The Cryptoregulation project of the Zicklin Center for Business Ethics Research examines the novel legal and ethical questions raised by cryptocurrencies, blockchain-based systems, and distributed ledger technologies. Led by Professor Kevin Werbach, it serves as a hub for regulators, market participants, and researchers seeking to promote innovation while achieving public policy objectives worldwide.

# Regulatory Considerations for Token Offerings

June 2018

*This report is based on the Reg@Tech Workshop on Cryptocurrencies and Token Offerings held at the Wharton School in Spring 2018. The meeting brought together over 40 regulators, legal advisors, token issuers, service providers, academics, and other experts from around the world. While we have attempted to reflect the spirit of the discussions, this document represents solely the perspective of the authors. It should not be taken as the consensus of the group, nor the views of any individual participant. The report was edited and revised by Kevin Werbach based on working group summaries prepared by David Gogel, Xiao Ling, André Geest, and Jonathan Cardenas.*

## Introduction

Cryptocurrency token offerings (often described as initial coin offerings or ICOs) pose significant challenges for regulators. On the one hand, these arrangements may promote innovative economic models that facilitate growth of novel network-based applications and democratize the process of venture fund-raising. On the other hand, they may undermine investor protections, open the door to fraud and other abuses, facilitate money laundering, and other problems. Squaring the novel attributes of digital tokens with existing regulatory frameworks will be difficult.

Financial regulation serves multiple goals, which are sometimes in conflict. For example, the U.S. Securities and Exchange Commission (SEC) states that its mission is "to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation."[1]

[1] https://www.sec.gov/Article/whatwedo.html

Steps that protect investors and promote market fairness may also reduce efficiency and slow innovative means of raising funds or generating returns. Moreover, financial regulation addresses several populations, including retail investors, firms seeking capital, institutions, and financial market professionals. No solution will be ideal for all of them.

This inconsistency of objectives and audiences long predated the development of cryptocurrencies. However, digital tokens pose a particularly stark challenge. The same technical artifact can serve very different purposes. And in contrast to the traditional path for exotic financial products, tokens reached retail customers before institutional players.

The trans-national character of cryptocurrencies is also difficult to align with the diversity of national regulatory regimes. The threshold for being subject to regulation by a jurisdiction is low in some cases. For example, an English-language website might be evidence of intent to solicit American investors, which triggers SEC jurisdiction even when all the offering activity is elsewhere. At the moment, the leading answers to this problem are either to exclude contributors from any country with uncertain jurisdiction or compliance with the most stringent national regime.

This report provides a high-level overview of the current legal situation for tokens around the world, and then discusses significant issues to be addressed.

## Regulatory Classification

### What are Possible Regulatory Categories for Tokens?

The treatment of token offerings is part of a larger discussion about the regulatory obligations associated with cryptocurrencies. There is no question that, to the extent they function as financial instruments, cryptocurrencies fall within the domain of financial regulation.[2] However, the obligations on particular parties—if any—depend on the relevant legal boundaries and categories. These vary greatly depending on the structure of regulatory regimes around the world.

[2] Most tokens are based on ERC20 smart contracts on the Ethereum network. Whether these deserve the label "cryptocurrencies," or that term should be reserved for distinct virtual monetary units with their own blockchain, is a question for regulators to consider.

The U.S. has a particularly fragmented financial regulatory regime. This makes it a useful illustration of potential classifications, as each agency has had to determine whether activities fit within its statutory mandate in order to assert jurisdiction.

In 2013, the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury, issued guidance clarifying how its regulations apply to users, administrators, and exchangers of "convertible virtual currency."[3] In the context of money transmission, businesses involved with the administration and exchange of virtual currencies must register with FinCEN and comply with federal anti-money-laundering laws, which impose a variety of recordkeeping and reporting responsibilities. A FinCEN letter in February 2018[4] seemed to suggest that all token issuers would need to register as MSBs within 180 days of commencing business, although workshop participants disagreed about its implications.

In 2014, the Commodity Futures Trading Commission (CFTC) declared virtual currencies to be a "commodity" subject to oversight under its authority under the Commodity Exchange Act (CEA).[5] While the CFTC does not regulate transactions in the spot market, where most bitcoin transactions take place, it does regulate bitcoin futures.

The Internal Revenue Service (IRS) in 2015 concluded that cryptocurrencies should be considered property, not currency, for purposes of income taxation. The IRS has subpoenaed customer records from the Coinbase exchange to identify users who are not reporting cryptocurrency gains for tax purposes.

The SEC has found some token offerings to be securities or investment contracts subject to regulation under the Securities Act of 1933, Securities Exchange Act of 1934, and the Investment Company Act of 1940. Its Chairman has observed that, "I believe every ICO I've seen is a security," but left open the possibility that some will not be. Recently, William Hinman, Director of the SEC Division of Corporation Finance, stated that, "if the network on which the token or coin is to function is sufficiently decentralized," ongoing transactions may not represent investment contracts.

[3] https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[4] https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf

[5]https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/backgrounder_virtualcurrency01.pdf

In jurisdictions with a unified financial regulator, these formal findings may not be necessary. However, the categories still track relevant activities associated with token offerings.

Tokens can serve many purposes. Bitcoin, the first successful cryptocurrency, was created as a form of money to facilitate digital payments. Ethereum and Ripple, today the second and third most valuable cryptocurrency networks, were created to support application utility (in Ethereum's case, distributed computation processing smart contracts, and in Ripple's case, international currency transactions between financial institutions). And many tokens are marketed as investment opportunities through which buyers hope to profit from appreciation in the value of the token due to the success of the application. Once tokens are available, they can be used as the foundation for more complex financial instruments such as futures and options.

These four possibilities—currency, utility, security, and commodity–form the basis of most discussions regarding token classification. When a token qualifies as a security is the most contentious issue in the regulatory debate. Instruments classified as securities, investment contracts, or similar categories are subject to significant disclosure, marketing, and other obligations in order to protect investors. Moreover, obligations apply to exchanges that list securities and to others that distribute securities. In most jurisdictions, securities may only be traded on regulated exchanges such as alternative trading systems ("ATS"). Too narrow a definition of security tokens would undermine investor protection regimes. On the other hand, too broad a definition would raise costs for token issuers, and burden users. If inherently consumptive goods could only be purchased through an account with a regulated broker-dealer, it could impose a level of inconvenience that would make many consumer uses infeasible.

This report does not attempt to answer when tokens should be treated as securities. That question is under active discussion in many countries. The goal of this report is to identify pathways to workable regulatory regimes around the world.

## How are Countries Approaching the Issues?

Legal systems among the countries where substantial numbers of ICOs occur vary greatly. For example, common-law jurisdictions such as the U.S. and U.K. are more likely to use case-by-case determinations to narrow down broad statutory definitions, while civil law jurisdictions prefer to define comprehensive frameworks. These differences contribute to the diversity of ICO regimes.

A few countries, notably China and South Korea, have banned token offerings entirely. Those that have not are taking a variety of approaches to the regulatory issues. These models are distinguished not only based on the categories defined, but on the structure of the regulatory regime. The list below is illustrative and not intended to be comprehensive.

**Switzerland model**: Switzerland distinguishes between payment tokens, utility tokens and asset tokens. FINMA, the Swiss regulator, has issued guidance on the definition of those categories and how they relate to the classification of an instrument as a security. Generally, speaking, payment and utility tokens will not be regulated as securities. For asset tokens, there is only a (civil law) prospectus requirement as a means of consumer protection.

**The Gibraltar model**: Under the proposed regulatory framework, token issuance for the primary market will be required to go through an authorized sponsor. The sponsor will be a licensed entity or person, who assures that the requirements around disclosures and measures against financial crime (AML, CFT, KYC) are complied with. These authorized sponsors will implement their code of practice, so there can be different codes for different markets/tokens. As an example, these codes could differ regarding lock-up or vesting periods. As a result, the marketplace itself will determine what good tokens look like, not the regulator. Enforcement will be ensured by sanctioning the authorized sponsor, which can lead to the revocation of its license.

**Singapore model**: Singapore has not introduced new regulations specifically for offers of digital tokens. The Monetary Authority of Singapore (MAS) has issued guidance that token issuance may be regulated if the tokens are capital markets products. These include securities, futures contracts and leveraged foreign exchange trading arrangements. Persons who directly or indirectly engage in any act which operates as a fraud or deception involving the trading of capital markets products may also be punished under the Securities and Futures Act. In enforcing these requirements for token offerings, the MAS typically evaluates the white paper, Terms and Conditions of the offer, and the code. General fraud protection administered by the Police under the Penal Code also applies, regardless of whether a token constitutes a capital market product.

**U.S. model**: In the U.S., securities and investment contracts are evaluated under the common-law *Howey* test as, "investment in a common enterprise premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial

efforts of others."[6] Purely consumptive uses are not treated as securities. However, the SEC does not formally recognize "utility tokens." It focuses on facts and circumstances of the offer, so some utility is not inconsistent with classification as a security or investment contract. All securities offerings must either be registered (and subject to extensive disclosure requirements) or fit within an exemption. The most prominent exemptions limit offerings to wealthy "accredited" investors. There are also exemptions for crowdfunding, which some token issuers are attempting to utilize. If a token offering meets the *Howey* requirements, exchanges and other intermediaries promoting those tokens must register as broker-dealers.

**French model**: The AMF, France's financial market regulator, held a public consultation and appears to be seriously considering a pre-market authorization approach. This approach was put forward by token offerors themselves, which wanted some kind of validation in order to separate themselves from fraudulent projects. This validation can lead to the creation of a "gold standard" for offerings that markets might value.

In addition to the classification of offerings as securities or other regulated forms of investment, jurisdictions differ on whether a project needs to be subject to permission from regulators. In the EU system for securities regulation, a prospectus is sent to the regulator, who grants or denies permission. If granted, this "passport" can then be taken to other EU countries. This is to be distinguished from a permissionless system, such as that in the U.S., where issuers cannot receive formal pre-approval, but rather bear the risk of enforcement if they fail to meet regulatory requirements. A third approach is for issuances to be given permission by a third party that is overseen by the regulator (e.g. the Gibraltar model).

## Self-Regulation and Co-Regulation

Self-regulation refers to private industry efforts to establish and adopt regulatory best practices. Co-regulation refers to private activity formally supervised by a regulator, which retains the option to intervene directly if needed.

Self or co-regulation could provide multiple benefits to the industry. An organization could start as a voluntary trade association like the Securities Industry and Financial Markets Association ("SIFMA"), but over time mature into an approved self-regulatory

[6] United Housing Foundation, Inc. v. Forman, 421 U.S. 837 at 852 (1975); SEC v. Edwards, 540 U.S. 389 (2004).

organization ("SRO"), which exercises rule-making, examination, and enforcement authority. It could be modeled after the Financial Industry Regulatory Authority (FINRA) and the National Futures Association ("NFA") in the U.S., which have statutory mandates and oversight by the SEC and CFTC. These existing SROs already have authority over token-based activities that constitute securities or derivatives transactions. A token-focused SRO would be particularly valuable for novel asset classes or markets.

In the short-term, an association would show good faith to regulatory bodies and potentially be a rational basis for slowing down enforcement actions. In the long-run, the association could craft and enforce best practices, serve as an ally for regulators, and help to police the marketplace. Lawyers could conceivably use standards set by the organization to issue opinion letters and provide clarity to clients. Over time, the organization could evolve to harmonize different but increasingly converging international approaches.

The organization could also make non-binding determinations based on vetted guidelines. Depending on the type of token sale involved, customized requirements covering tailored disclosures, consumer and investor assessments, security audits for smart contracts, vetted and approved models for utility tokens (e.g. token-curated registries, curved bonding, etc.), and rules related to refunds and marketing could be crafted. Finally, given the significant cybersecurity risks associated with token sales, including the loss of investment and personal information caused by hacks of platforms and wallets, the SRO could help to collectively elevate standards to prevent cyberattacks.

While the ultimate success of an association or SRO depends on buy-in from major exchanges and other key players, an organization could be beneficial and help to clarify many questions faced by all industry participants. The association could set boundaries and provide tools to categorize tokens, providing exchanges with clarity on what they can and cannot list. For example, relying on recent legislation from the U.S. state of Wyoming, the organization could certify that a token is not a security if it meets a certain set of characteristics.

An SRO could also help with enforcement and monitoring members' activities. It would have oversight authority to remove non-complying members and to refer bad actors to regulators. Furthermore, it would be responsible for developing a set of tools to monitor secondary markets on an ongoing basis and for pushing members to report requirements such as material ownership and milestone development.

Supporting ideas can also be taken from a comparison to product labels in other industries. With product labels, a group of providers comes together to create a label, e.g.,

for dietary products. Through this, they create a stamp that customers over time associate with quality. Enforcement is done by regulators, such as the U.S. Federal Trade Commission (FTC), which can bring forward a deception case if those self-imposed standards have been violated. The FTC does not say what the standards or code of conduct shall be. This is done by the industries themselves. This form of self-regulation often arises in markets where there is a wide range of actors, and good faith projects want to distinguish themselves.

The most important and least intrusive way of protecting investors and consumers is education. Education is especially important in a decentralized system where it is hard to determine the right access point for regulation. There is always the underlying risk of information overload, which leads to everything being regarded as a risk. Misinformation in the marketplace needs to be corrected, e.g., by giving investors/consumers updates on the rates of failures of token offerings. Moreover, the risk of celebrity endorsement/crypto-celebrity endorsement for fraudulent activities should be addressed.

Disclosure is also important for external parties who can assess and process all of this information for consumers. Comparable to lead investors in crowdfunding, there are lead consumers or consumer protection advocates. These consumer advocates serve as "watchdogs" and evaluate whether a platform's Terms and Conditions are consumer friendly. The emergence of lead investors or lead consumers promotes a brand.

This type of self-regulation can exist in parallel to government regulation or could serve as a substitute for government regulation. With the rise of investor/consumer protection advocates comes the issue that if everyone can be such an advocate, this will lead to a race to the bottom, and ultimately everyone can comply. The right incentive needs to exist; the investor protectors need to have skin in the game. This means that they need a stake in the projects they are evaluating. On the downside, this incentive can lead to a conflict of interest.

## Identity and AML/KYC

The regulatory concerns around token offerings are not limited to investor protection and market oversight. Cryptocurrencies can function as money, which can be used for nefarious purposes. Anti-money laundering ("AML") refers to measures designed to prevent the use of a legitimate financial system to conceal illegally obtained funds. Know your customer (also known as "know your client" or "KYC") is an anti-money laundering due diligence process through which financial entities verify the identity of their clients. Having verified identities associated with all funds transfers facilitates the

exclusion of actors or transactions involved in money laundering. It also supports enforcement of sanctions regimes that bar financial transactions with certain entities or countries.

AML/KYC rules, such as the Bank Secrecy Act in the U.S., impose registration, recordkeeping, and reporting requirements on banks and other financial services businesses. These are designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the country. Compliance with these rules can entail substantial costs, and can require firms to adjust their business models to obtain and track the necessary customer data. The key question is therefore whether an entity or activity is subject to AML/KYC requirements. In the U.S., the scope of obligations was extended to many non-bank businesses by the USA PATRIOT Act. AML/KYC frameworks exist in all major financial hubs, although the particular definition of covered entities is not uniform.

There is a need for greater clarity about how AML/KYC requirements apply to various forms of cryptocurrency-related activity. This challenge is multiplied when there are multiple sets of rules within the same national jurisdiction. For example, New York State has promulgated a regulatory framework known as the BitLicense which imposes significant AML/KYC obligations on "virtual currency business activity," a category that may be different than those subject to U.S. federal rules.

In 2015, FinCEN took enforcement action against Ripple for failure to implement adequate AML/KYC practices. And its February 2018 letter to Senator Wyden stated that a "developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency is a money transmitter and must comply with [AML/KYC] requirements." There is significant uncertainty about whether this statement represents a formal change in policy, and its implications for ICOs. However, given the seriousness of AML/KYC concerns and the potential sanctions for violations, those engaged in ICOs would be wise to incorporate some level of AML compliance.

There are a number of other emerging challenges in applying AML/KYC to ICOs. The Bitcoin blockchain identifies the origination of all funds as block rewards from mining. However, bitcoin contributed to an ICO may have been subject to multiple subsequent transactions which were not tracked under an AML/KYC regime. How far back do coins need to be tracked to ensure they were not proceeds from crimes or originating in sanctioned countries? In some cases, ICO participants form syndicates with a designated accredited investor as the front person. KYC checks of that investor may not fully identify the sources of funds. In addition, a number of KYC service providers have

emerged with the growth of ICOs to provide identity checks for token issuers. While some of these are developing sophisticated technologies for identity verification, others may provide insufficient levels of verification of information security. The KYC required to verify accredited investor status under U.S. securities laws is not necessarily the same required for AML and sanctions compliance purposes.

Going forward, the challenges are likely to become even more substantial. Privacy coins such as Monero and ZCash use zero knowledge proofs, a novel form of cryptography, to make it extremely difficult to identify the source of transactions. How this technology can be squared with AML/KYC requirements is an open question. The implementation of new data protection rules such as the General Data Protection Regulation (GDPR) in the European Union is also likely to create tensions between the transparency orientation of AML/KYC and the desire to enforce strong privacy protections. On the other hand, blockchain-based solutions offer promising means of enhancing and streamlining AML/KYC processes.

## Conclusion

Although token offerings have been conducted for several years, the dramatic growth of ICOs in 2017 created a severe challenge for regulators. A "wild west" environment allowed innovative projects to attract contributors and raise capital quickly, but also opened the door for unscrupulous actors and created substantial regulatory uncertainty. We are now moving into an environment where forward-looking regulators seek to balance investor protection, capital formation, and innovation promotion goals, while at the same time, responsible token issuers and supporting entities seek the certainty and reputational benefits of legal compliance. This will be an iterative process, and one that follows different paths around the world. The Cryptoregulation initiative at Wharton will continue to work with both public and private sector actors to develop greater understanding and facilitate robust solutions.

## Appendix A: Spring 2018 Workshop Participant List

*Affiliations listed for informational purposes only*

| | | | |
|---|---|---|---|
| Albrecht | Julian | SMP Law | Sr. Associate |
| Catalini | Christian | MIT Sloan School | Professor |
| Channing | Emma | Satis Group | CEO and GC |
| Chilson | Neil | FTC | Acting Chief Technologist |
| Corva | Matt | Consensys | Head of Legal |
| Crosbie | David | University of Pennsylvania | Lecturer in Engineering School |
| Czarnecki | Jacek | GC, MakerDAO | General Counsel |
| Finck | Michele | Max Planck Institute | Professor |
| Garcia | Joey | Isolas LLP | Partner |
| Geest | André | Bucerius Law School | Student |
| Herrada | Jorge | CFTC | Technology Lead, LabCFTC |
| Jain | Kavita | FINRA | Emerging Regulatory Issues Director |
| Jones | Sian | Gibraltar FSC | Senior Advisor on DLT |
| Klayman | Josh | Morrison & Foerster | Of Counsel |
| Kreiterling | Christoph | German Federal Financial Supervisory Authority (BaFin) | Senior Officer |
| Laufer | William | Wharton School | Professor of Legal Studies & Business Ethics |
| Lee | Wendy | Ex-Block.one | |
| Levin | Rick | Polsinelli | Shareholder |
| Lim | Yann Lee | Monetary Authority of Singapore | Deputy Dir, Corporate Finance & Consumer |
| Long | Caitlin | Ex-Symbiont | |
| Meyer | Stephan | MME (Zurich) | Attorney |
| Moser | Malte | Princeton University | PhD Student |
| Murck | Patrick | Cooley | Special Counsel |
| Murphy | Greg | Outlier Ventures | Partner & Head of Compliance |
| Petkoski | Djordjija | Zicklin Center | Senior Fellow |
| Reed | Dummond | Evernym | Chief Trust Offficer |
| Resas | Daniel | Organizer | Zicklin Center |
| Rosekrans | Hector | Messari | Director of Policy & Operations |
| Santori | Marco | Blockchain | President & Chief Legal Officer |
| Schneider | Lee | McDermott Will & Emery | Partner |
| Seidl | Tobias | Sicos | Co-founder |
| Siedler | Nina | DWF law firm | Partner |
| Sillaber | Christian | Organizer | Zicklin Center |
| Simmchen | Christoph | Gnosis | Legal Counsel |
| Singer | Ryan | Chia Network | CEO |
| Sixt | Elfriede | Fintech Academy | Founder |
| Stein | Josh | Harbor | President & Chief Legal Officer |
| Szczepanik | Valerie | SEC | Head of DLT Task Force |
| Telpner | Joel | Sullivan & Worcester | Partner and head of Fintech |
| Tinianow | Andrea | Global Kompass | Ex-Founder & Director, Global Delaware |
| Van Cleef | Carol | Baker Hostetler | Partner and head of Fintech |
| Van Valkenburgh | Peter | Coin Center | Director of Research |
| Werbach | Kevin | Wharton School | Professor of Legal Studies & Business Ethics |
| Wright | Aaron | Cardozo Law School | Associate Clinical Professor |
| Zilgalvis | Peteris | European Commission | Head of Unit, Start-ups & Innovation |