

A COMPREHENSIVE APPROACH TO CRYPTO REGULATION

Brett Hemenway Falk* & Sarah Hammer**

INTRODUCTION	416
I. A UNIQUE CHALLENGE IN REGULATING CRYPTO	418
A. How Crypto Works.....	418
B. Features of Smart Contracts and Cryptocurrency.....	420
C. Challenges for Policymakers.....	421
C. Example of Standards in Financial Regulation	422
D. Examples of Standards in the Digital World.....	423
II. APPLYING STANDARDS TO STABLECOIN RESERVES.....	424
A. Benefits of Standards.....	426
B. Limitations of Standards.....	427
C. Standards as One Pillar of the Policy Approach.....	427
III. CONTINUED CHALLENGES FOR REGULATION	428
A. What is a Stablecoin	429

Nothing in this Article endorses or is intended to endorse any particular blockchain, cryptocurrency, asset, practice, approach, or company, public or private. Furthermore, nothing in this Article is intended to provide nor does provide legal, tax, financial, investment, or any other form of advice. The information and data provided in this Article is as of the date of writing, and may have changed by the time of publication.

* Brett Hemenway Falk is Research Assistant Professor in the Department of Computer and Information Science at the University of Pennsylvania School of Engineering and Applied Science. Professor Falk’s team seeks to use tools from math and computer science to address large-scale societal goals. Professor Falk has worked extensively designing and implementing protocols for secure computation that effectively allow a collection of stakeholders to collaborate securely, without sharing sensitive data and without the need for a centralized trusted authority. He holds a B.Sc. in Mathematics from Brown University and a Ph.D. in Mathematics from the University of California, Los Angeles.

** Sarah Hammer, Esq., is Managing Director of the Stevens Center for Innovation in Finance at the Wharton School and Adjunct Professor of Law at the University of Pennsylvania Law School. She previously served as Acting Deputy Assistant Secretary for Financial Institutions at the U.S. Department of the Treasury, and prior to that, held various leadership positions throughout financial services in general management, portfolio management, trading, marketing, research, and analytics at the Vanguard Group, PIMCO, JP Morgan Chase, BlackRock, and Tudor Investments. She holds a J.D. from the University of Pennsylvania Law School, an M.B.A. from the Wharton School, and a Master of Studies from Oxford University. She is a Harry S. Truman Scholar and a member of the American Law Institute.

B. The Terra Luna Collapse of 2022.....	432
C. Freezing, Clawbacks, Blacklisting, Wrapping	433
D. Bankruptcy and Insolvency	436
E. Limited Terms of Service	438
IV. NATIONAL INVESTOR AND CONSUMER PROTECTION FRAMEWORK	439
A. Regulatory Gaps and Challenges.....	443
B. Investor and Consumer Protection Considerations.....	445
V. GLOBAL STANDARD SETTING.....	447
CONCLUSION	448

INTRODUCTION

Regulation of cryptocurrency is a key policymaking issue of our time. There are many challenges associated with developing and applying legal frameworks to cryptocurrency, as the technology, business practices, and uses of cryptocurrency vary significantly from traditional financial services. Moreover, the ecosystem exhibits a rapid speed of innovation and very high level of complexity. Nevertheless, regulating cryptocurrency, particularly as it relates to users, is essential to achieve sufficient investor and consumer protection, as well as to provide the clarity that innovators need to build their businesses.¹

One unique challenge in policymaking related to cryptocurrency is the potential lack of a central entity or traditional intermediary that would be the subject of regulatory authority. In the crypto space, activities are often originated by individual developers, decentralized organizations, or even algorithms—a set of instructions left in place by programmers. A key example of this dynamic is stablecoins, where the cryptocurrency is pegged to a reference asset considered to be stable (such as the U.S. dollar). With stablecoins, certain provisions such as reserves, lockups, clawbacks, blacklisting, fees, and wrapping have given rise to considerations about their behavior and user accessibility. Examination of the relevant limited terms of service/use, auditors' reports, and business models have implications for credit, liquidity, and operations, as well as consumer protection and financial stability.

1. The authors would like to note that, given the meteoric speed of change in crypto, market conditions, activities, institutions, and dynamics will likely have changed by the time this paper is published. Nevertheless, we lay out what we believe to be important long-term principles for policymaking in the space.

Because there may not be a central entity or traditional intermediary to regulate for many stablecoins, we propose a first pillar of cryptocurrency regulation: establishing new “Crypto Standards” that could be applied to the smart contracts of not only stablecoins, but across the burgeoning web3 landscape. Crypto Standards offer potential benefits, including progress towards public policy goals of consumer protection and financial stability, as well as tools to promote interoperability, security, and responsible technological innovation.

However, numerous other practices give rise to concern about activities in cryptocurrency. The Terra Luna meltdown of 2022 highlighted serious concerns about potentially unfair, deceptive, and fraudulent business practices in the cryptocurrency space. In addition, within reserve-backed stablecoins, consumer protection questions arise over certain practices by issuers. For example, many stablecoins maintain the ability to prevent redemption of tokens for fiat money, retrieve tokens without consent (“clawbacks”), or even unilaterally block certain digital wallet addresses from transacting (“freezing”). Most or all stablecoins set forth no formal procedure for how these decisions are made, leading to concerns that they are non-transparent or even arbitrary.

In addition, stablecoins frequently change their online disclosures (if any) and limited terms of service without providing notice to stablecoin users. The use of limited terms of service combined with extreme practices in the stablecoin space raises significant questions regarding stablecoin behavior and user accessibility, as well as the validity and enforcement of contracts of adhesion and consumer protection. Additionally, these activities have implications for credit, liquidity, and operations, as well as financial stability.

While Crypto Standards offer potential benefits, including progress towards public policy goals of consumer protection and financial stability, as well as tools to promote interoperability, security, and responsible technological innovation, standards alone are not sufficient to address all of the practices discussed in this paper. We therefore propose a second pillar of cryptocurrency regulation: an additional national overlay of very strong investor and/or consumer protections, as absolutely necessary to address activities in this space. This national overlay should encompass five consumer protection themes that we discuss in this paper, and regulatory consistency and cooperation should be achieved through a federal interagency rule-making process.

The third pillar of this comprehensive approach is international standard-setting. International standard-setting is essential to achieving cooperation and collaboration between jurisdictions and consumer

protections mentioned herein. While standard-setting can be a long and arduous process, it is imperative to achieving long-term efficacy in cryptocurrency regulation. All together, these three pillars (Crypto Standards, national consumer protection regulation, and international standard-setting) can provide a comprehensive approach to investor and consumer protection in cryptocurrency.

I. A UNIQUE CHALLENGE IN REGULATING CRYPTO

A unique challenge in policymaking related to cryptocurrency is the potential lack of central entity or traditional intermediary that would be the subject of regulatory authority. In the crypto space, activities are often originated by individual developers, decentralized organizations, or even algorithms—a set of instructions left in place by programmers. A key example of this dynamic is stablecoins, where the cryptocurrency is pegged to a reference asset considered to be stable (such as the U.S. dollar). With stablecoins, certain provisions such as reserves, lockups, clawbacks, blacklisting, fees, and wrapping have given rise to considerations about their behavior and user accessibility. Examination of the relevant limited terms of service/use, auditors' reports, and business models have implications for credit, liquidity, and operations, as well as consumer protection and financial stability.

Because there may not be a central entity or traditional intermediary to regulate for many stablecoins, we propose establishing new “Crypto Standards” that could be applied to the smart contracts of not only stablecoins, but across the burgeoning web3 landscape. Crypto Standards offer potential benefits, including progress towards public policy goals of consumer protection and financial stability, as well as tools to promote interoperability, security, and responsible technological innovation.

A. How Crypto Works

Blockchain is a shared, immutable ledger that facilitates the recording of transactions in a network. Individual users can submit requests (“transactions”) to update the state of the ledger, and those transactions are processed by “validators.” The assets tracked on a blockchain can be tangible assets, such as cash, gold, or real estate; intangible assets, such as intellectual property, copyrights, or licenses; or cryptocurrencies, such as Bitcoin. Blockchain arose with the invention of Bitcoin in 2009, a digital currency launched by a person or persons known by the pseudonym Satoshi

Nakamoto.² Bitcoin was created to eliminate the need for a central monetary authority to monitor, verify and approve transactions, by enabling a peer-to-peer network in which transactions are “mined” by individuals using software to solve mathematical puzzles. The Bitcoin blockchain was created to track the ownership of bitcoins, but many of the subsequently developed blockchains are designed to record any transaction or track the movement of any asset, not just bitcoins.³ Today, thousands of cryptocurrencies are powered by blockchain technology. In addition, blockchain technology is used across a variety of industries, from health care, to education, to supply chain management in logistics.

“Smart contracts” are a critical component of cryptocurrencies and decentralized applications being built on blockchain. Smart contracts are computer code that is stored on the blockchain itself and can automatically update the blockchain ledger. The code of a smart contract can either be the sole manifestation of an agreement between parties or a complement to a traditional text-based contract. The code is replicated across multiple nodes of a blockchain and, therefore, it potentially benefits from the attributes of security, permanence, and immutability that may be offered by blockchain. Despite the name “contract,” smart contracts are simply computer programs, and as such are written in programming languages suited for computer programming, rather than legal contracts.⁴ Smart contracts are not self-executing, instead they can only respond to the actions of users (or other contracts). Because most major blockchains are open to the public, sophisticated users can predict the behavior of a contract in response to a user’s action. This predictability is what gives smart contracts their potential power. In one sense, they may be viewed as an intermediary between otherwise distrustful actors.

Creating a new cryptocurrency involves coding a smart contract that defines the rules for creating (“minting”), destroying (“burning”), and transferring the tokens (updating token balances recorded within the contract), as well as tracking ownership of the tokens. On a blockchain like Ethereum, separate smart contracts control almost all of the different

2. See SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008), <https://bitcoin.org/bitcoin.pdf> [<https://perma.cc/3BVB-KTSH>] (explaining how a theoretical decentralized currency would operate).

3. See generally Sarah Hammer, The Blockchain Ecosystem (Nov. 8, 2018) (unpublished manuscript), <https://dx.doi.org/10.2139/ssrn.3281020>.

4. See Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 26, 2018), <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> [<https://perma.cc/265L-RVPE>] (explaining how smart contracts function).

cryptocurrencies (or “tokens”). To date, over half a million token contracts have been deployed on Ethereum.⁵ Each of these token contracts can be thought of as a database tracking how many tokens are owned by each crypto wallet address. When a user wishes to transfer a token, the user makes a request of the smart contract, and the smart contract updates its database. Exactly how, or even whether, the contract updates its internal database is governed exclusively by the code of the smart contract. In essence, smart contracts themselves offer a focal point for policymaking in the cryptocurrency space.

B. Features of Smart Contracts and Cryptocurrency

One key point about smart contracts is that they may contain features that create complexity for the user. For example, some tokens are “deflationary,” meaning that whenever a transfer is initiated, a portion of the transferred funds are destroyed (“burned”). Some tokens are also “pausable,” meaning that an administrator can shut down all transfer activity. These functionalities can be set so that transfers from certain wallet addresses incur a fee, but transfers from other wallet addresses do not. Some tokens are also “ownable,” meaning that administrators are given special rights such as the ability to mint new tokens or adjust transfer fees. Other common features included in token contracts are “clawbacks,” “freezing,” and “wrapping,” which will be explained later in this Article. Another important feature is the immutability of the smart contract, meaning once it has been deployed to the blockchain, the code cannot be changed.

The computer code that defines cryptocurrency behavior can be extremely complex, and, without examining the smart contract, it can be difficult to know exactly how a token will behave. The challenge can be even greater when the token is intended to confer ownership of a physical asset such as gold or a fiat currency. For example, many stablecoins are pegged to a reference asset such as the U.S. dollar, and in turn the stablecoin issuer states that the tokens can be redeemed for such dollars. However, the smart contract itself cannot ensure that the issuer has enough dollar reserves to redeem the outstanding tokens, or that the token issuer will honor redemption requests. In fact, for all major fiat-backed stablecoins,⁶ the contract code on the blockchain (“on-chain”) makes no reference to assets off the blockchain (“off-chain”) or the possibility of redemption. Any claims about the

5. *Token Tracker*, ETHERSCAN, <https://etherscan.io/tokens> [<https://perma.cc/5QCS-PN> AK] (last visited Nov. 15, 2022).

6. Major fiat-backed stablecoins include USDT, USDC, BUSD, USDP, etc.

redeemability of fiat-backed stablecoins are typically made on the issuer's website vis-à-vis terms of service. The terms of service pertinent to the particular token are often posted online, changed frequently, and may contain provisions that are highly unfavorable to the user.

C. Challenges for Policymakers

A key challenge for policymakers is that some cryptocurrencies do not involve a central entity that could be subject to the regulation and supervision of a federal agency. Rather, they are governed by Decentralized Autonomous Organizations (DAOs). For example, the stablecoin Dai (DAI) is issued by MakerDAO, a decentralized "community" that governs the smart contracts that power Dai.⁷ The fact that DAI is governed by a DAO is key to understanding its dynamics. Although DAI is pegged to U.S. dollars, it is not actually backed by a fiat currency. Instead, it is backed by other cryptocurrencies. At the time of this writing, DAI is backed by a basket of cryptocurrencies that includes WETH, WBTC, and USDC. Because DAI is governed by a DAO, holders of its governance token can vote to change the composition of the collateral at any time. Moreover, because DAI's collateral consists of other cryptocurrencies rather than US dollars, there is also no traditional custodian that could be subject to federal or state regulation.⁸

Another key challenge for policymakers in the crypto space is that it can be difficult to detect market manipulation. Transactions occur on a blockchain, and, while each transaction is recorded and available to see, that visibility extends only down to an alphanumeric identifier, known as an "address." Although the blockchain records and displays the address that sent or received assets, it does not record the identity of the person who controls those assets. This is known as "pseudonymity."

Although the blockchain itself is decentralized, individual tokens are controlled exclusively by their smart contracts. In the case of stablecoins backed by cryptocurrencies, while no physical custodian is involved, the smart contract itself has some functions similar to a custodian. In addition, where stablecoin collateral differs from the peg (as in the case of DAI), a "price oracle" is required to determine the price of the pegged asset relative to the collateral. A price oracle is essentially a data feed that transfers real-world information onto a blockchain so that it can be read by a smart contract. The price oracle potentially offers yet another point of

7. A separate governance token, MKR, allows users to vote on governance proposals, e.g., changing reserve rates.

8. The reserve currencies are custodied on the blockchain by a smart contract.

centralization. Initially, Maker DAO used the median price of fourteen anonymous price oracles to post the ETH/USD price to the blockchain. The system has since evolved to allow new price oracles to be added.⁹

C. Example of Standards in Financial Regulation

In financial regulation, standards are commonly used to achieve goals of fair, safe, liquid, and efficient financial markets while protecting consumers and financial stability. Sometimes, these standard setting bodies are even given regulatory mandates. One example is the Financial Industry Regulatory Authority (FINRA), a nongovernmental organization that writes and enforces rules for brokers and dealers and examines them for compliance. FINRA administers qualifying exams that securities professionals must pass to sell securities or supervise others who do so. FINRA was formed by a consolidation of member regulation, enforcement, and operations of the New York Stock Exchange, as well as the National Association of Securities Dealers. FINRA is authorized by Congress to oversee more than 624,000 brokers and is overseen by the Securities Exchange Commission.¹⁰

The Municipal Securities Rulemaking Board (MSRB) is another self-regulatory organization, established by section 15B of the Securities Exchange Act of 1934.¹¹ It establishes rules for municipal advisors and dealers in the municipal securities market, conducts required exams and continuing education for municipal market professionals, and provides guidance to the SEC and others for compliance with and enforcement of MSRB rules. The MSRB is authorized by Congress to regulate the activities of broker-dealers and banks that buy, sell, and underwrite municipal securities. Like FINRA, the MSRB is registered with the Securities Exchange Commission (SEC). The SEC and federal bank regulators share responsibility for enforcement and compliance examinations.¹²

In the international context, standards become even more important. As activities move globally, commonly accepted standards are essential to

9. See Wanyun Catherine Gu, Anika Raghuvanshi & Dan Boneh, *Empirical Measurements on Pricing Oracles and Decentralized Governance for Stablecoins*, CRYPTOECONOMIC SYS., Oct. 21, 2021 (describing the “practical operation of a pricing oracle and a decentralized governance mechanism in a large deployed system”).

10. See FINRA, <https://www.finra.org> [<https://perma.cc/9EA7-C7MT>] (detailing FINRA’s duties and goals) (last visited Nov. 15, 2022).

11. 15 U.S.C. § 78o-4(b).

12. See MUNICIPAL SEC. RULEMAKING BD., *THE ROLE AND JURISDICTION OF THE MSRB*, (2021), <https://www.msrb.org/msrb1/pdfs/Role-and-Jurisdiction-of-MSRB.pdf> [<https://perma.cc/F7K9-G7N9>] (detailing the history and purpose of the board).

achieving public policy goals of consumer protection, financial stability, interoperability, security, and responsible technological innovation. Moreover, the global landscape continues to undergo rapid transformation, with changes in business and political climates, competition, the development of economies, and rapid technological advancement. International standard setting is also important for individual companies wishing to operate in different jurisdictions and needing to comply with the requirements of each jurisdiction.

International standard-setting involves a deliberate process of collaborative discussion, negotiation, and individual countries moving towards high quality global frameworks. A key example of this is the Basel Accords, issued by the Basel Committee on Banking Supervision (BCBS). The BCBS maintains a secretariat at the Bank for International Settlements in Basel, Switzerland, and the committee of representatives from central banks and regulatory authorities of the Group of Ten plus G-20 major economies meet there. The BCBS has issued Basel Accords I, II, and III, which are recommendations for financial regulations across the global banking industry.¹³

D. Examples of Standards in the Digital World

Standards are also well known in the world of computer science—they are essentially the core of the internet. The Hypertext Transfer Protocol (HTTP) standard allows a web browser such as Chrome or Safari to communicate with a server that is running on a completely different machine using different hardware and software.¹⁴ The Hypertext Markup Language (HTML) standard ensures that the data received from a web server is displayed consistently regardless of which browser or operating system is being used.¹⁵ The Simple Mail Transfer Protocol (SMTP) standard makes it possible to send an email using one system, such as Gmail, that can later be retrieved by someone using a different email system, such as Microsoft Outlook.¹⁶

13. *The Basel Committee – Overview*, BANK FOR INT’L SETTLEMENTS, <https://www.bis.org/bcbs/> [<https://perma.cc/G2LE-S3PV>] (last visited Nov. 15, 2022).

14. See *Brief History of HTTP*, HIGH PERFORMANCE BROWSER NETWORKING, <https://hpbn.co/brief-history-of-http/> [<https://perma.cc/BAC8-UN5S>] (last visited Nov. 15, 2022) (detailing the history, purpose, and evolution of the protocol).

15. See *History of the Web*, WORLD WIDE WEB FOUND., <https://webfoundation.org/about/vision/history-of-the-web/> [<https://perma.cc/Y4JD-M974>] (last visited Jan. 22, 2022) (discussing the HTML standard).

16. Bettina Specht, *Everything You Need to Know About SMTP (Simple Mail Transfer*

In the newer blockchain space, similar standards have begun to emerge. The most relevant are smart contract standards that outline the minimum functionality of a smart contract. In the Ethereum blockchain network, for example, new standards can be proposed by anyone in the blockchain community, and proposed standards are selected and finalized by community members. Two of the most important standards here are the ERC-20¹⁷ and ERC-721¹⁸ standards. The ERC-20 token standard outlines how smart contracts that implement fungible tokens on Ethereum should behave; the ERC-721 token standard outlines how non-fungible tokens (NFTs) should behave.

The ERC-20 and ERC-721 standards have become dominant standards in the Ethereum ecosystem. To be successful, the ERC-20 and ERC-721 standards had to define a minimum functionality that a smart contract had to adhere to, without being overly prescriptive. Thus, developers are given a wide latitude on how to implement the particular functionality of the smart contract while still remaining compliant with the standard. To increase adoption of standards and reduce duplication of efforts, some organizations provide tools to create and automate blockchain applications that can be freely copied, modified, and deployed.¹⁹

II. APPLYING STANDARDS TO STABLECOIN RESERVES

To demonstrate the potential benefits of standards, we outline an example standard for reporting reserves for asset-backed stablecoins such as USDT or USDC. For context, the price stability of an asset-backed stablecoin is tied to the quality and quantity of the issuer's reserves. Currently, however, stablecoin reserve reporting is largely inconsistent and contains little to no detail on composition of the reserves. This lack of reporting impedes thorough analysis of the risks posed by these reserve assets.

Protocol), POSTMARK (Sept. 13, 2022), <https://postmarkapp.com/guides/everything-you-need-to-know-about-smtp> [https://perma.cc/57C4-PTT8].

17. *ERC-20 Token Standard*, ETHEREUM (Aug. 15, 2022), <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/> [https://perma.cc/95AN-9454].

18. *ERC-721 Non-Fungible Token Standard*, ETHEREUM (Aug. 15, 2022), <https://ethereum.org/en/developers/docs/standards/tokens/erc-721/> [https://perma.cc/U987-96EW].

19. *Contracts*, OPENZEPPELIN: DOCS, <https://docs.openzeppelin.com/contracts/4.x/> [https://perma.cc/B9TZ-ASU2] (last visited Jan. 22, 2023).

Potential for On-Chain Reserve Reporting for Major Stablecoins			
	USDT	USDC	DAI
Market Cap	\$66.49 Billion	\$54.19 Billion	\$7.52 Billion
Reports On-Chain	No	No	Yes
Frequency of Reports	Quarterly	Monthly	24/7
Report Type	Attestation discloses assets, liabilities, capital position, and a breakdown of reserves	Attestation discloses number of coins in circulation, value of reserves, and breakdown of reserves	Attestation discloses number of coins in circulation, value of reserves, exact breakdown of reserves, debt ceiling, and collateralization ratio
Ability to Report On-Chain	Possible. Since Tether cannot completely alter the contract, they would have to deploy a new contract, which would have a new contract address	Easy. The USDC contract can be replaced at will	DAI is already fully on-chain, so it wouldn't need any changes at all.
Applicable Regulator	Unknown	Licensed as a money transmitter in 47 states	Unknown
Note one significant policy recommendation from the Stevens Center for Innovation in Finance at the Wharton School: Reserve reporting for fiat-backed stablecoins should take place on chain, at least on a daily basis. Requirements for daily (or even more frequent) reporting on chain are highly feasible and may enable more effective supervision and enforcement.			

Figure 1. Potential for on-chain reserve reporting for major stablecoins²⁰

Implementing a standard for stablecoin reserve reporting on blockchain (on-chain) could dramatically increase transparency in this asset class and would provide more information to stablecoin users, allowing them to make more informed decisions. A standard for reserve reporting could require that smart contracts would have methods to retrieve and store information about stablecoin reserve composition and categorization, as well as an attestation from their individual auditing firm.

Requiring on-chain reporting of stablecoin reserves could offer several potential benefits:

1. The data could be easily discoverable. Currently, the smart contracts that control stablecoins do not contain any reference to the issuer's name or website, where the limited terms of service are held. With this standard, the data would be associated directly with the on-chain token and would be easily discoverable by anyone

20. This chart was compiled based on available data from CoinMarketCap in October 2022 and from the website information of the stablecoin issuers, their terms of service, and based on evaluation of their smart contracts. See COINMARKETCAP, <https://coinmarketcap.com/>. This chart was created by the Blockchain Laboratory Team at the Wharton School. Joseph Jasperse, Potential for On-Chain Reserve Reporting for Major Stablecoins. Draft for discussion. Not intended as legal advice. Updated as of August 9, 2022.

- who interacts with the contract.
2. The data could be easier to analyze. Currently, data analysis requires manually identifying the location of certain reports, manually extracting reserve information from those reports, and attempting to understand and reconcile the reserve categories. If reserve data were stored on-chain, it could be easy to create analytics tools that continually monitor and compare the quality of reserves of different stablecoins.
 3. The data could be permanently stored. Currently, stablecoin issuers post data reports on their websites that can be deleted or modified at will. If reserve data were reported on-chain, the complete history of all reserve reports could be available for inspection and the complete history would be preserved on blockchain.

Stablecoin reserve-reporting is just one example of how standards could be used to improve transparency and accountability for on-chain assets. Crypto Standards could also include several other features, e.g., limited terms of service embedded into the contract, or standardized methods for handling the freezing or repossession of tokens.

A. Benefits of Standards

Standards are a simple way to meet public policy goals of consumer protection, financial stability, interoperability, security, and responsible technological innovation. Setting standards may require significant industry collaboration. In this respect, non-profit working groups like the Internet Engineering Task Force (IETF), which maintains the HTTP standard, or the Worldwide Web Consortium (W3C), which maintains the HTML standard, could be useful for developing and maintaining standards that are up-to-date and trusted by the community.

Upgrading existing contracts to comply with new standards will incur some costs. However, standards can also reduce future costs by allowing multiple organizations to reuse (standardized) computer code. Currently, some organizations develop secure “reference implementations” for token contracts for all the major token standards like ERC-20 and ERC-721. These reference implementations are widely used by the blockchain community. If a standard-setting body were to develop reference implementations for new stablecoin standards, this could significantly reduce development costs because issuers could reuse the standard code rather than developing their own custom implementations.

Finally, standards can be made global, similar to the Unicode character encoding standards, which support the exchange of written text, or, as

discussed earlier, the Basel Accords.²¹ Setting standards globally, in a collaborative and transparent process, is necessary because crypto is global. As crypto crosses borders, jurisdictions may likewise choose to establish standard-setting that addresses their activities. Moreover, making standards global has the potential to further improve interoperability and international transactions, such as payments, settlement, and trades.

B. Limitations of Standards

Of course, there are certainly limitations to the use of standards. First and foremost, they are voluntary. For standards to have the greatest impact, there should be industry input into developing and formalizing them so that the industry itself has a vested interest in compliance. Otherwise, key parties will not adhere to the standards. In addition, standards do not have the force of law. Therefore, those developing these standards should consider the potential repercussions of parties not adhering to standards, and whether or not a regulatory mandate would be helpful (as in the case of FINRA).

Moreover, standards cannot verify the content of the data put on-chain. Issues around accuracy or even fraud in data reporting will still exist. Simply put, standards cannot make people tell the truth. Notably, however, requiring reserve reporting on-chain would mitigate some of these negative effects, as any fraudulent reports could be permanently stored on the blockchain and could not be hidden or removed. Finally, standards cannot control off-chain activities, and therefore other compliance- and enforcement-related activity would have to be handled by a different mechanism.

C. Standards as One Pillar of the Policy Approach

As noted, a continued challenge in policymaking related to cryptocurrency is the potential lack of a central entity or a traditional intermediary that would be the subject of regulatory authority. In the crypto space, activities are often originated by individual developers, decentralized organizations, or even algorithms—a set of instructions left in place by programmers. With stablecoins, certain provisions such as reserves, lockups, clawbacks, fees, and wrapping have given rise to considerations about their behaviors and user accessibility. Examination of the relevant limited terms of service/use, auditors' reports, and business models have implications for credit, liquidity, and operations, as well as consumer protection and financial

21. *About the Unicode Standard*, UNICODE: THE UNICODE STANDARD, <https://unicode.org/standard/standard.html/> [<https://perma.cc/M2XP-CH2F>] (last updated June 22, 2016).

stability.

Because there may not be a central entity or a traditional intermediary to regulate for many stablecoins, we propose the establishment of new “Crypto Standards” that could be applied to the smart contracts of not only stablecoins, but across the burgeoning web3 landscape. In financial regulation, standards such as the Basel Accords are commonly used to achieve regulatory objectives while protecting consumers and financial stability. Standards are also well known in the world of computer science and form the core of the internet, including the Hypertext Transfer Protocol (HTTP) and the Hypertext Markup Language (HTML). Crypto Standards offer many potential benefits, including progress towards public policy goals of consumer protection and financial stability, as well as tools to promote interoperability, security, and responsible technological innovation.

III. CONTINUED CHALLENGES FOR REGULATION

Our recommendation for Crypto Standards is not meant to suggest that they are a panacea to address all activities in the crypto space. Very strong additional regulation is required. In May of 2022, a stablecoin ecosystem known as Terra Luna collapsed. The value of Terra’s native asset, Luna, dropped to zero, and its stablecoin, TerraUSD (UST), de-pegged. A vast number of other cryptocurrencies and market participants were intertwined in the disaster, providing but one example of the chaos and deep losses that can be incurred when an algorithmic stablecoin does not maintain its peg. Moreover, the Terra Luna meltdown highlighted serious concerns about potentially unfair, deceptive, and fraudulent business practices in the cryptocurrency space.

Numerous additional practices within stablecoins give rise to serious concerns over consumer protection. Within reserve-backed stablecoins, questions arise over certain practices by issuers. For example, many stablecoins maintain the ability to prevent redemption of tokens for fiat money, retrieve tokens without consent (“clawbacks”), or even unilaterally block certain digital wallet addresses from transacting (“freezing”). Most or all stablecoins set forth no formal procedure for how these decisions are made, leading to concerns that they are non-transparent or even arbitrary.

In addition, stablecoins frequently change their online disclosures (if any) and limited terms of service without providing notice to stablecoin users. The use of limited terms of service combined with extreme practices in the stablecoin space raises significant questions regarding stablecoin behavior and user accessibility, as well as the validity and enforcement of contracts of adhesion and consumer protection. Additionally, these activities

have implications for credit, liquidity, and operations, as well as financial stability.

In addition to the Crypto Standards recommended in this paper, an additional overlay of very strong investor and/or consumer protections is absolutely necessary to address activities in this space, in order to create a comprehensive approach to regulation of cryptocurrency and stablecoins. Combined with participation in international standard-setting processes and adherence to agreed-upon standards, these three pillars (Crypto Standards, national consumer protection regulation, and international standard-setting) can provide a comprehensive approach to investor and consumer protection in digital assets.²²

To address the need for a very strong consumer protection overlay in crypto regulation, the authors evaluated existing regulatory statements, reports, principles, and rules related to consumer protection across four major geographic regions and the four largest international standard-setting bodies.²³ We also unpacked consumer protections set forth in recent U.S. legislative proposals related to crypto.²⁴ Based on our assessment, we propose five important, high-level consumer protection themes to be included in clear national crypto regulation.

A. What is a Stablecoin

In order to fully unpack the crypto crash of spring 2022 and the urgent need for very strong consumer protections, we will explain stablecoins in further detail. Stablecoins are digital assets that are intended to maintain a stable value relative to a currency or other reference asset. Stablecoins may be used to facilitate trading, clearing, settlement, lending, or borrowing. Proponents of stablecoins believe they could be used effectively as a means of payment for both individuals and businesses. Stablecoins are sometimes purported to potentially support faster, more efficient global payment systems.

22. If appropriate, collaboration with states may also be additive to the process.

23. The authors evaluated existing crypto policymaking in the four major geographic regions that have set forth significant thought leadership or rulemaking on crypto. These four geographic regions include the European Union (EU); the United Kingdom (UK); the Middle East and North Africa (MENA), specifically, the Dubai Financial Services Authority (DFSA); and the Asia-Pacific (APAC) region, specifically, the Monetary Authority of Singapore (MAS).

24. The authors evaluated two significant and recent legislative proposals from the U.S. Senate, the Lummis-Gillibrand Responsible Financial Innovation Act, S. 4356, 117th Cong. (2022), and Senator Boozman, Stabenow, Booker, and Thune's Digital Commodities Consumer Protection Act of 2022, S. 4760, 117th Cong. (2022).

Table 1. Differences in Fiat Backed, Commodity Backed, Crypto Backed, and Algorithmic Coins²⁵

	Reserve Backing	Maintenance of Peg	Price Stability
Fiat Backed	Fully backed by fiat currency and fiat currency-equivalents such as cash and cash-equivalents.	When \$1 is invested, \$1 worth of the stablecoin is received and \$1 is added to the reserve. When \$1 is redeemed, \$1 worth of the stablecoin is burned.	Generally higher
Commodity Backed	Backed by commodities such as precious metals or real estate.	Each token is backed by a certain amount of the commodity. For example, Paxos Gold (PAXG) is backed by one fine troy ounce of a 400-ounce London Good Delivery gold bar, stored in Brink's vaults.	Generally higher
Crypto Backed	Backed by other cryptocurrencies.	Are typically overcollateralized due to price volatility of cryptocurrencies. For example, Maker's DAI is pegged to the US dollar, but is backed by cryptocurrencies such as ETH, BAT, WBTC, and USDC.	Generally lower
Algorithmic	Use a two-coin system in which one coin is intended to absorb market volatility, and the other intends to maintain the peg.	Terra Luna was one example of an algorithmic stablecoin. The peg is generally unstable and may depend on arbitrage investors attempting to profit from weakness in demand or supply to maintain the peg.	Low

There are several different types of stablecoins, and their price stability varies based on how they are structured. Fiat-backed stablecoins are backed by the fiat currency of a government. For example, a USD Coin (USDC) is a stablecoin said to be backed 1:1 by the U.S. dollar. So, for each USDC that goes into circulation, one U.S. dollar is supposed to be held in reserve by the issuer, Circle. Fiat-backed stablecoins are considered to be more price stable than other types of cryptocurrencies, but they are also more centralized in their governance.²⁶

Commodity-backed stablecoins are backed by physical commodities, such as gold, silver, or oil. Essentially, commodity-backed stablecoins are a

25. Derived from research by the Blockchain Laboratory Team at the Wharton School.

26. For example, they are issued by a central company, such as USDT and Circle.

digital representation of a real-world asset. Gold is a commonly used collateral in commodity-backed stablecoins. Commodity-backed stablecoins are purported to make investing in a real asset easier or more accessible, as the asset holds the same value as the collateral and can be liquidated when desired. Commodity-backed stablecoins are sometimes considered to be somewhat price stable, and still centralized in governance.

A third type of stablecoin is the crypto-backed stablecoin. These stablecoins are backed by other cryptocurrencies, and they do not employ a 1:1 peg. Instead, crypto-backed stablecoins are purportedly overcollateralized to compensate for the very high price volatility of the cryptocurrency reserves. For example, SUSD is a dollar-pegged stablecoin issued by the Synthetix protocol that is backed by SNX and ETH. In order to maintain the peg, the value of the collateral must stay above the pegged value of the circulating stablecoins. This means that crypto-backed stablecoins must be significantly over-collateralized in order to account for the fluctuating value of their collateral.

Another example of a crypto-backed stablecoin is DAI, which can currently be borrowed from the MakerDAO lending platform on the Ethereum blockchain. If the borrower deposits some crypto collateral, usually USDC or ETH, the protocol loans DAI to the user. The protocol currently requires a minimum collateralization ratio (e.g., 150%).²⁷ If users' collateral loses too much value after being deposited, they may have to liquidate it and return the borrowed DAI. Another example is Wrapped Bitcoin (WBTC), which exists on the Ethereum blockchain but is backed by Bitcoin. Crypto-backed stablecoins have a lower level of price stability but are said to have a higher level of decentralized governance than fiat-backed or commodity-backed stablecoins.

The last type of stablecoin is the algorithmic stablecoin. Unlike the other types of stablecoins discussed here, algorithmic stablecoins are not backed by any assets. Algorithmic stablecoins are controlled by computerized algorithms that are intended to maintain their value. For example, TerraUSD (UST) was an algorithmic stablecoin pegged to the U.S. dollar but not backed by any assets, and was intended to maintain its value through a relationship with Luna (LUNA), the "native asset" on the Terra blockchain. To attempt to maintain price stability, the Terra blockchain allowed users to convert one UST to \$1 worth of LUNA at any time. If the price of one UST exceeded \$1 in value, some of it would be burned. But if the price fell below \$1, LUNA would be burned, pushing the price back

27. DAI collateralization is determined by the DAO vote; however, the collateralization ratio is based on the collateral itself.

towards the peg. As the crypto crash of 2022 showed, algorithmic stablecoins are generally not considered to be price stable and they are highly decentralized.

B. The Terra Luna Collapse of 2022

The UST stablecoin was at the center of the spring 2022 crypto crash. As discussed above, UST is an algorithmic stablecoin, which means that it was not backed by U.S. dollars, commodities, or other cryptocurrencies. Rather, it was backed by an on-blockchain algorithm that facilitates changes in supply and demand between the stablecoin and a cryptocurrency that was created to help maintain the stablecoin peg, called a “native token.” In this case, the native token of UST was LUNA. As of May 2022, there was over \$18.5 billion worth of UST in circulation and the market capitalization of LUNA was \$40 billion.²⁸

While there are different theories about what happened with UST, essentially, UST dipped below \$1, and neither the Terra protocol algorithm (which maintains the mathematical relationship with Luna) nor lending out of the Luna Foundation Guard (an organization that supports Terra) could bring the value of UST back to \$1. As the price of UST dropped below \$1, users began converting UST to LUNA. Each conversion of UST to LUNA increased the supply of LUNA, which pushed down the price of LUNA. The rapid increase in the supply of LUNA tokens drove its price to nearly zero.

When the Terra peg broke, the Luna Foundation Guard purchased UST with bitcoin in an effort to support the peg. This created direct downward pressure on the price of bitcoin. The situation was complicated by the fact that bitcoin and other cryptocurrencies have been found to be correlated with other risk assets, such as stocks. For example, research data showed the ninety-day correlation between bitcoin and the S&P 500 reached an all-time high in March of 2022.²⁹

This high correlation with risk assets complicates matters for crypto. Notably, a large amount of bitcoin (more than 90%, by some accounts) is said to be concentrated among the same small group of holders. This concentration may result in greater price volatility. In addition, some assert that bitcoin is associated with tech stocks (such as PayPal or CashApp) since they utilize bitcoin. If bitcoin is considered to be a risk asset, rather than a

28. *Terra Classic*, COINMARKETCAP, <https://coinmarketcap.com/currencies/terra-luna/> [https://perma.cc/ZH6U-MUKR].

29. Vette Lunde, *Bitcoin's Correlation to U.S. Equities Grows Further*, ARCANE: RSCH. (May 9, 2022), <https://arcane.no/research/bitcoins-correlation-to-us-equities-grows-further/> [https://perma.cc/EQ4M-EC3W].

store of value, then it may explain the high correlation with other risk assets. Therefore, if the price of stocks falls, the price of crypto falls as well.³⁰

Many individual users and investors lost money in the 2022 crypto crash. Investors in UST and other cryptocurrencies lost a great deal of money. Some reports account for investors putting their life savings into UST and losing everything. Other reports noted that investors had put emergency funds or the down payment on a house into UST, only to lose the funds. Of course, the venture investors backing the Luna Foundation also lost their investments. Altogether, it is estimated that more than \$40 billion of value was lost.³¹

C. Freezing, Clawbacks, Blacklisting, Wrapping

There are certainly other dynamics in the crypto space that give rise to very significant investor and consumer protection concerns. Due to the decentralized nature of the blockchain that executes these stablecoin smart contracts, it can be almost impossible to restrict access to the functions of the contract once it has been written. For example, when the SEC began scrutinizing synthetic assets, Uniswap Labs (the development firm behind the decentralized crypto exchange Uniswap) could not shut down the exchange that the SEC had deemed problematic.³²

The smart contracts in question were not upgradable nor could they be paused. Therefore, in an attempt to comply with the SEC, Uniswap removed these trading pairs from its website. Uniswap Labs cited the “evolving regulatory landscape” in explaining its actions.³³ Notably, the Uniswap website is just a “front-end interface,” built to improve the user experience. Determined users could still trade these synthetic tokens by interacting directly with the Ethereum contract.

Although it can be extremely difficult to censor transactions on blockchain, individual tokens (including stablecoins) are controlled by distinct smart contracts, and these smart contracts can include censorship mechanisms. Assets like Bitcoin (BTC) or Ethereum (ETH) were in fact

30. Vetle Lunde, *A Very Correlated Crypto Market*, ARCANE: RSCH. (Mar. 14, 2022), <https://arcane.no/research/a-very-correlated-crypto-market/> [<https://perma.cc/6KYZ-2DHS>]

31. David Yaffe-Bellany & Erin Griffith, *How a Trash-Talking Crypto Founder Caused a \$40 Billion Crash*, N.Y. TIMES (May 20, 2022), <https://www.nytimes.com/2022/05/18/technology/terra-luna-cryptocurrency-do-kwon.html> [<https://perma.cc/K85R-WY22>].

32. Kollen Post & Frank Chaparro, *Uniswap Labs Restricts Access to Certain Tokens*, THE BLOCK (July 23, 2021, 7:10 PM), <https://www.theblockcrypto.com/linkedin/112399/uniswap-labs-culls-synthetic-stock-and-derivatives-citing-evolving-regulatory-landscape/> [<https://perma.cc/M7KX-Z8G3>].

33. *Id.*

designed to prevent censorship, and therefore cannot be locked or “frozen.” However, stablecoins such as USDC or USDT are controlled by smart contracts and therefore can be frozen. In fact, smart contracts can be locked to prevent users from transferring them.

One such method of locking is called “pausing,” which halts all transactions with the token. A more granular approach is called “blacklisting,” in which only certain digital addresses are restricted from transferring tokens. Most stablecoins that are backed by off-chain reserve assets offer some form of blacklisting. These features must be built into the smart contract at the time it is deployed, or, at the time the contract is originally built, it must be designed to be upgradeable. If not, features such as pausing and blacklisting cannot be added later.

Another similar feature is called “clawback,” which provides a method for the contract owner of fiat-backed stablecoins to empty a user’s wallet without a signature from the user.³⁴ Clawbacks and freezing are closely related, and one might argue that the primary difference is one of bookkeeping. If a user’s assets are frozen, they cannot be transferred, and are thus essentially useless. The assets do, however, remain “on the books” and if one were to query the “balanceOf()” or the “totalSupply()” functions on the token contract, the frozen assets would still be counted. A clawback goes beyond a freeze, eliminating the frozen tokens from on-chain bookkeeping.

Blacklisting is primarily used to address unwanted user behavior, whereas clawbacks can be used to recover stolen funds, as well as to recover lost or misplaced funds. From time to time, users may transfer tokens to an incorrect digital address and, in many cases, these funds cannot be recovered. If, however, a user sends USDT to an incorrect address, even if the recipient has no way to return the funds, Tether can claw those funds back from the recipient. Using this mechanism Tether has recovered more than \$87 million in user funds that might have otherwise been lost.³⁵

A simple method for circumventing locking and clawback features is known as “wrapping” and may also be included in a smart contract. Token wrapping can take many forms, but the basic idea is to use another smart contract as an intermediary, similar to a custodian. For example, a user can potentially deposit USDC into the DAI Peg Stability Module (PSM) in exchange for DAI tokens. From the perspective of the USDC contract, the

34. In most token contracts, transferring a token requires a signature from the token owner.

35. Yogita Khatri, *Tether Has Recovered \$87 Million in USDT Sent to Wrong Addresses since Its Launch*, THE BLOCK (Jan. 22, 2022, 8:45 AM), <https://www.theblock.co/post/131258/tether-recovered-87-million-usdt-wrong-addresses-since-launch> [<https://perma.cc/KP74-MHGE>].

DAI PSM is now the owner, but a user can then transfer the DAI. At the time of this writing, the DAI PSM is currently the largest holder of USDC on the Ethereum blockchain.

Another method of token wrapping is known as “bridging.” Bridges do not actually move tokens from one chain to another—instead, they retain custody of the tokens on the original source blockchain and issue new “wrapped” tokens on the destination chain. So, if a user sends USDC across the Solana Wormhole Bridge,³⁶ or the Avalanche Bridge,³⁷ the bridge contract attempts to act similarly to a custodian for the USDC tokens and issues the user-wrapped USDC (which cannot be frozen) on the destination chain. These wrapped tokens are controlled by the bridge contract, and not by the original issuer.

Interacting with bridges exposes users to any vulnerabilities that may exist in the bridge contract. To be sure, there are many serious instances of security problems on bridges. In February 2022, the Solana Wormhole Bridge was the victim of a hack³⁸ that stole more than \$320 million worth of ETH.³⁹ In August 2022, the Nomad Token Bridge was hacked for \$190 million.⁴⁰ In a recent report, Chainalysis found that more than \$2 billion has been stolen across thirteen separate bridges, most of which occurred in 2022.⁴¹ Notably, bridging can also potentially be used to circumvent lockouts, clawbacks, and transfer fees that may affect the underlying token.

Bridging stablecoins is very common, and in some situations, bridge-wrapped tokens are more popular than their original counterparts. For example, Circle issues USDC on the Avalanche blockchain, but as of February 2022, there were only about 340 million USDC (controlled by Circle), and more than 1.8 billion “bridge wrapped” USDC (controlled by

36. Wormhole, SOLANA (Apr. 3, 2020), <https://solana.com/wormhole> [<https://perma.cc/2HL7-UBGF>].

37. Avalanche Bridge™ FAQ, AVALANCHE, <https://support.avax.network/en/articles/6092559-avalanche-bridge-faq> [<https://perma.cc/JV6L-ZY9A>] (last updated Jan. 2023).

38. *Solana's Wormhole Hack Post-Mortem Analysis*, MEDIUM: EXTROPY.IO (Feb. 8, 2022), <https://extropy-io.medium.com/solanas-wormhole-hack-post-mortem-analysis-3b68b9e88e13> [<https://perma.cc/6VQY-KYRV>].

39. Jonathan Ponciano, *Jump Crypto Fronts \$325 Million in Stolen Crypto One Day After Solana's Biggest Hack Ever*, FORBES (Feb. 3, 2022, 2:43 PM), <https://www.forbes.com/sites/jonathanponciano/2022/02/03/vc-backer-replaces-325-million-in-stolen-crypto-one-day-after-solanas-biggest-hack-ever/> [<https://perma.cc/9J2K-2PYT>].

40. Jason Nelson, *Crypto Bridge Nomad Exploited for \$190M in 'Frenzied Free-For-All'*, DECRYPT (Aug. 2, 2022), <https://decrypt.co/106459/crypto-bridge-nomad-exploited-190m-frenzied-free-for-all> [<https://perma.cc/C79R-6T7L>].

41. *Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk*, CHAINALYSIS (Aug. 2, 2022), <https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/> [<https://perma.cc/KPL5-FKYA>].

Avalanche Bridge) on the Avalanche blockchain. This situation presents an interesting problem, since the USDC on the Avalanche blockchain is not within the security controls built directly into the USDC contract. As of November 2022, the amount of “real” USDC⁴² on the Avalanche blockchain has surpassed the amount of “bridge-wrapped” USDC,⁴³ but over 191M “bridge-wrapped” USDC remains in circulation on Avalanche, and these wrapped tokens remain outside of Circle’s control.

Another method for potential token wrapping is through decentralized exchanges. For example, stablecoins like USDC or USDT can be deposited in Curve’s 3Pool⁴⁴ in exchange for 3Crv tokens,⁴⁵ which cannot be frozen, and can be redeemed by the underlying USDC or USDT in the 3Pool contract. Balancer take this process a step further, allowing users to maintain internal balances in the Balancer Vault contract.⁴⁶ The Balancer Vault contract holds the user’s tokens, and this allows the user to transfer their tokens within the Balancer ecosystem without communicating with the issuing contract.

D. Bankruptcy and Insolvency

It is important to recognize that if the dynamics or practices mentioned result in insolvency of a crypto scheme, there is no legal clarity on how resolution of a failed arrangement will be handled. Many key policy issues loom regarding the resolution of a failed crypto company. Among those issues to be considered are identification of the primary insolvency regulator, the applicable customer protection regime, what is the relevant resolution rulebook, who will be the receiver in insolvency, whether public funding is available, the applicability of an automatic stay to short-term liabilities, and the order of claims.

42. Overview of USDC Controlled by Circle, SNOWTRACE, <https://snowtrace.io/token/0xb97ef9ef8734c71904d8002f8b6bc66dd9c48a6e> (last visited Nov. 9, 2022).

43. Overview of USDC Controlled by Avalanche Bridge, SNOWTRACE <https://snowtrace.io/token/0xa7d7079b0fead91f3e65f86e8915cb59c1a4c664> (last visited Nov. 9, 2022).

44. Curve’s 3pool, CURVE, <https://curve.fi/3pool> (last visited Oct. 29, 2022).

45. *LP 3pool Curve*, COINMARKETCAP, <https://coinmarketcap.com/currencies/lp-3pool-curve/> (last visited Oct. 29, 2022) (providing an overview of the 3Crv token).

46. *The Vault: Internal Balances*, BALANCER, <https://docs.balancer.fi/products/the-vault/#internal-balances> [<https://perma.cc/Y5PP-LC3X>] (last modified Dec. 6, 2022).

Calibrating Resolution Regimes for Traditional Financial Institutions & Crypto							
	Lehman Brothers U.S. Broker Dealer	Man Financial ("MF Global")	Mt. Gox	Celsius Network	Voyager Digital	FTX	Systemically Important Financial Institution (Post 2010 Dodd Frank Act)
Business Activities	Brokerage, lending, trading	Brokerage, lending, trading	Brokerage, lending, trading	Brokerage, lending, trading	Brokerage, lending, trading	Brokerage, lending, trading	Brokerage, lending, trading
Primary Regulator	U.S. Securities Exchange Commission	U.S. Commodity Futures Trading Commission	Japanese Ministry of Finance	California Department of Financial Protection and Innovation	States (Money Transmitter Licenses)	FTX: Bahamas, other global, etc FTX US: States (Money Transmitter Licenses), U.S. Commodity Futures Trading Commission	The Federal Reserve, U.S. Securities Exchange Commission, U.S. Commodity Futures Trading Commission
Customer Assets at Risk (approximate)	\$106 billion	\$8.1 billion	750,000 Bitcoin	\$4.72 billion	Over \$1.67 billion. Exact amount unknown	\$10-50 billion	N/A
Number of Customer Accounts	110,000+	38,000	24,000	1.7 million users as of June 2022 (CNBC)	3.5 million users as of July 2022 (Axios)	2.2 million+	N/A
Leverage Ratio (approximate)	30.7x	30-40x	Unknown	Unknown	Unknown	Unknown, likely highly leveraged	Minimum 3% Capital to Exposure (under Basel III)
Customer Protection Regime	U.S. securities regulation, SEC Rule 15c3-3 (the Customer Protection Rule)	U.S. securities regulation, SEC Rule 15c3-3 (the Customer Protection Rule)	None	None	None	None	U.S. securities regulation, SEC Rule 15c3-3 (the Customer Protection Rule)
Receiver in Insolvency	The Securities Investor Protection Corporation (SIPC)	The Securities Investor Protection Corporation (SIPC)	Unknown	Unknown	Unknown	Unknown	The Federal Deposit Insurance Corporation or SIPC
Bankruptcy Regime	Chapter 11 of the U.S. Bankruptcy Code	Chapter 11 of the U.S. Bankruptcy Code	Bankruptcy Protection in Tokyo District Court	Chapter 11 of the U.S. Bankruptcy Code	Chapter 11 of the U.S. Bankruptcy Code	Chapter 11 of the U.S. Bankruptcy Code	Title II of the Dodd-Frank Wall Street Reform and Protection Act
Funding Available	The SIPC Fund, up to \$500,000 with a \$250,000 limit for cash	The SIPC Fund, up to \$500,000 with a \$250,000 limit for cash	None	None	None	None	FDIC up to \$250,000, SIPC up to \$500,000, note that the Orderly Liquidation Fund (OLF) has yet to be funded
Ultimate Customer Losses	Zero	Zero	750,000 Bitcoin	Unknown	Unknown	Unknown	Zero (theoretically)
<p>Many key policy issues loom regarding the resolution of a failed crypto company: identification of the primary regulator, the applicable customer protection regime, what is the applicable resolution regime, who will be the receiver in insolvency, whether funding is available, applicability of an automatic stay to short-term liabilities, and the order of claims. This last issue, the order of claims, is especially critical if a decentralized finance protocol pre-specifies the treatment of assets in a resolution process in a way that differs from the traditional order of claims. A related issue is whether voidable transfer provisions will then apply. This draft is not intended as a legal advice.</p>							

Figure 2. Calibrating Resolution Regimes for Traditional Financial Institutions and Crypto⁴⁷

47. This chart was created by the Blockchain Laboratory Team at the Wharton School.

This last issue, the order of claims, is especially critical if a decentralized finance protocol pre-specifies the treatment of assets in a resolution process in a way that differs from the traditional order of claims.

A related issue is whether voidable transfer provisions will then apply. Although we do not address bankruptcy and insolvency regimes in this Article, given the importance of clarity in the resolution regime to provide confidence to investors and users of crypto assets, the authors recommend that policymakers evaluate and provide clarity on these issues with all due haste.

E. Limited Terms of Service

To address functionality and the activities of stablecoins, many issuers employ limited terms of service in the form of a “contract of adhesion.” Contracts of adhesion are contracts between two parties where the terms and conditions are set by one party and the other has little or no ability to negotiate. Contracts of adhesion are presented to the consumer on a take it or leave it basis. For example, when sending an express package, the consumer signs a receipt for payment that also lists the limited terms of service of the mail carrier. Limited terms of service and contracts of adhesion have become synonymous and ubiquitous through e-commerce and modern-day high volume internet sales.

Online limited terms of service are widespread and presumptively valid when entered into via what is known as a “click-wrap” agreement, which requires users to select “I Agree” when using a website. On the issuer side, companies can enforce their own limited terms of service by refusing to provide service to the user. For the user, terms of service are enforceable via contract law.⁴⁸ Remedies for breach could be sought through contract law mechanisms, and certain provisions could be challenged under the doctrines of fraud or unconscionability.⁴⁹ These remedies may require lengthy and

Joseph Jasperse & Sarah Hammer, *Calibrating Resolution Regimes for Traditional Financial Institutions and Crypto 1–2* (Nov. 15, 2022) (unpublished manuscript), <https://dx.doi.org/10.2139/ssrn.4228350>. Note that these and other crypto-related bankruptcy cases are ongoing, and therefore the information provided is subject to additional discovery, argumentation, and evolving interpretations of jurisdiction, law, and regulation.

48. See, e.g., *McInnes v. LPL Financial, LLC*, 994 N.E.2d 790, 798–99 (Mass. 2013) (stating that contracts of adhesion are enforceable unless they are unconscionable, offend public policy, or are shown to be unfair in the particular circumstances).

49. See U.C.C. § 2-302 cmt. 1 (Am. L. Inst. & Unif. L. Comm’n 1977) (“The basic test is whether, in the light of the general commercial background and the commercial needs of the particular trade or case, the clauses involved are so one-sided as to be unconscionable

expensive litigation.

Importantly, many users may be surprised to learn that the limited terms of service primarily confer rights on the provider, and they actually have very few rights as users. The terms of service typically confer most rights and legal provisions only to providers. Another key challenge of terms of service is the ability of users to comprehend them. Even if the user takes the time to read the agreements, they often contain a high degree of jargon and verbosity that obfuscates the meaning of the terms of service. Moreover, the terms of service can be changed at any time, are freely assignable, and if there is an amendment, there is often no notice or consent requirement.⁵⁰

The employment of limited terms of service to stablecoins and cryptocurrency generally creates several additional challenges. First, the terms of service typically allow the provider broad rights to engage in complicated crypto-related activities. For example, freezing, clawbacks, and blacklisting practices such as those described in previous sections are widely permitted. In addition, the terms of service typically do not clarify treatment of customer assets in the event of financial distress of the provider. Indeed, most stablecoin or cryptocurrency holders have no recourse to recover their assets in the event of collapse of the issuer.⁵¹ As noted previously, this ambiguity is especially problematic in insolvency.

IV. NATIONAL INVESTOR AND CONSUMER PROTECTION FRAMEWORK

It is well known that a key point of tension in the U.S. regulatory framework relating to crypto is whether securities law or commodities law applies or should apply. A directly related question is which regulatory agency should be the primary crypto regulator, the SEC or the Commodity Futures Trading Commission (CFTC). This issue has been the subject of numerous articles, speeches, legislative proposals, and political discussions. While some have suggested that the United States will not have clarity on this issue until new laws are passed by Congress, others have claimed that

under the circumstances existing at the time of the making of the contract. . . . The principle is one of the prevention of oppression and unfair surprise and not of disturbance of allocation of risks because of superior bargaining power.”)

50. Overview of Terms of Service, TETHER, <https://tether.to/en/legal/> (last visited Oct. 29, 2022). For example, for Tether, section 17 states: “These Terms of Service, and any of the rights, duties, and obligations contained herein, are freely assignable by Tether without notice or your consent.”

51. See Kara Bruce, Christopher K. Odinet & Andrea Tosato, *The Private Law of Stablecoins*, 55 ARIZ. ST. L.J. (forthcoming 2023) (discussing the lack of recourse for cryptocurrency and stablecoin owners).

existing law already provides sufficient clarity.⁵²

The SEC employs a test known as the *Howey* Test to determine whether a thing is an investment contract and therefore falls within the securities law regime. The *Howey* Test originates from a 1946 Supreme Court Case, *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). The *Howey* Test consists of four prongs, all of which must be satisfied in order for the SEC to classify a thing as an investment contract: (1) it must be an investment of money, (2) in a common enterprise, (3) with an expectation of profit, (4) to be derived from the efforts of others.⁵³ It is unclear whether many cryptocurrencies pass the *Howey* Test due to either the lack of a common enterprise and/or, in the case of stablecoins, the expectation of profit.

SEC Chair Gary Gensler has stated that most cryptocurrencies qualify as securities and therefore fall under the umbrella of the securities laws and within the purview of the SEC:

The fact is, most crypto tokens involve a group of entrepreneurs raising money from the public in anticipation of profits—the hallmark of an investment contract or security under our jurisdiction. Some, probably only a few, are like digital gold; thus, they might be like commodities. Even fewer, if any, are actually being used in general commerce for payments.⁵⁴

Chair Gensler has also stated that Bitcoin is the only crypto asset that qualifies as a commodity—implying that even Ethereum is a security.⁵⁵

On the other hand, the CFTC in 2015 defined Bitcoin and other virtual currencies as commodities under the U.S. Commodity Exchange Act (the CEA).⁵⁶ Under the CEA, the term “commodity” includes “all other goods and articles . . . and all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt with.”⁵⁷ The CFTC’s determination that Bitcoin and other virtual currencies are properly defined

52. Jeremy Chan, *SEC Chair Gary Gensler Says Crypto Assets are Securities and thus ‘Core to Our Remit,’* FIN. NEWS (May 11, 2022, 7:03 PM), <https://www.fn london.com/articles/sec-chair-gary-gensler-says-crypto-assets-are-securities-and-thus-core-to-our-remit-2022-0511> [<https://perma.cc/R5FL-M4DU>].

53. *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

54. Gary Gensler, “A ‘New’ New Era.” *Prepared Remarks Before the International Swaps and Derivatives Association Annual Meeting*, SEC (May 11, 2022), <https://www.sec.gov/news/speech/gensler-remarks-swaps-and-derivatives-association-annual-meeting-051122> [<https://perma.cc/LMP4-QABF>].

55. CNBC Television, *SEC Chair Gary Gensler discusses potential crypto regulation and stablecoins*, YOUTUBE (June 27, 2022), https://youtu.be/oTa_3W8rMno [<https://perma.cc/WU3K-PGSZ>].

56. *In re Coinflip, Inc.*, CFTC No. 15-19, 2015 WL 5535736 (Sept. 17, 2015).

57. *See* 7 U.S.C. § 1a(1)(9) (defining the term “commodity”).

as commodities in 2015 was articulated in an enforcement action, *In re Coinflip, Inc.*⁵⁸ In the settlement order, the CFTC stated that individuals who had created a platform for the purchase and sale of Bitcoin options were actually operating a facility for the trading and processing of swaps without being registered as a swap execution facility or a designated contract market.⁵⁹

The CFTC applied the broad definition of commodity as laid out in the CEA and found that the scope of that definition included Bitcoin: “The definition of a ‘commodity’ is broad. Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.”⁶⁰ In October 2019, Chairman Heath Tarbert stated his view that Ether, the world’s second-largest cryptocurrency by market capitalization, is a commodity and therefore would fall within the CFTC’s jurisdiction as well.⁶¹ Current CFTC Chair Rostin Behnam has stated that “[t]he CFTC is ready and well situated to address the risks in the cash markets for digital assets through direct oversight.”⁶²

At the time of this writing, jurisdiction of the SEC and the CFTC remains in flux. In July 2022, the SEC announced charges against a former Coinbase manager and two others in a crypto asset insider trading action. The SEC’s complaint in *SEC v. Wahi* alleges that an individual, Ishan Wahi, helped to coordinate the platforms’ public listing announcements and tipped the timing and content of listing announcements to his brother and friend.⁶³ This led to purchases of at least twenty-five crypto assets, at least nine of which were securities (according to the complaint), then sold them shortly after the announcements for profits totaling more than \$1.1 million.⁶⁴ The *Wahi* case could also have implications for Coinbase as well, which made a

58. *In re Coinflip, Inc.*, 2015 WL 5535736.

59. *Id.* at *2–3.

60. *Id.* at *2 (internal citations omitted).

61. *IN CASE YOU MISSED IT: Chairman Tarbert Comments on Cryptocurrency Regulation at Yahoo! Finance All Markets Summit*, COMMODITY FUTURES TRADING COMM’N (Oct. 10, 2019), <https://www.cftc.gov/PressRoom/PressReleases/8051-19> [<https://perma.cc/JX3H-YCG8>].

62. *Keynote Address of Chairman Rostin Behnam at the Brookings Institution Webcast on the Future of Crypto Regulation*, COMMODITY FUTURES TRADING COMM’N (July 25, 2022), <https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam24> [<https://perma.cc/KWX5-ZAUP>].

63. Complaint at 1, *SEC v. Wahi*, No. 2:22-cv-01009 (W.D. Wash. July 21, 2022).

64. *SEC Charges Former Coinbase Manager Two Others in Crypto Asset Insider Trading Action*, SEC (July 21, 2022), <https://www.sec.gov/news/press-release/2022-127> [<https://perma.cc/ZNX5-URZE>].

statement that the assets at issue are not securities.⁶⁵

Underscoring the case, CFTC Commissioner Caroline Pham made a statement following the SEC announcement that:

The case *SEC v. Wahi* is a striking example of ‘regulation by enforcement.’ The SEC complaint alleges that dozens of digital assets, including those that could be described as utility tokens and/or certain tokens relating to decentralized autonomous organizations (DAOs), are securities.

The SEC’s allegations could have broad implications beyond this single case, underscoring how critical and urgent it is that regulators work together.⁶⁶

On September 27, 2022, CFTC Commissioner Pham made another statement related to jurisdiction over crypto regulation, calling for the establishment of a new Office of the Retail Advocate which would that would “further enshrine the CFTC’s current customer protection mandate under Dodd Frank.”⁶⁷ Commissioner Pham argued that the CFTC already has the experience, expertise, and track record to oversee retail crypto markets, but if Congress were to grant the CFTC clear authority over spot crypto markets, it should also establish an office that would further advance customer protection.⁶⁸ Surely, more policy statements and developments will continue to take place as the federal financial regulatory agencies clarify their scope over crypto regulation.

It is worth noting that, depending on whether the crypto asset in question is a stablecoin backed by fiat, commodities, crypto, or an algorithm, yet another regulator—the Office of the Comptroller of the Currency (OCC)—may be considered an additional appropriate regulatory authority.

65. Paul Grewal, *Coinbase Does Not List Securities. End of Story.*, COINBASE: BLOG (July 21, 2022), <https://blog.coinbase.com/coinbase-does-not-list-securities-end-of-story-e58dc873be79> [<https://perma.cc/F4UL-ALRV>].

66. *Statement of Commissioner Caroline D. Pham on SEC v. Wahi*, COMMODITY FUTURES TRADING COMM’N (July 21, 2022), <https://www.cftc.gov/PressRoom/SpeechesTestimony/phamstatement072122> [<https://perma.cc/Z45J-RCQG>].

67. *Keynote Address by Commissioner Caroline D. Pham at CordaCon 2022, A Voice for the People: A Proposal for A New Office of the Retail Advocate*, COMMODITY FUTURES TRADING COMM’N (Sept. 27, 2022), <https://www.cftc.gov/PressRoom/SpeechesTestimony/opapham5> [<https://perma.cc/Z9DT-HX3Z>].

68. *Id.*

In previous OCC Interpretive Letters 1170,⁶⁹ 1172,⁷⁰ and 1174,⁷¹ issued in 2020 and 2021, the OCC granted provisional authority to banks to offer cryptocurrency custody services to customers, to hold stablecoin reserves, and to facilitate payment transactions using stablecoins, respectively. While these letters are under review,⁷² the exiting permissions granted by the OCC certainly implicate its supervisory authorities to promote safety and soundness.

The Federal Reserve may of course also have supervisory jurisdiction. The Federal Reserve has released a Supervision and Regulation Letter SR 22-6/CA 22-6 stipulating that Federal-Reserve supervised banking organization engaging or seeking to engage in crypto-asset related activities must notify its lead point of contact at the Federal Reserve.⁷³ A supervised banking organization must ensure its activities are legally permissible and determine whether any filings are required under federal law.⁷⁴

A. Regulatory Gaps and Challenges

The challenge in protecting users of crypto, then, is manifold. First, as discussed in our article *Taming the Wild West: Achieving Public Policy*

69. Office of the Comptroller of the Currency, Interpretive Letter #1170, Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 2, 2020), <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf> [<https://perma.cc/R7LJ-ABPV>].

70. Office of the Comptroller of the Currency, Interpretive Letter #1172, OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves (Sept. 21, 2020), <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf> [<https://perma.cc/FJQ6-CXRB>].

71. Office of the Comptroller of the Currency, Interpretive Letter #1174, OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities (Jan. 4, 2021), <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf> [<https://perma.cc/J37Q-VMSM>].

72. *OCC Clarifies Bank Authority to Engage in Certain Cryptocurrency Activities and Authority of OCC to Charter National Trust Banks*, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Nov. 23, 2021), <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-121.html> [<https://perma.cc/DX3Z-UJHJ>].

73. Bd. of Governors of the Fed. Reserve Sys., Letter on Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations to the Officer in Charge of Supervision and Appropriate Supervisory and Examination Staff at Each Federal Reserve Bank and Banking Organizations Supervised by the Federal Reserve (Aug. 16, 2022), <https://www.federalreserve.gov/supervisionreg/srletters/SR2206.htm> [<https://perma.cc/9MVQ-7WWL>].

74. *Id.*

Goals Through Crypto Standards,⁷⁵ there may not be a central entity or traditional intermediary that would be the subject of regulatory authority. Without a central entity or traditional intermediary to regulate, standard setting is essential to set the stage for responsible industry practices.⁷⁶ In addition, it is unclear whether securities laws or commodities laws apply or should apply, and whether the SEC or CFTC has or should have legal jurisdiction. Finally, without clarity around securities or commodities laws applicability, there cannot be complete clarity as to whether the consumer protection framework can provide an overlay.

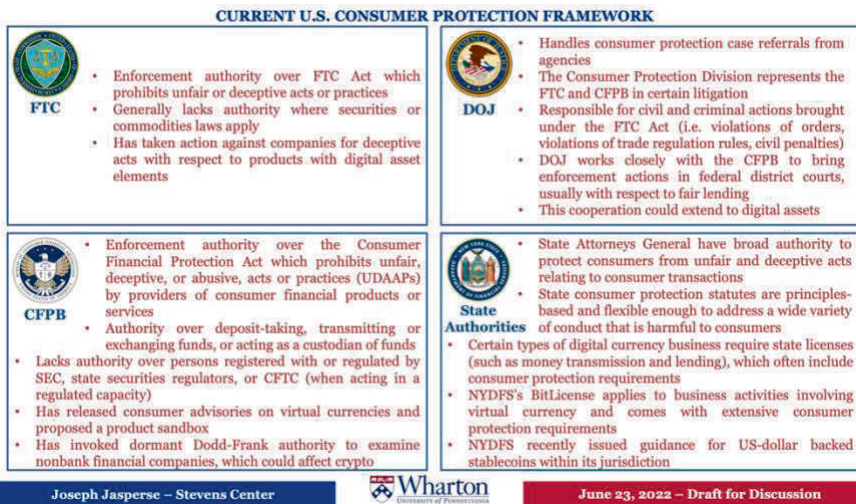


Figure 3. Current U.S. Consumer Protection Framework

Two additional relevant government agencies overseeing consumer protection are the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC). Established by the Dodd-Frank Wall Street and Consumer Protection Act of 2010, the CFPB has enforcement authority over the Consumer Financial Protection Act, which prohibits unfair, deceptive, or abusive acts or practices (UDAAPs) by providers of consumer financial products or services.⁷⁷ However, the CFPB may lack authority over persons registered with or regulated by the SEC, state

75. Brett Falk & Sarah Hammer, *Taming the Wild West: Achieving Public Policy Goals Through Crypto Standards* (Apr. 8, 2020) (unpublished working paper), <https://dx.doi.org/10.2139/ssrn.4096816>.

76. The authors have proposed *Crypto Standards*.

77. 12 U.S.C. §§ 5481, 5531, 5536(a) (2010).

securities regulators, or the CFTC (when the entity is acting in a regulated capacity).⁷⁸

Likewise, the FTC has some consumer protection authorities, based on its principal mission of enforcing civil U.S. antitrust law and promoting consumer protection. Generally, the FTC has enforcement authority over the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.⁷⁹ The FTC has acted against companies for deceptive acts with respect to products that have digital asset elements.⁸⁰ However, like the CFPB, the FTC may lack authority where securities or commodities laws apply.⁸¹

To be clear, consumer financial protections are much different from securities laws or commodities laws protections, as they are focused on the prohibition of UDAAPs. Securities laws are focused on investor disclosures and prohibit deceit, misrepresentation, and other fraud.⁸² Commodities laws protections maintain anti-fraud, false reporting, and anti-market manipulation authority over the markets.⁸³ To be sure, policy decisions about which regulatory framework applies or should apply will have long-term implications for the industry and users of crypto.

B. Investor and Consumer Protection Considerations

In light of the complexity and fragmentation of the existing regulatory framework, in this paper, we set forth a comprehensive approach to investor and consumer protection for crypto users that consists of three fundamental pillars:

78. *Id.* §§ 5481(20)–(21). And while the Consumer Financial Protection Bureau recently invoked its dormant Dodd Frank Act authority to examine nonbank financial companies, current Director of the Consumer Financial Protection Bureau Rohit Chopra has stated that crypto does not fall within the scope of its authority, since it is not yet used primarily for personal, family, or household purposes. Kyle Tayman, Andrew Kim & Collin Grier, *What to Expect from CFPB's Entry into Cryptocurrency Arena*, LAW360 (June 6, 2022), <https://www.law360.com/real-estate-authority/commercial/articles/1497776/what-to-expect-from-cfpb-s-entry-into-cryptocurrency-arena> [<https://perma.cc/3DNU-JDTJ>].

79. 15 U.S.C. § 45(a).

80. *See, e.g.*, Complaint, *FTC v. BF Labs, Inc.*, No. 4:14-CV-00815 (W.D. Mo. Sept. 17, 2014); Complaint, *FTC v. Equiliv Invs.*, No. 2:2015-CV-04379 (D.N.J. June 29, 2015); Complaint, *FTC v. Dluca*, No. 0:18-CV-60379 (S.D. Fla. Feb. 20, 2018).

81. 7 U.S.C. § 2.

82. *See What We Do*, SEC, <https://www.sec.gov/about/what-we-do> [<https://perma.cc/K7GA-S2PY>] (last modified Nov. 22, 2021) (providing an overview of SEC's responsibilities).

83. *Keynote Address of Chairman Rostin Behnam on the Future of Crypto Regulation*, COMMODITY FUTURES TRADING COMM'N (July 25, 2022), <https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam24> [<https://perma.cc/SZG7-5TWE>].

1. Crypto standard setting by non-governmental entities, with input by and leadership on implementation from industry.
2. Clear, strong national regulation, with consistency brought forth by cooperative interagency rule-making processes.
3. Participation in recognized international standard-setting bodies as well as adherence to agreed-upon global standards.⁸⁴

As discussed, to be effective, Crypto Standards must be grounded in evidence and objectivity and have buy-in from industry participants as well as respected policymakers. Without this, they cannot be effective, nor will they have any binding force. Crypto Standards may also be combined with a regulatory mandate to provide them with the force of law.

However, it is clear that Crypto Standards alone will not be sufficient to address certain industry practices or bad actors. Crypto Standards should be overlaid with clear regulatory requirements for very strong consumer protections. Setting aside the question of which federal financial regulatory agency should have primary authority over crypto, the key question then is which consumer protections should be applied. To answer this question, the authors evaluated existing regulatory statements, reports, principles, and rules related to consumer protection across four major geographic regions and the four largest international standard-setting bodies.⁸⁵ We also unpacked consumer protections enshrined in recent U.S. legislative proposals related to crypto.⁸⁶

In our assessment, we synthesized the following high-level consumer protection themes to be included in clear national crypto regulation:

- Crypto issuers should be required to act honestly, fairly, and professionally, and identify, prevent, manage, and disclose conflicts of interest. There should be a mechanism for managing customer complaints.
- Crypto issuers should be required to set forth and maintain disclosures. Such disclosures should include information on rights, risks, reserves, redemption, lending arrangements, rehypothecation policies, fees, and dispute resolution processes.
- Crypto issuers should be required to maintain and disclose

84. It is worth noting that another potentially important component of a comprehensive policy framework is private law solutions to certain crypto issuers practices including those related to limited terms of service. *See* Bruce et al., *supra* note 51 (manuscript at 53–64) (describing private law remedies to protect coinholders from the risk of stablecoins).

85. *See* discussion *supra* note 23.

86. The authors evaluated two significant and recent legislative proposals from the U.S. Senate: the Responsible Financial Innovation Act, S. 4346, 117th Cong. (2022), and the Digital Commodities Consumer Protection Act, S. 4760, 117th Cong. (2022).

governance, processes, and procedures for decision-making around freezing, clawbacks, and blacklisting, among other practices.

- Crypto issuers should clarify how customer assets will be treated in bankruptcy or insolvency, consistent with relevant customer protection rules and pursuant to the appropriate order of priority in bankruptcy.
- Crypto issuers should provide transparency into the technology powering the crypto asset and provide timely notice and disclosure of any updates or material source code version changes related to the crypto asset.

Practically speaking, it may be some time before there is clear legislative designation of a single federal financial regulatory agency having full jurisdiction and enforcement authority over crypto. In the absence of such designation, the supervisory framework will continue to be fragmented. But even if this legislative designation were to take place, other non-financial regulatory agencies will continue to have relevant and important authority.

Also, even with the explicit specification of the aforementioned consumer protections, fragmentation would continue to be problematic, given the speed of innovation and vast decentralization of crypto. To the fullest extent possible, consumer protections should be consistent across industry and jurisdiction. Therefore, we also strongly urge a robust interagency rule-making process to make crypto protections for users consistent across national regulatory systems.⁸⁷ Such a rule-making process is essential to ensure that regulatory gaps do not detract from essential consumer protections. In the final analysis, standard setting in crypto combined with a thorough and consistent federal financial regulatory framework as well as thoughtful global standards can effectively set the stage for effective consumer protections and responsible long-term innovation in the crypto space.

V. GLOBAL STANDARD SETTING

The third pillar of our approach to cryptocurrency regulation is global standard setting. Differences in national approaches to regulation make it difficult for businesses to develop internationally as well as for governments to enforce their domestic rules. This is especially true for cryptocurrency, where regulation is fragmented, and opportunists may look to circumvent

87. One clear example of federal financial regulatory interagency rulemaking was the implementation of the Volcker Rule, 12 U.S.C. § 1851 (2018). The authors recommend learning from most positive and negative lessons gleaned from that process, before embarking on crypto rulemaking.

rules. Global standards are therefore important to achieve clear, consistent, and comprehensive regulatory frameworks. While global standards do not carry the force of law, the development process can result in buy-in by national governments that increases the probability of successful adoption. An in-depth analysis of the global standard setting process is best saved for another paper; suffice to say, the process can be arduous—but it is well worth the effort. Essential ingredients of international standard setting include transparency, openness, deliberation, and participation. Finally, equally important to global standard setting is the adoption and implementation process.

CONCLUSION

Cryptocurrency regulation is a critical policy issue that necessitates industry, national, and global action. The rapid pace of change and complexity of business practices require careful consideration and deliberate measures. The authors therefore propose a comprehensive three pillar approach to cryptocurrency regulation comprised of industry standards, national regulation, and global standard-setting.

Because there may not be a central entity or traditional intermediary to regulate for many stablecoins, we propose a first pillar of cryptocurrency regulation: establishing new “Crypto Standards” that could be applied across the burgeoning web3 landscape. Crypto Standards offer many benefits, including progress towards public policy goals of consumer protection and financial stability, as well as tools to promote interoperability, security, and responsible technological innovation.

While Crypto Standards offer many benefits, standards alone are not sufficient to address all of the practices discussed in this paper. We therefore propose a second pillar of cryptocurrency regulation: an additional national overlay of very strong investor and/or consumer protections, as absolutely necessary to address activities in this space. This national overlay should encompass five consumer protection themes that we discuss in this paper, and regulatory consistency and cooperation should be achieved through a federal interagency rule-making process.

The third pillar of this comprehensive approach is international standard-setting. International standard-setting is essential to achieving cooperation and collaboration between jurisdictions on the investor and consumer protections mentioned herein. While standard-setting can be a long and arduous process, it is imperative to achieving long-term efficacy in cryptocurrency regulation. All together, these three pillars (Crypto Standards, national consumer protection regulation, and international

standard-setting) can provide a comprehensive approach to investor and consumer protection in cryptocurrency.