AFR Americans for Financial Reform

Department of Financial Protection and Innovation
Attn: Legal Division
2101 Arena Boulevard
Sacramento, CA 95834

January 12, 2024

Dear Colleagues,

Thank you for the opportunity to submit written informal comments in anticipation of DFPI's formal rulemaking process that will implement the Digital Financial Assets Law (DFAL).

Americans for Financial Reform (AFR) is a national, nonpartisan, nonprofit coalition of more than two hundred civil rights, community-based, consumer, labor, small business, investor, faith-based, civic groups, and individual experts. We fight for a fair and just financial system that contributes to shared prosperity for all families and communities.

In our view the passage of DFAL presents a potential opportunity for California to prioritize investor and consumer protection for individuals who have invested in or maybe exposed to the risks present in the crypto assets marketplace.

Despite many claims by crypto industry players, the crypto industry has failed to demonstrate meaningful or viable use cases for crypto assets which prove industry claims that crypto will transform finance and boost financial inclusion. Instead, what we've observed is an industry whose business model is often built on forms of 'predatory' financial inclusion, which mirror many of the risks and harms present in the existing financial system. As such, there needs to be real and immediate action by policymakers to support consumers and investors harmed by their exposure to crypto assets and to prevent future harms as well.

At a bare minimum, there needs to be robust oversight and accountability for crypto assets, actors, and activities. A key factor contributing to the risks and harms crypto assets present is the lack of comprehensive regulatory frameworks and supervision of the industry at the federal and state level. That framework should be consistent with the standards found elsewhere in the financial system; a more permissive regulatory framework crafted in the name of the industry's so-called innovative potential at best would fail to provide adequate protections for consumers and at worst could legitimize poor practices within the industry, increasing chances that future crypto-related scams and volatility would have much broader impact than the recent crypto crash.

States like California have an important role to play in both providing such oversight and protection. In recent months, federal regulators have taken action to curb risks and harms found throughout the industry, as well as other state regulators. We and many other national advocacy organizations believe that federal regulators largely have the tools and statutory frameworks in place to effectively regulate the crypto industry, and they should continue to use such tools to provide consumer, investors and markets with the safeguards and guidance needed.

But, to the extent federal policymakers continue to debate whether and to what extent additional legislation is needed to enhance or clarify such a framework, states can in the meantime play a

leadership role in providing regulatory oversight and accountability. It is also important for states to act because the opposite can be true. Other states have chosen to provide more lax regulatory standards for the crypto industry. Without leadership at the state level, weak state regulatory standards can create a race to the bottom, where bad actors in the crypto sector will seek out state with such lax standards.

As such, we offer the following points of analysis as context to inform how the Department and other stakeholders approach implementation of this new law.

1) Crypto assets and markets pose significant risks and harms to consumers, investors, and financial markets.

Crypto industry advocates claim that by deploying a blend of cryptography and distributed ledger technologies, tech firms can create and offer digital asset-based products and services to consumers with less or no reliance on either regulatory agencies or traditional financial institutions as intermediaries. The logic is that this use of these technologies to 'disrupt' the financial sector will bring new opportunities and benefits. On the investment side, crypto has been marketed as a tool for wealth creation that lowers the barriers to entry for individuals often marginalized by the traditional financial system. On the consumer side, the industry claims crypto can support payment and banking services that are faster, cheaper, more reliable, and more secure than existing systems.

The main problem with these claims is that they generally don't match the reality of crypto markets. Instead, crypto markets are largely vehicles for speculative investment, appear rife with scams and fraud, and due to lack of adequate regulation, many crypto market participants lack the basic types of consumer and investor protection measures found in traditional finance.

- The FBI's Internet Crime Complaint Center (IC3), which receives reports of internet crime and analyzes related data, found that in 2022 cryptocurrency-related investment fraud reported to the FBI amounted to $2.57 billion in 2022, an increase of a whopping 183% from the previous year ($907 million), and amounted to more than **two-thirds of all internet investment scam losses reported in 2022** (a total of $3.31 billion), and more than one-fifth of all reported online fraud losses ($10.3 billion).[1]
- Meanwhile, according to crypto market data analysis, consumers and investors lost the equivalent of $**7.8 billion dollars to cryptocurrency scams alone in 2021**, up 82% from 2020. This same data reported that the equivalent of $3.2 billion in crypto assets were lost to theft in 2021, a staggering 516% increase compared to 2020.[2]These figures have only increased in 2022.
- Furthermore, Americans reported a record $1 billion lost to cryptocurrency scams to the Federal Trade Commission (FTC) in 2021, which is 60 times higher than the amount lost in 2018. Per the data, crypto related scams accounted **for one-quarter of all dollars lost to fraud reported to FTC during this period, more than any other type of scam.**[3]
- Finally, for the year 2021 the Better Business Bureau (BBB) ranked cryptocurrency scams as the second riskiest type of scam reported to the bureau. Although they only made up 1.9% of scams

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[2] https://go.chainalysis.com/2022-Crypto-Crime-Report.html
[3] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

reported to the BBB, the median victim lost $1,200, and 66% of people targeted by this scam reported losing money.[4]

Second, crypto can be employed in scams or fraud in several ways. It can serve as the means of payment for another crime (such as ransomware attacks), as an asset that is itself stolen (through hacks or physical theft of cold wallets), as a ruse for an related affinity fraud (such as romance scams), or as the core feature of a fraud scheme (e.g., such those investors who had assets in custody with FTX, only to find their deposits allegedly stolen by the platform's operators). These overlapping schemes, fueled by crypto's unique attributes (such as pseudonymity, wash trading, etc.) as well as lack of adequate regulatory oversight, suggest the footprint of harm is even larger than these figures indicate.

Lastly, these figures don't fully capture the loss of crypto assets through crypto's infamous volatility, instability, and significant market failures. We have some indication of the volume of that loss: at its height in early 2022, the market capitalization of crypto markets was estimated to be more than $3 trillion in value. Subsequent losses in value tied to the failure of Terra, Celsius, Voyager, FTX, crypto hedge fund 3AC and other crypto platforms are estimated to be more than $2 trillion.[5] And, the failure of additional firms in the near future seems likely as well.

Much has been made of Americans' interest in cryptocurrency. A NBC News poll from March 2022 found that one in five adults in America report having invested in, traded, or used cryptocurrency, and subsequent polls have captured similar figures, often noting that African-American or Latinx consumers report having participated in crypto investing in numbers greater than their White counterparts.[6] Yet, a poll conducted just months later by Pew Research Center in August 2022 showed that 46% of poll respondents reported their crypto investments performed worse than they expected – and this was before collapse of FTX and other platforms.[7] One market research firm estimated that an investor that bought $1,000 worth of Bitcoin (BTC) just after the flurry crypto related Super Bowl ads in February 2022 would have owned $513.22 worth of BTC a year later in 2023 (soon after the FTX collapse) – a loss of 48.7%.[8]

Recent price increases in Bitcoin (BTC) notwithstanding, this example underscores the volatility and risk involved in crypto investing – risk that traditionally wealthy investors might be able to weather, but which is borne much harder by investors with low incomes and/or are from communities of color, who are more likely to lack wealth or other resources to absorb such losses.

Moreover, crypto platforms have largely failed to demonstrate lasting value in the payments space. Most crypto activity is focused on speculative investment activities. Crypto-derived payment platforms have struggled to demonstrate viable mainstream use. Stablecoins, which were initially created with the intention of being used to facilitate crypto payments outside crypto platforms, are still largely used for

[4] https://bbbfoundation.images.worldnow.com/library/259c7333-0fb3-4bc0-a059-4b116594c473.pdf

[5] https://www.cnbc.com/2022/12/23/bitcoin-lost-over-60-percent-of-its-value-in-2022.html. Note: estimates of crypto market values, market capitalization, etc., vary and are not well defined.

[6] https://www.cnbc.com/2022/03/31/cryptocurrency-news-21percent-of-adults-have-traded-or-used-crypto-nbc-poll-shows.html

[7] https://www.pewresearch.org/fact-tank/2022/08/23/46-of-americans-who-have-invested-in-cryptocurrency-say-its-done-worse-than expected/

[8] https://www.benzinga.com/markets/cryptocurrency/23/02/30880044/if-you-invested-1-000-in-bitcoin-after-super-bowl-lvi-aka-the crypto-bowl-heres-how-much-y

speculative investment and rely on fiat currency and legacy financial institutions to facilitate off-chain transactions for goods and services.

Stablecoins have also demonstrated real fragility; famously, in the case of the collapse of Terra, the algorithmic stablecoin whose collapse (and likely fraud) precipitated the larger collapse of crypto markets beginning in May 2022. But even stablecoins perceived as more 'stable' such as Circle and Tether have faced so-called 'depegging' events, which at a minimum suggest stablecoins operate more in a manner like loosely regulated money market funds than as an actual "currency" or "bank deposits."

Meanwhile, crypto platforms themselves often charge high fees for buying, selling, or exchanging crypto on or off platforms. The famed speed of cryptocurrency's clearing and settling abilities is belied by the fact that the consensus mechanisms used to verify blockchain transactions are infamously slow – processing a very small number of transactions per second, especially in comparison to existing payments systems, which can process tens thousands of transactions per second.[9]Attempts to speed up these processes – by creating extra layers of code on top of an existing blockchain, or by creating off-chain software solutions – create significant security risks for individuals engaging in such transactions, and also defeat the purpose of using the blockchain's 'immutable' properties to provide security for such transactions.[10]

Blockchain proponents often argue that the technology is still in the "early days" of its development. This claim is used either offensively – to suggest that the technology offers significant unrealized potential benefits that will emerge in the near future – or defensively, to explain why the consistent failures of blockchain-based technology are not indicative of its enduring limitations but constitute "growing pains" that are a natural and necessary phase in the technology's development.

A relatively well-known essay by Molly White, a software programmer and noted critic of crypto assets and blockchain, entitled, "It's not still the early days" lays out the basics of a rebuttal to this argument.11In summary, White points out that Bitcoin was launched in 2009; Ethereum in 2015. Many first generation and second generation blockchain applications are anywhere from 7-13 years old. During that same time range, numerous other technological products, and platforms (some new, some established) have been further developed and achieved stable, widespread use more rapidly. These products include things as varied as major social media platforms, online ride-sharing apps and platforms, new computer processors, new database programs, programming languages, operating systems, payment apps, and more.

While the nature of these innovations varies widely (and bring with them their own variety of benefits and negative externalities, some of which are profound in scope and are a core focus of other advocacy efforts), what they have in common is that arguably, they have all demonstrated their relative utility, scalability, and viability in a relatively short period of time. In contrast, crypto and

[9] https://crypto.com/university/blockchain scalability#:~:text=The%20Transaction%20Speed%20of%20Cryptocurrencies&text=While%20Visa%20can%20process%20up,capability%2 0to%20achieve%20mass%20adoption.
[10] https://coingeek.com/the-unsecure-lightning-network-as-btc-layer-2-scaling protocol/#:~:text=Inefficiency%20and%20noncompliance%20with%20the,is%20the%20pretense%20and%20untruth
[11] https://blog.mollywhite.net/its-not-still-the-early-days/

blockchain products have not demonstrated nearly the same levels of uptake within a similar time frame.

2) Crypto assets, actors, and activities lack adequate regulatory oversight and related consumer and investor protections.

Traditional financial regulatory frameworks require a set of minimum standards and protections for firms to operate. On the investing side, exchanges, broker-dealers, and issuers of securities must register with regulators and provide significant information about the nature of their business or product offering, managerial structure and composition, financial statements, potential conflicts of interest, and more. Once registered, these actors must provide disclosures on an ongoing basis to investors and regulators and must abide by a host of anti-fraud and market manipulation rules, as well as rules intended to ensure that such actors are operating in the best interests of their clients – such as fiduciary duty or best execution rules. Often, such standards require firms to disaggregate their operations to avoid perpetuating conflicts of interest and mitigate the possibility of insider trading or front running.

On the banking and payments side, banking and consumer financial protection rules require a host of regulatory measures, prudential supervision and examinations, anti-money laundering compliance standards, capital requirements, fair lending disclosures and policies, payment dispute resolution requirements, and many other measures that ensure the companies and actors in this space have some minimum standard of oversight and that consumers have both protections and recourse should plans go awry.

None of these regimes are perfect; regulators can still fail to adequately enforce these standards and bad actors are still able to skirt, evade or undermine them. However, they represent over a century of lessons learned from past financial crises and schemes and serve as a reliable means of preventing financial risk and harm and protecting consumers, investors, and markets when such harm occurs.

Unfortunately, very little of the crypto industry is currently held to or meets these same standards. Most crypto firms register at the state level under money transmitter or money service business licensing regimes that, with some exceptions, usually do not offer the same level of consumer and investor protections as outlined above. Many crypto platforms are structured such that their services are aggregated or vertically integrated, with the platforms providing their clients asset custody services, brokering, market making, and more – conditions which all too often can lead to exchanges misusing or abusing these overlapping roles to benefit at their clients' expense. Crypto firms have shown difficulty in providing safe and secure custody of their client's assets. These assets are generally not protected by either deposit insurance programs or securities investor protection programs.

Additionally, many firms have failed to segregate such assets to protect them in the event of insolvency. As a result, many of the clients of firms such as Celsius, Voyager and FTX are all ensnared in lengthy and complex bankruptcy proceedings, waiting in the back of the line behind other creditors with little hope of reclaiming the full value of their assets. Meanwhile, stablecoin issuers who claim that the coins they are issue are fully collateralized, redeemable in full on demand, have often either failed to meet these standards or have operated under a cloud of questions and uncertainty about the quality and quantity of their collateral and their ability to honor on demand redemption agreements.

Claims by proponents of so-called decentralized finance (DeFi) that their platforms avoid these conflicts of interests and potential misdeeds by avoiding reliance on intermediaries and rely instead on the so-called transparency of the blockchain and smart contracts should be considered wishful thinking. In addition to the potential cybersecurity risks posed by smart contracts developed via open-source code, even decentralized platforms are prone to centralization in one form or another.

For example, as of January 2023, two mining pools controlled 51% of Bitcoin's hash rate (with similar levels of concentration found on other chains);[12] 66.7% of all crypto trading on centralized exchanges (which themselves constitute the bulk of all crypto trading) now occurs on Binance;[13] and as of July 2022 one analysis determined that .04% of BTC addresses (or wallets) held 62.25% of all Bitcoins issued.[14]

Other sources have offered confirmation of this ongoing trend of centralization - for example, a recent *Wall Street Journal* article revealed how a group of roughly half a dozen coders "serve as stewards of Bitcoin Core, an open-source program that keeps the cryptocurrency's digital ledger up-to-date on thousands of computers that make up its network."[15] Meanwhile, many of the decentralized autonomous organizations (DAOs) that are meant to provide governance or oversight of decentralized blockchain platforms exhibit similar levels of concentration, with a small number of wallets controlling a disproportionately high number of so-called governance tokens.

It's not clear if true decentralization could achieve a level of transparency and security that would protect consumers and investors in a meaningful way without the need for intermediation by regulators – we're skeptical that would be the case. But, regardless, what does seem to be true is that these platforms struggle to achieve the decentralization they claim drives the immutability, security, and transparency that blockchain platforms are supposed to provide.

3) State laws that require robust regulatory oversight and accountability for the crypto industry can help provide consumer and investor protection and complement or go beyond federal regulatory standards.

Federal regulators have taken several recent actions to respond to the crypto crash and draw bright lines regarding the risks that crypto assets pose to consumers and investors. In January 2023 the Fed, OCC and FDIC issued a "Joint Statement on Crypto-Asset Risks to Banking Organizations."[16] The statement laid out in clear detail how the unique properties and risks posed by crypto assets may be incompatible with the safety and soundness standards banking institutions must meet. Meanwhile, the Securities and Exchange Commission, after making many public statements indicating their clear view that most crypto assets are securities and those offering them should seek registration with the SEC, has ramped up enforcement of traditional securities laws. The SEC's legal track record in this regard is largely sound – as of January 18, 2023, the SEC had brought 127 crypto related enforcement actions

[12] https://cryptoslate.com/behind-the-two-mining-pools-controlling-51-percent-of-the-global-hash-rate/
[13] https://cryptonews.com/news/binance-has-grabbed-two-thirds-of-all-crypto-trading-volume-what-happened-to-the-decentralization of-finance.htm
[14] https://cointelegraph.com/news/hodlers-and-whales-who-owns-the-most-bitcoin-in-2022
[15] https://www.wsj.com/articles/bitcoin-core-maintainers-crypto-7b93804
[16] https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf

without losing a single case.[17] More recently, the SEC's regulatory strategy has both upheld and challenged by disparate rulings in federal courts. Those cases do have some bearing on jurisdictional questions, but do not outweigh this larger body of consistently successful enforcement actions and decisions.

There are many other examples, but the pattern is clear – existing banking, securities and consumer protection regulations are relevant to crypto asset and activities and should be applied consistently and robustly to provide consumers and investors with comparable levels of protection. As the mantra goes, financial firms offering the same types of services or activities, with the same risks, should be subject to the same rules and same supervision.

Yet, on almost every front, the crypto industry has argued the technological infrastructure used to create their products and offer their services makes them fundamentally different, and either have rejected application of existing regulatory frameworks or advocated for frameworks that provide them with special exceptions, which not only risks establishing overly permissive standards but, in many cases, may erode regulatory standards across the financial industry.

For example, crypto industry advocates have objected to equivalent treatment under federal tax reporting laws,[18] federal anti-money laundering laws,[19] sanctions compliance,[20] securities registration,[21] supervision as payment providers,[22] consumer protection requirements such as dispute resolutions and chargebacks (such as those offering under EFTA and other federal statutes) and more.[23]

In a similar vein, they've advocated for crypto regulatory frameworks that would exempt blockchain developers, admins, validators and miners from any real substantive regulatory obligations, despite their clear involvement as intermediaries in financial activity.[24] They've advocated for permissive regulatory standards for stablecoin issuers that allow such issuers to, like many non-bank entities before them, receive the privileges that banking institutions receive under federal law without commensurate oversight and regulatory obligations.[25] And, they've advocated at the federal level for crypto market regulatory proposals that would use decentralization as justification for exemptions from a range of standard securities-based regulatory measures – which would not only

[17] Cornerstone Research, "SEC Tightens Cryptocurrency Enforcement," January 18, 2023, https://www.cornerstone.com/insights/press releases/sec-tightens-cryptocurrency-enforcement/; John Reed Stark, "Why 'SEC Regulation by Enforcement' is a Bogus Big Crypto Catchphrase," LinkedIn, January 23, 2023. https://www.linkedin.com/pulse/why-sec-regulation-enforcement-bogus-big-crypto-john reed-stark/?published=t.
[18] https://www.coindesk.com/consensus-magazine/2023/11/14/what-the-irs-gets-wrong-about-defi-and-crypto-in-its-latest-tax-reporting-proposal/
[19] https://www.americanbanker.com/opinion/a-new-anti-money-laundering-paradigm-is-needed-for-digital-wallets
[20] https://www.theblock.co/post/233000/crypto-policy-tornado-cash-sanctions-legal-brief
[21] https://blog.kraken.com/news/kraken-continues-to-fight-for-its-mission-and-crypto-innovation-in-the-united-states
[22] https://www.defieducationfund.org/_files/ugd/84ba66_4bdb18a7e1b94bfea406dfbb0a0ffcc8.pdf
[23] https://news.bitcoin.com/blockchain-association-rebuffs-cfpbs-proposal-on-payment-apps-and-digital-assets/
[24] https://digitalchamber.org/blockchain-regulatory-certainty-act-statement-of-support/
[25] https://theblockchainassociation.org/blockchain-association-announces-principles-for-stablecoin-legislation-and-urges-congressional-action/

risk leaving crypto investors with fewer protections but could upend existing securities laws and safeguards for non-crypto investors, financial products and services providers.[26]

This is part of a broader pattern: fintech firms and even traditional financial firms often claim that the technological innovations they offer require a soft touch from regulatory agencies in order to avoid stifling these new supposedly transformative offerings. Yet, in the experience of consumer advocacy organizations like AFR, the innovation that is being offered by these firms is all too often a form of regulatory arbitrage, rather than a product that offers meaningful benefit to consumers, and that their calls for soft touch 'regulation' are in fact deregulatory in all but name.

Real innovation benefits from sound and robust regulatory standards, which rewards innovators who can meet such standards. Private sector firms have a role in producing products and services they believe can provide real value while generating returns for firms and investors. Regulators have a different role: ensuring that such firms, products, and services operate in a way that avoids harming consumers, investors, communities, and markets while providing real and lasting benefits to the same.

It is important for States to act to protect consumers and investors from the clear risks and harms found within the crypto sector. Those that do take such action are able to make a meaningful difference, especially given that there is still debate in Washington about the scope and nature of the federal regulatory framework for digital assets across the board. Those that do not, or seek more permissive regulatory frameworks for digital assets, run the risk of becoming a haven for risky or predatory practices we have seen throughout this industry – and could undermine more effective regulatory standards at the federal level as well.

Thank you for taking the time to review these comments. We hope the Department takes these points into consideration as it initiates its formal rulemaking process and look forward to contributing to this process once it begins.

Sincerely,

Mark Hays
Senior Policy Analyst
Americans for Financial Reform

[26] https://cryptoforinnovation.org/wp-content/uploads/2023/07/CCI-Letter-of-Support-H.R.4763-Financial-Innovation-and-Technology-for-the-21st-Century-Act-2.pdf