Testimony of Jonah Crane
Maryland Consumer Protection Commission
June 5, 2018

Thank you to the Commission for inviting me to share my views on issues related to cryptocurrencies, initial coin offerings (ICOs), cryptocurrency exchanges, and other blockchain technologies.

I am an advisor to financial technology companies, Regulator in Residence at the FinTech Innovation Lab in New York, Executive Director of the RegTech Lab in Washington, D.C., and co-author of a forthcoming paper on blockchain technology with Commission Chairman Gary Gensler, among others.[1] Prior to January 2017, I was Deputy Assistant Secretary and a Senior Advisor at the U.S. Treasury Department. Before joining the Treasury Department I was a senior policy advisor to Senator Chuck Schumer of New York, where I advised Senator Schumer on the Dodd-Frank Act, JOBS Act, and other financial services and economic policy issues.

I appreciate the opportunity to testify in front of this Commission on a such a timely and important topic. Given the sheer dollar figures involved, it is critical that policymakers closely examine issues related to virtual currencies and ICOs, and take appropriate actions to protect investors and consumers. This Commission is uniquely well-suited to conduct a comprehensive and thorough analysis, identify all of the tools available to state authorities to protect Marylanders, and help to coordinate a regulatory response that makes efficient use of all available resources to maximize investor and consumer protection.

Introduction

It is often said that we must strike a balance between regulation and innovation. Structuring a regulatory framework certainly involves tradeoffs, and some choices may better facilitate innovation and competition than other choices. However, that framing implies a false choice: That we must choose between *either* regulating to protect consumers and investors *or* allowing innovation to flourish. In financial services and other industries where trust and confidence are central to well-functioning markets, a sound regulatory foundation is critical.

That does not mean that we shouldn't work hard to craft the right regulatory framework, or that regulation doesn't need to adapt as technology evolves. But we don't need to reinvent the wheel for every new vehicle. We generally regulate financial activities (payments, lending, insurance, securities issuance) rather than particular technologies. This functional approach, when applied

[1] The views expressed herein are mine alone, and do not represent the views of any of my clients or any other organization with which I am affiliated. I have no financial interest in any digital currency, or any blockchain-related business.

to blockchain technology, would look first at which activity is being facilitated by the technology, and seek to apply the existing rules to the extent possible.[2] Ideally, the rules would establish a level playing field for all those engaged in the same activity--no matter their choice of technology. Policymakers should be guided by their regulatory and policy objectives. We must always ask, regardless of the technologies involved: what risks are we seeking to address via regulation, and what rules are necessary to address those risks--to consumers, investors, or the broader system?

There are complicated questions about the appropriate regulatory framework for various activities involving blockchain technology and cryptocurrencies, and these questions may take some time to sort out. However, given the amount of money raised to date, and the access ordinary investors and consumers have to many cryptocurrencies, regulators should prioritize investor and consumer protection using all available tools under existing authorities and interpretations.

State regulators and other legal authorities can play several important roles with respect to cryptocurrencies, ICOs, and related blockchain-technology issues. I recommend that Maryland regulators and policymakers focus on the following areas:

- First, enforce existing state laws in cases where they clearly apply, and examine the need to adapt state-level regulations in light of technological changes. In the case of cryptocurrencies, state money-transmission laws provide important protections to consumers transferring money outside the regulated banking system, and many types of cryptocurrency transactions likely are--or should be--covered by those laws.

- Second, state regulators can act as force multipliers for federal regulators. States have an important role to play both as front-line cops on the beat and as reinforcement for federal authorities. State-level enforcement can be an effective supplement to federal efforts either when federal regulators step back from properly enforcing the law--which I do not believe to be the case in cryptocurrencies, though it may be elsewhere, as this Commission has pointed out[3]--or where there is simply a need for more resources.

---

[2] Kevin Tu & Michael Meredith, Rethinking Virtual Currency Regulation in the Bitcoin Age, 90 Wash. L. Rev. 271, 276 (2015) ("examining the regulatory objectives advanced by existing laws, as applied to virtual currency, provides valuable supplementary guidance to policymakers in the ongoing process of developing an appropriate legal framework").

[3] See Maryland Consumer Protection Commission, Interim Report, January 26, 2018, *available at* http://dls.maryland.gov/pubs/prod/NoPblTabMtg/MdFinProtCmsn/2017-Interim-Report.pdf (hereinafter "Interim Report").

- Third, state consumer protection laws, including prohibitions against unfair and deceptive acts and practices (so-called "UDAP" authority) and general anti-fraud laws can also be used to protect consumers. These authorities should be used in cases where consumers have been misled and the application of other laws is unclear, thereby protecting consumers without allowing "bad cases" to make bad law.

- Fourth, in areas like data privacy there may be important gaps for state regulators to fill, and blockchain technology may complicate basic protections for consumers related to their identities and personal data such as credit reports.

- Finally, explore the potential to participate in a multi-state regulatory sandbox to facilitate live pilot testing of both blockchain-related and non-blockchain products.

In each area, coordination will be the key to effectiveness: coordination among the state-level authorities, coordination with other states' regulators, and coordination with federal authorities. This Commission, composed of a broad cross-section of stakeholders, is uniquely well-suited to facilitate coordination. If the Commission itself is not extended beyond its initial term, I would recommend that a similarly-inclusive council be assembled and tasked with coordinating efforts across the relevant authorities.

The remainder of my testimony provides additional background and detail on each of the recommendations.

1. Money transmission laws

The complexity of the state money-transmission licensing regime is often cited as an obstacle to innovation in payment services in the United States. Increased uniformity of state money transmission laws could have beneficial effects for a broad cross-section of FinTech payments companies. Payments is inherently a network industry, from which users would derive little value if they cannot make payments across state lines. A 2016 report on the regulation of money services businesses noted rapid growth in the number of state licenses for money transmission, but fewer independent companies.[4] In other words, the industry was consolidating precisely to facilitate multi-state activity. Greater streamlining of state licensing processes and substantive

[4] See Conf. of State Bank Regulators & Money Transmitter Regulators Ass'n, The State of Money Services Businesses Regulation & Supervision, May 2016, *available at* https://www.csbs.org/sites/default/files/2017-11/State%20of%20State%20MSB%20Regulation%20and%20Supervision%202.pdf.

requirements would also diminish the desire for a federal alternative such as the Office of the Comptroller of the Currency's proposed special purpose charter.[5]

However, the complexity of the state-by-state licensing regime is not unique to virtual currency or blockchain-related businesses--all companies working on innovative payments solutions face the same complexity. More important than uniformity or licensing reforms for digital currency-related activities, is increased clarity about which activities are subject to money-transmission laws to begin with.

Maryland regulators should review the state's money transmission statute, with a focus on which virtual currency activities present the risks the statute is designed to address, and clarify activities are subject to those rules.

State money transmission laws are, above all else, designed to protect consumers from the risk that those entrusted with taking possession of a consumer's money for the purpose of transferring it in accordance with the customer's instructions, fail to do so.[6] State laws generally protect against the risk of fraud by requiring applicants to submit to background checks, and protect against the risk of loss of the customer's funds by imposing certain prudential requirements such as minimum capital requirements or the posting of a surety bond. Many states exempt so-called "agents of the payee" even where the agents come into possession of funds, because they typically receive funds as an agent for a merchant with whom they have a long-term contractual relationship.

Virtual currencies and other peer-to-peer payment networks raise the question of whether money transmission laws should apply in cases where the intermediary never takes custody of the funds. However, because transacting directly in virtual currencies is complex, most retail users currently access virtual currencies through digital "wallets" and other service providers, who facilitate purchases and sales on cryptocurrency exchanges. As discussed below in Section 3, it may be possible to protect consumers even where money transmission laws do not apply, but policymakers should review money transmission laws and clarify which virtual currency activities are covered.

Guidance issued in 2013 by the Treasury Department's Financial Crimes Enforcement Network (FinCEN) may provide a useful starting point. FinCEN issued guidance regarding the application

---

[5] See Office of the Comptroller of the Currency, Exploring Special Purpose National Bank Charters for Fintech Companies, December 2016, *available at* https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf.

[6] See https://www.law.ua.edu/pubs/lrarticles/Volume%2065/Issue%201/2%20Tu%2077-138.pdf.

of its regulations implementing the Bank Secrecy Act (BSA) to convertible virtual currencies, which it defined as currency that does not have legal tender status, and either "has an equivalent value in real currency, or acts as a substitute for real currency."[7] FinCEN determined that its regulations should apply to "exchangers" and "administrators" of virtual currencies, but not "users" who obtain virtual currency to purchase goods or services.

While FinCEN's guidance is a useful starting place for determining whether state money transmission laws should apply to virtual currency-related activities, it was designed to address specific policy goals--the prevention and deterrence of money laundering and other financial crimes. As noted above, state money transmission laws are generally designed to address different policy goals, principally consumer protection. Accordingly, policymakers should review the application of money transmission laws to virtual currency activities through the lens of their own regulatory objectives.

2. Securities Laws

In 2016, promoters and developers of projects--often but not always involving cryptocurrencies or blockchain technology--increasingly issued "tokens" or "coins" in what became referred to as initial coin offerings, or ICOs. In 2016, there were 43 ICOs, which raised a total of over $95 million.[8] The pace and size of offerings began to accelerate in the second quarter of 2017,[9] with many tokens being offered to the general public amidst an apparent belief by many of the issuers that U.S. securities laws did not apply.

The Securities and Exchange Commission (SEC) responded by issuing an investigative report on The DAO, a virtual, unincorporated organization that issued tokens to raise funds that were to be invested in projects chosen by token holders.[10] The SEC determined that the DAO tokens were securities, and therefore had been issued in violation of U.S. securities laws, but nonetheless declined to take any enforcement action. The SEC issued the report "to advise those who would use a ... distributed ledger or blockchain-enabled means for capital raising, to take appropriate steps to ensure compliance with the U.S. federal securities laws."[11]

---

[7] See FinCEN, FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013, *available at* https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[8] See Coinschedule, https://www.coinschedule.com/stats.html?year=2016.

[9] See Coinschedule, https://www.coinschedule.com/stats.html?year=2017.

[10] Securities and Exchange Commission, Release No. 81207, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, July 25, 2017, *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf.

[11] *Id.* at 2.

In many ways, this was a remarkable step for an enforcement authority to take. Rather than bring an enforcement action, the SEC described at length how it would apply "fundamental principles" of securities law to "a new paradigm." The DAO report was not just a shot across the bow--though it was certainly that--is was also a guide to how the SEC would analyze cryptocurrencies or tokens to determine whether they should be deemed securities and thus subject to U.S. federal securities laws.

The SEC was rewarded for its thoughtfulness, forbearance, and transparency with a flood of ICOs. Issuance dipped slightly in the month following the report, but continued to accelerate thereafter, with over a billion dollars being raised via token sales in December alone.[12]

The SEC has brought several enforcement actions since issuing the DAO report, including cases where the organizers used celebrity endorsements to promote the offering, or promised guaranteed returns to early investors.[13] Several cases have involved outright fraud, such as promising the first-ever real estate-backed token when no such operations existed,[14] or falsely claiming to have agreements with Mastercard and Visa to issue "crypto credit cards."[15]

Several large token offerings that took place following the issuance of the DAO report took the guidance therein to heart, complying with the conditions for one of the available exemptions from registration.[16] Kodak, which announced an ICO for its own photo-sharing site, put the offering on hold to verify the accredited investor status of the purchasers,[17] eventually restructuring the offering as a private placement pursuant to Regulation D.[18] However, numerous ICOs have since been conducted without issuing a prospectus or qualifying for an exemption, leading SEC Chairman Clayton and other SEC staff to increase the strength of their warnings in

---

[12] See Coinschedule, https://www.coinschedule.com/stats.html?year=2017.
[13] See *Securities and Exchange Commission v. PlexCorps, et al.*, Civil Action No. 17-cv-07007 (E.D.N.Y., filed Dec. 1, 2017).
[14] See *Securities and Exchange Commission v. REcoin Group Foundation, et al.*, Civil Action No. 17-cv-05725 (E.D.N.Y., filed Sep. 29, 2017).
[15] See SEC Halts Fraudulent Scheme Involving Unregistered ICO, April 2, 2018, *available at* https://www.sec.gov/news/press-release/2018-53.
[16] See Protocol Labs Private Placement Memorandum, *available at* https://coinlist.co/assets/index/filecoin_index/Protocol%20Labs%20-%20SAFT%20-%20Private%20Placement%20Memorandum-bbd65da01fdc4a15219c49ad20fb9e28681adec9fae744c41cccd124545c4c73.pdf, and tZero Offering Memorandum, *available at* https://www.sec.gov/Archives/edgar/data/1130713/000110465918013731/a18-7242_1ex99d1.htm, both structured to be compliant with Regulation D and Rule 506(c).
[17] See Kodak Postponsed ICO to Verify 'Accredited' Status of 40k Potential Investors, *available at* https://cointelegraph.com/news/kodak-postpones-ico-to-verify-accredited-status-of-40k-potential-investors.
[18] KODAKCoin to Issue SAFT, Seeks $176.5 Million ICO, March 19, 2018, *available at* https://www.crowdfundinsider.com/2018/03/130496-kodakcoin-to-issue-saft-seeks-176-5-million-ico/.

speeches, testimony, and op-eds. The SEC has also issued warnings to investors, going so far as to launch a mock ICO that led to a record number of visits to its investor education website.[19]

The post-DAO offerings highlight the availability of an array of offering structures to token issuers. The Filecoin and tZero offerings, for example, relied on Reg D, the exemption for private offerings to accredited investors. Specifically, they relied on Rule 506(c) under Reg D, which was adopted pursuant to the JOBS Act to permit general solicitation of private offerings under certain conditions. Others have discussed the possibility of using so-called Reg A-plus,[20] also implemented pursuant to the JOBS Act, which permits public offerings up to $50 million if certain disclosure and accounting requirements are met.

So, what can state securities regulators do to protect investors and encourage compliance with federal and state securities laws? When it come to cryptocurrencies, there is no more apt call to action than the words of House Speaker Micheal Busch, in connection with the release of this Commission's Interim Report in January: "Now, more than ever, we need to devote more State resources to protecting Maryland consumers and not less."[21]

Just because a token offering should be deemed a security doesn't mean the SEC has exclusive jurisdiction and doesn't mean it will get around to bringing an enforcement case. The SEC is hard at work but with hundreds of ICOs in the past two years alone, the sheer volume may be overwhelming.

The SEC's entire budget for FY2019 is $1.652 billion, and the CFTC's less than $450 million.[22] These figures represent increases over prior years, but both agencies have been woefully underfunded ever since the financial crisis. The Division of Enforcement is the SEC's largest division, but has only about 1,350 staff to oversee $75 trillion in annual securities trading activity and over 26,000 registered firms.[23]

The SEC has made enforcement in the area of cryptocurrencies a priority, but at the risk of taking its eye off the ball in other much-needed areas. By taking on an increased role in enforcing securities laws--in cryptocurrency markets or elsewhere--state securities regulators can free up SEC resources across the board. I am mindful that this requires resources at the state level as

---

[19] See https://www.howeycoins.com/index.html.
[20] Reg A-Plus Is Perfect For Initial Coin Offerings, January 10, 2018, *available at* https://www.law360.com/articles/1000365/reg-a-plus-is-perfect-for-initial-coin-offerings.
[21] See Press Release, SENATE PRESIDENT, SPEAKER OF THE HOUSE, FINANCIAL CONSUMER PROTECTION COMMISSION ANNOUNCE RECOMMENDATIONS, January 26, 2018, *available at* http://dls.maryland.gov/pubs/prod/NoPblTabMtg/MdFinProtCmsn/Press-Release-01-26-2018.pdf.
[22] H.R. 1625, *available at* https://www.congress.gov/115/bills/hr1625/BILLS-115hr1625enr.pdf.
[23] See Securities and Exchange Commission, FY2019 Congressional Budget Justification and Annual Performance Plan, *available at* https://www.sec.gov/files/secfy19congbudgjust.pdf.

well. Coordination can reduce the amount of duplication and wasted resources, but there is no substitute for putting more cops on the beat.

State regulators can assist in educating and warning investors, as they did in January when they issued a bulletin warning investors of the risks of investing in cryptocurrencies.[24] In April, New York's Attorney General launched an inquiry into the activities of cryptocurrency exchanges.[25] And more recently, the North American Securities Administrators Association announced a broad, coordinated "sweep," covering 70 token offerings.[26] Securities regulators from more than 40 jurisdictions--including Maryland--participated in the sweep, which was described as the "tip of the iceberg." These are welcome actions.

While all or nearly all tokens issued to date appear likely to qualify as securities, difficult legal and analytical questions remain about whether certain tokens, or promises to deliver tokens in the future, are properly characterized as "securities" under applicable law. As some of the projects that have raised money via a form of token sale or pre-sale become operational, and those tokens begin to take on additional characteristics of a virtual currency,[27] the application of the *Howey* test will no longer be so straightforward.

All of the enforcement cases brought to date have involved offerings that appear to fall squarely within existing definitions of a "security." In other words, we haven't seen the "hard cases" yet. As every law student learns, hard cases can make bad law. However, those knotty, and to-date largely hypothetical, legal questions need not prevent regulators from protecting investors in these offerings. By using all available authorities, regulators may be able to protect consumers without resorting to those hard cases--at least the for time being.

It seems unlikely that this precaution would meaningfully limit the ability to protect investors. For one thing, the SEC has made clear that the vast majority of token offerings to date likely meet the *Howey* test and are therefore subject to the securities laws. So the universe of truly hard cases is likely narrow. For another, all of the enforcement actions to date have involved blatantly

---

[24] See Nat'l Ass'n of State Securities Regulators, NASAA Reminds Investors to Approach Cryptocurrencies, Initial Coin Offerings and Other Cryptocurrency-Related Investment Products with Caution, January 4, 2018, *available at* http://www.nasaa.org/44073/nasaa-reminds-investors-approach-cryptocurrencies-initial-coin-offerings-cryptocurrency-related-investment-products-caution/

[25] See Press Release, A.G. Schneiderman Launches Inquiry Into Cryptocurrency Exchanges, April 17, 2018, *available at* https://ag.ny.gov/press-release/ag-schneiderman-launches-inquiry-cryptocurrency-exchanges.

[26] See NASAA, State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown, May 21, 2018, *available at* http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/.

[27] The term "virtual currency," as used here, is intended to be used as defined by FinCEN in its 2013 guidance: a medium of exchange that is not legal tender, but has a value denominated in real currency and/or can be exchanged for real currency.

fraudulent activity, and therefore may be subject to broader anti-fraud or consumer protection laws, so that recourse to securities laws is not necessary to protect investors.

Finally, this Commission might also recommend to the Maryland Congressional delegation that they support the SEC in using its authority to issue no-action letters to begin to provide some certainty for market participants regarding acceptable practices. Eventually, the SEC may decide that new rules are necessary, but in the meantime no-action letters would encourage teams contemplating a token offering to proactively work with the SEC to ensure the offering is structured in a manner consistent with the securities laws. Using the no-action letter process would allow the SEC to determine the conditions on which cryptocurrency offerings could be conducted, while beginning to further define the scope of what is--or isn't--a security.

3. Consumer protection (UDAP) laws

State consumer protection laws, including UDAP authority, may be particularly useful in addressing risks to consumers in cases where the application of money transmission or securities laws is unclear.

For example, companies who facilitate peer-to-peer payments and do not hold customer funds may not be subject to prudential regulation of the sort applied to money transmitters. That does not mean those businesses should be completely unregulated--indeed, especially given the complexity of transacting in virtual currencies, consumers must be provided with clear and easy-to-understand disclosures regarding their transactions.

A recent Federal Trade Commission (FTC) settlement with Venmo is instructive. The FTC brought its action under its own UDAP authority under the Federal Trade Commission Act, alleging that Venmo misled consumers about the availability of funds when receiving payments from others via the Venmo app, and violated Gramm-Leach-Bliley's privacy and data security requirements.[28] This enforcement action was independent of Venmo's status as a money transmitter--indeed, the activity in question involved transfers between users' bank accounts facilitated by Venmo, not the users' own Venmo accounts. Similar authorities may be used to protect consumers from risks at businesses that facilitate virtual currency payments but do not take custody of customer funds.

---

[28] See Federal Trade Commission Press Release, PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act, February 27, 2018, *available at* https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

4. Data Privacy

There is no comprehensive framework for data privacy in the United States. Europe's General Data Protection Rule recently went into effect, establishing a comprehensive and uniform set of protections across the European Union. In the U.S., data privacy is protected primarily at the state level, and in the case of financial services under the Gramm-Leach-Bliley Act. Blockchains, which are pseudonymous but public ledgers of transactions, may raise unique issues with respect to the application of traditional data privacy rules.

Blockchain technology has the potential to create a more consumer-centric data regime--one where consumers control their own important data, and grant permission to use various attributes to third parties of their own choosing in exchange, presumably, for value. However, many of these potential solutions, based on the current state of technology, require heroic assumptions about the ability and willingness of consumers to manage their own data. Moreover, from a policy perspective, existing data privacy laws are built on the assumption there is a party that is trusted to maintain privacy and ensure security. The FTC and state regulators should examine existing data privacy rules, including data breach notification requirements, to assess their application to blockchain-based businesses.

This Commission has also made recommendations related to credit bureaus in the past, and as blockchain-based consumer applications become operational there may be implications for consumer protection. For example, when consumers are denied credit or employment on the basis of inaccurate information contained in a credit report, they must have the opportunity to work with credit bureaus and information furnishers to correct that information. If the data is contained in an immutable blockchain, that may not be possible. These applications are not yet in production, but policymakers will need to consider these and other implications related to the accuracy of consumer data as the technology advances.

5. Sandbox Participation

A regulatory sandbox is a "formal process for firms to conduct tests of new products, services, delivery channels, or business models in a live environment, with regulatory oversight and subject to appropriate conditions and safeguards."[29]

Like no-action letter policies, sandboxes can encourage firms to proactively engage regulators before bringing a product to market. As highlighted in a recent report issued by RegTech Lab,[30]

[29] See RegTech Lab, Thinking Inside the Sandbox: An Analysis of Regulatory Efforts to Facilitate Financial Innovation, June 2018, *available at* https://www.regtechlab.io/report-thinking-inside-the-sandbox.
[30] *Id.*

sandboxes have not been used to implement parallel, regulation-light regimes for FinTech, as feared by some detractors. Rather, as the Financial Conduct Authority's efforts in the UK have demonstrated, sandboxes may be particularly useful where a license is required to engage in a particular activity, by allowing regulators to use data from live pilot tests to inform their decision.

To be useful for companies engaged in payments or other networked businesses, state-level sandboxes would need to be coordinated across multiple states. Arizona has announced a regulatory sandbox, and offered mutual recognition for companies participating in any other state's sandbox,[31] and Illinois has proposed legislation to create its own sandbox. But without coordination, and the ability to leverage a sandbox to accelerate a licensing process across multiple jurisdictions, it's not clear that there would be sufficient value to justify the expense of participating state-level sandboxes.

[31] H.B. 2434 (2018), *available at* https://apps.azleg.gov/BillStatus/GetDocumentPdf/459033.