITY REINVESTMENT COALITION (Nov. 2019), [https://nrcr.org/afb-standards/#\\_edn2](https://nrcr.org/afb-standards/#_edn2).

227 Marguerite DeLiema, Martha Deevy, Annamaria Lusardi & Olivia S Mitchell, *Financial Fraud Among Older Americans: Evidence and Implications*, NATIONAL LIBRARY OF MEDICINE (2020), at 861-868, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7328021>.

228 JOINT CENTER FOR HOUSING STUDIES OF HARVARD UNIVERSITY, *Housing America's Older Adults 2019*, (2019), [https://www.jchs.harvard.edu/sites/default/files/Harvard\\_JCHS\\_Housing\\_Americas\\_Older\\_Adults\\_2019.pdf](https://www.jchs.harvard.edu/sites/default/files/Harvard_JCHS_Housing_Americas_Older_Adults_2019.pdf).

229 FEDERAL BUREAU OF INVESTIGATION, *Elder Fraud Report 2021*, (2021), <https://www.justice.gov/file/1523276/download#:~:text=The%20number%20of%20elderly%20victims,over%20losses%20reported%20in%202020>.

230 Michal Gromek, *Digital Investment Fraud Wave Hits Seniors*, FORBES (Oct. 31, 2019), <https://www.forbes.com/sites/michalgromek/2019/10/31/digital-investment-fraud-wave-hits-seniors/?sh=3ace68102780>.

CFPB involved crypto-assets or crypto platforms in the last two years.<sup>231</sup>

### *Privacy and Surveillance Risks*

Despite generally purported benefits of increased privacy with crypto-asset transactions, as discussed above, it is possible to use data aggregation techniques to uncover users' wallet addresses and track every transaction related to that wallet. Ledger instruments like digital wallets record payments "on the books," and DLT systems increasingly rely on centralized intermediaries, meaning that many crypto-asset systems require an operator who sees that money's movement on the ledger.<sup>232</sup> As a result, ledger distribution modulates, but does not eliminate, the ability to track ledger money, undermining the claim that DLT can provide greater anonymity than traditional bank accounts or bearer instruments, such as physical cash and coins. The absence of anonymity may dissuade members of some communities who place a high value on privacy from engaging with crypto-asset products and services.

Crypto-asset companies also have the ability to collect a variety of their users' financial, technical, and personal data.<sup>233</sup> Such information may be shared with, or collected from, third-party companies, and these policies may not always be disclosed clearly to the consumer.<sup>234</sup> In addition, crypto-asset companies have the potential to use payments data and digital transactions to gather sensitive data about consumers' behavior, which may expose individuals to unwanted tracking and other privacy violations, worsening existing economic and social disparities. In addition, it has been reported that a digital crypto-asset platform has entered into a contract allowing a government agency to access data caches containing information, including geo-tracking to monitor transactions made through twelve different currencies including Ether, Tether, and Bitcoin.<sup>235</sup>

Americans in general are skeptical of commercial and government information collection.<sup>236</sup> Certain groups within the BIPOC community, in particular, both feel more vulnerable to having their private information exposed and are concerned about private or public entities having access to their information.<sup>237</sup> The lack of pseudonymity in crypto-asset markets and information sharing relationships between crypto-asset firms may thus have disparate impacts on individuals within these communities.

- 
- 231 From September 6, 2020 to September 6, 2022, there were 305 published complaints from servicemembers about crypto-assets. For the purposes of this and other CFPB complaint data, crypto-asset complaints refer to published complaints submitted to the CFPB in which servicemembers selected the sub-product "virtual currency" as the subject of the complaint. Published complaints do not represent total complaints submitted. See CFPB, *CFPB Complaint Database*, [https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&date\\_received\\_max=2022-09-06&date\\_received\\_min=2020-09-06&lens=Overview&product=Money%20transfer%2C%20virtual%20currency%2C%20or%20money%20service%E2%80%A2Virtual%20currency&searchField=all&tab=Trends&tags=Servicemember](https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&date_received_max=2022-09-06&date_received_min=2020-09-06&lens=Overview&product=Money%20transfer%2C%20virtual%20currency%2C%20or%20money%20service%E2%80%A2Virtual%20currency&searchField=all&tab=Trends&tags=Servicemember).
- 232 Angela Walch, *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, in *CRYPTO ASSETS: LEGAL AND MONETARY PERSPECTIVES*, OXFORD UNIVERSITY PRESS (Chris Brummer ed., 2019), <https://ssrn.com/abstract=3326244>.
- 233 See Anna Baydakova, *How Binance, Coinbase and 22 Other Crypto Exchanges Handle Your Data*, COINDESK (Jan. 27, 2022), <https://www.coindesk.com/layer2/privacyweek/2022/01/27/before-you-click-i-agree-how-binance-coinbase-and-22-other-crypto-exchanges-handle-your-data>.
- 234 *Id.*
- 235 See Gabriella Sotelo, *Coinbase Is Selling Data on Crypto and 'Geotracking' to ICE*, GIZMODO (Jun. 30, 2022), <https://gizmodo.com/coinbase-selling-crypto-data-geotracking-to-ice-1849130014>.
- 236 See PEW RESEARCH CENTER, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information>.
- 237 *Id.*

## VI. RECOMMENDATIONS

This report reviews the risks associated with primary use cases and prospective opportunities for crypto-assets. Consumers, investors, and businesses are vulnerable to an array of risks in the crypto-asset ecosystem.

Consistent with the objectives in the Executive Order to protect consumers, investors, and businesses as well as responsible development of payment innovations and digital assets, this report recommends a multi-pronged approach, described below. This approach builds on and complements other recommended actions as described in the President's Working Group on Financial Markets (PWG) Report on Stablecoins<sup>238</sup> as well as other reports pursuant to the Executive Order, including the report under Section 4 on the future of money and payments, and the report under Section 6, on financial stability risks and regulatory gaps.

Even as stakeholders continue to deliberate on legislative proposals on the subject of crypto-asset market regulation, there are much needed actions to be undertaken in the meantime using the existing authorities available to the regulators to protect the U.S. consumers, investors, and businesses. These actions are described below.

**Recommendation 1:** U.S. regulatory and law enforcement authorities should, as appropriate, pursue vigilant monitoring of the crypto-asset sector for unlawful activity, aggressively pursue investigations, and bring civil and criminal actions to enforce applicable laws with a particular focus on consumer, investor, and market protection.

As discussed earlier in Part IV, frauds, thefts, and scams have emerged as an especially grave area of concern in the crypto-asset space. These unlawful activities cause significant financial harm to U.S. consumers, investors, and businesses, amounting to over \$1.6 billion in total losses reported to the FBI in 2021 alone.

- *Expand and Increase Investigations and Enforcement:* Regulators and law enforcement should continue and consider expanding efforts to investigate, and, where appropriate, bring enforcement or other legal action against unlawful activity in crypto-asset markets. In particular, authorities should, where appropriate, increase investigation into misrepresentations made to consumers and investors in crypto-assets, including, for example, false or misleading advertising, terms of service, claims of returns or income potential, or statements of protections available to users of crypto-assets. Even though overall crypto-asset activity appears to have decreased in the recent months, regulators and law enforcement should remain vigilant in case unlawful conduct does not subside or new types of illegal activities develop in the market.

Crypto-asset use cases trigger obligations under federal consumer protection laws at least to the extent they are used for or in connection with offering or providing consumer deposits, stored value instruments, retail and other consumer payment mechanisms, the transmittal, exchange, or storage of consumer funds, or in consumer credit arrangements. Relevant obligations include, but are not limited to, the prohibition on unfair, deceptive, or abusive acts or practices. Other potential uses of crypto-assets—including but not limited to the marketing and sale of crypto-

---

238 See, e.g., PRESIDENT'S WORKING GROUP ON FINANCIAL MARKETS, THE FEDERAL DEPOSIT INSURANCE CORPORATION & THE OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 8.

assets as collectibles, or as features of gaming, entertainment, and other applications—are equally susceptible to various forms of unfair, fraudulent, misleading, or deceptive practices. As such, the CFPB and the FTC should continue to monitor and, as appropriate, expand efforts to conduct investigations of consumer complaints and use their authorities to enforce against and prevent unfair, deceptive, or abusive acts or practices in the industry. Similarly, to the extent that crypto-assets are marketed to retirement plans, the Department of Labor should conduct investigations to ensure proper fiduciary conduct, and to protect plans and plan participants from aggressive marketing, conflicts of interest, and imprudent and disloyal investments.

Moreover, to the extent that trading, lending, borrowing, or other activity in crypto-assets involves securities or derivatives transactions, then these activities must be conducted in compliance with federal securities laws and the Commodity Exchange Act, including applicable regulations. The SEC and CFTC have engaged actively in the enforcement of fraud and other violations of federal laws and regulations and have allocated additional resources to these efforts. These efforts, maintaining crypto-assets as an enforcement priority, and continued development of specialized personnel and resources are all important for investor protection.

- *Coordinate Cross-Agency Enforcement Actions:* Law enforcement officials and regulators should, as appropriate, continue to coordinate and combat fraud to deter unlawful behavior and improve practices in crypto-asset markets. For example, the Department of Justice has an established team in its Market Integrity and Major Frauds Unit that leads national efforts to combat fraud and market manipulation involving cryptocurrency, in coordination with the Federal Reserve Board, the SEC, the CFTC, and other agencies. Other coordinated or parallel actions, such as the Federal Reserve and FDIC’s cease and desist notices regarding false or misleading representations of deposit insurance status, and the CFPB’s release of guidance on the same topic, are impactful and should be used more frequently, as appropriate—especially where consumers are likely to be misled by such misrepresentations.
- *Share Information on Illegal Crypto-asset Activity:* Crypto-assets are continually evolving, as is the illegal activity that uses crypto-assets. To ensure broad and consistent enforcement and to supplement private sector analytics tools, regulators and law enforcement officials should, as appropriate, share information regarding the type and scale of fraudulent, misleading, or manipulative market practices they are observing and investigating. For example, sharing data could help identify relevant clusters of unlawful activity and spot trends in scams and fraud types.

**Recommendation 2:** U.S. regulatory agencies should use their existing authorities to issue supervisory guidance and rules, as needed, to address current and emerging risks in crypto-asset products and services for consumers, investors, and businesses. Agencies should work collaboratively to promote consistent and comprehensive oversight.

The U.S. agencies should, as appropriate, review existing regulations and take steps to clarify regulatory requirements applicable to crypto-asset products and services, address novel fraudulent practices, and enhance disclosure requirements. These reviews should conclude with issuing clarifications, as appropriate, such as the recently released FDIC fact sheet on the scope of deposit insurance coverage that indicates that by federal law, the FDIC only insures deposits held in insured

banks and savings associations and only in the unlikely event of an insured bank's failure. Where appropriate, agencies should also clarify that some crypto-asset products and services are regulated—despite assertions to the contrary by firms promoting these products and services—to help address gaps in disclosures.

Crypto-asset products and services are new and rapidly developing, which can invoke jurisdictions and interests of multiple federal and state regulatory and law enforcement authorities in potentially novel ways. Further, crypto-assets and related intermediaries are subject to unique and evolving operational risks, including cyber risks. As such, active collaboration and coordination is necessary to ensure that crypto-asset products and services are subject to, and in compliance with, appropriate supervision, oversight, regulation, collection, and disclosure requirements.

- *Provide Guidance through Individual Actions:* U.S. authorities have already taken useful steps to provide clarity in the crypto-asset space through individual agency actions such as supervisory guidance or rulemakings. Examples of such actions include the OCC's interpretive letters that clarify expectations of its regulated entities in regards to safeguarding digital assets for customers, holding deposits that serve as reserves backing a stablecoin, and using distributed ledger technology to facilitate payments; the FDIC's cease and desist actions for false or misleading representations about deposit insurance; and the SEC's special purpose broker-dealer statement on digital asset custody that identifies the circumstances in which the SEC will not take certain enforcement action against broker-dealers with respect to digital asset securities. As appropriate, regulators should pursue supervisory guidance or rulemaking to ensure that all crypto-asset intermediaries properly account for novel operational risks, cyber risks, and consumer protection.
- *Collaborate to Improve Clarity:* Collaborative cross-agency initiatives such as crypto-asset "policy sprints" undertaken by the U.S. federal prudential banking agencies provide meaningful benefits for consumers, investors, and businesses. The "policy sprints" resulted in productive engagements around common vocabulary, the identification and assessment of key risks, and the roadmap that identified areas of future focus. Interagency bodies such as the PWG's Financial and Banking Information Infrastructure Committee (FBIIC) may also provide forums through which more targeted coordination and supervision of cyber and other operational risks can be developed. Such interagency coordination and parallel actions should continue, and, where appropriate, be further strengthened through the formation of new working groups to address emerging issues in crypto-asset markets and formal agreements to coordinate enforcement actions and share data.
- *Provide Plain Language Guidance:* Given significant interest of individual consumers, investors, and populations vulnerable to disparate impacts in crypto-assets, and the many non-traditional forms of projects and firms involved in crypto-asset activities, regulatory agencies should, as much as possible, issue guidance, interpretations, and rulemaking related to crypto-assets in plain language. Plain language guidance is that which is readily understandable by an audience of laypersons, technologists, and non-professional parties with interests in the topic. One example of plain language guidance is the Department of Labor's compliance assistance issued in March 2022, which presented that agency's "serious concerns" with cryptocurrencies as investments in defined contribution plans, such as 401(k) plans, in plain language easily understandable by plan fiduciaries, employers, and plan participants. Candid descriptions of the potential risks associated

with new categories of investments are an essential part of improving practices of plan fiduciaries when acting on behalf of plan participants in managing retirement holdings.

**Recommendation 3:** U.S. authorities should, where appropriate, work individually and through the Financial Literacy and Education Commission (FLEC) to ensure that U.S. consumers, investors, and businesses have access to trustworthy information on crypto-assets.

Users of crypto-asset platforms have significant exposure to risks, including risks of default and outright theft. Further, users often may not be fully aware of these risks, given crypto-asset market participants' frequent emphasis on trading profits with minimal reference to losses, as well as the general lack of comprehensive disclosure. For these reasons, the FLEC should, as appropriate, coordinate and promote consumer education efforts on crypto-assets. These efforts should ensure that consumer-friendly, trustworthy, and consistent education materials are accessible and inclusive, to the maximum extent possible. Such materials should:

- (i) Highlight risks associated with investors' or consumers' use of crypto-assets, including heightened risks of frauds, thefts, and scams;
- (ii) Identify and warn against common practices employed by perpetrators of frauds, thefts, and scams;
- (iii) Provide information on how to report unlawful practices and submit consumer and investor complaints; and
- (iv) Provide information on operational risks that are unique to the crypto-asset ecosystem and how they may impact investment value.

Considering the lack of data and information on use of crypto-assets by populations vulnerable to disparate impacts, FLEC member agencies should also consider exploring using existing surveys to collect new or additional data, as appropriate.

Finally, the FLEC should, where appropriate, engage with industry leaders, academics, and other relevant parties to promote and coordinate public and private strategies for financial education outreach to consumers.

