KNOWLEDGE@WHARTON

FINANCE

Initial Coin Offerings: Can Regulators Curb the Risks?

Mar 27, 2018

Global Focus, North America

For tech startups hungry for capital, an initial coin offering seems to offer a dream: It lets them raise millions of dollars online with just an idea for a product or service to be delivered in the future. For investors, the allure is the ability to invest any amount very early on in startups whose cryptocurrency could soar in value. Such is the attraction of ICOs that the first quarter saw a record 152 offerings hit the market, raising $4.83 billion — already bigger than last year's tally of $3.9 billion, according to Coinschedule.

An initial coin offering lets a young company raise money — in addition to venture capital, angel investors and others — by selling tokens that can come in the form of its own cryptocurrency. In return, investors from Main Street to Wall Street get free or discounted products and other perks once the startup actually launches the business. Investors can also sell

or trade these cryptocurrencies for other tokens in crypto exchanges. But unlike crowdfunding, ICOs typically are global, most leverage blockchain and their investors seek a return on their investment.

Since they are so new, ICOs operate with little, if any, regulatory purview. But that's about to change. With such big sums being raised and the danger of scams proliferating, regulators are seeking ways to create the right framework for supervision, according to the recent Wharton Reg@Tech conference, where key government officials, cryptocurrency entrepreneurs, academics and lawyers met to discuss avenues for regulation. The conference was hosted by The Zicklin Center for Business Ethics Research.

"Enforcement is generally seen by regulators as an important challenge," said Kevin Werbach, Wharton professor of legal studies and business ethics and one of the forum's main organizers. Regulators' viewpoints range from "creating completely new regulations for token offerings to stating that traditional securities rules can apply without any changes," he said.

The Wharton conference, which was by invitation only and included a private session for just regulators from around the world, gave authorities the opportunity to compare notes informally, Werbach added. "We asked the regulators where they see gaps in existing legal frameworks." He said there also was discussion about the prospects for self-regulation, although it's too early to say whether authorities were in favor of it or not.

According to a pre-conference survey of participants, regulators believe the most valuable thing the private sector could do to address the governments' concerns would be to make sure they comply with existing rules. Authorities also want startups to engage in active discussions with regulators as well as establish standards and improve transparency. As for entrepreneurs, they want regulators to be more clear about how they can avoid legal action.

Regulation Is Not Easy

The regulators' goal is to protect consumers and preserve the stability of the markets while continuing to foster innovation. But crafting ICO and cryptocurrency regulations is harder than it looks, according to discussions by conference participants. For one, the blockchain is a decentralized ledger system that makes monitoring tougher because it lacks a central body to be held to account.

Also, since these offerings have a global reach because they're conducted online, they pit government authorities against each other. For example, if a startup is incorporated in the U.S. but its founders and top management team live and work in Hong Kong, which country has

jurisdiction over the business?

Even within a country, there's a question of competing jurisdictions as well. When a startup sells tokens in an ICO that can be exchanged for future products, is it selling a security since investors can hope to make money if the token goes up in value? That means securities laws kick in to be enforced by the U.S. Securities and Exchange Commission (SEC).

But what if the exchangeable tokens are commodities? Then the lead regulator is the U.S. Commodity Futures Trading Commission (CFTC). FinCEN, the Financial Crimes Enforcement Network, has also weighed in. It said a company with a virtual currency trading platform is a money transmitter and thus must comply with related rules.

No matter, the SEC has charged ahead. In recent months, it has stepped up its scrutiny of ICOs by issuing dozens of subpoenas, according to *The Wall Street Journal*. SEC chairman Jay Clayton has said that cryptocurrency and ICO markets have "substantially less investor protection" than traditional securities markets, with "correspondingly greater opportunities for fraud and manipulation."

In January, the SEC halted the ICO of AriseBank, calling it "allegedly fraudulent." AriseBank described itself as a decentralized bank and sold its AriseCoin cryptocurrency as tokens to investors to be used on future products and services. At one point, it also claimed that its accounts were FDIC insured.

> **"There are points of commonality across global regulators. They all are striving to protect their citizens from nefarious schemes. They all want to promote capital formation and job creation, and they all want market integrity."**
>
> –Rick Levin

Global Regulators Coordinate

Despite overlapping jurisdictions, regulators globally are collaborating just like they do on other cross-border issues like money laundering. The key is to find common ground first and then customize for local needs. "There are points of commonality across global regulators," Rick Levin, chairman of the fintech and regulation practice at law firm Polsinelli, told Knowledge@Wharton. "They all are striving to protect their citizens from nefarious schemes.

They all want to promote capital formation and job creation, and they all want market integrity. So harmonization is something that can be strived towards ... but also there's an appreciation that each country has separate lawmaking bodies."

Kavita Jain, director of emerging regulatory issues at the U.S. Financial Industry Regulatory Authority (FINRA), added that regulators want to be helpful. "As regulators, we want to support innovation because it provides consumers access to better, cheaper, faster services — sometimes access to services they may not have had in the past," she said in an interview. "It also has the potential to create efficiencies in the marketplace, but it has to be done within the guardrails of investor protection and market integrity. ... We're trying to maintain that balance."

But Peter Van Valkenburgh, director of research at Coin Center, said the industry's view on regulation is mixed. "Some people think the government's taking a somewhat too draconian or conflicting approach that has been too hard for the industry to parse," he said in a Knowledge@Wharton interview. Others believe the industry has to "grow up and deal with it. This is regulation just like any other regulation." His opinion is that regulators have a mixed report card. The SEC, which he said has been labeled as being heavy handed on the industry, actually is "very sensible" by doing enforcements on a case-by-case basis.

In contrast, China and South Korea have banned ICOs outright. Van Valkenburgh said such a "sweeping, aggressive" approach is premature, especially when dealing with a fast-changing technology. "If the environment changes ... maybe you [would] have missed out on a lot of potential innovation." By being "somewhat obstructionary," China could be ceding blockchain innovation to nations like Singapore, Japan and the West. In his view, Singapore's pro-innovation policy is working out well for ICOs and cryptocurrencies. "I wish we had such a clear path in the U.S., but it also means a clear path for bad policy as well."

Approach for Regulators

When developing rules for cryptocurrencies and ICOs, regulators must ask themselves three questions: What is the goal? Who is the target of the regulation? What is the method of enforcement? For example, the objective could be consumer protection, according to a European researcher. Other goals could be anti-money laundering or counter-terrorism. But when it comes to choosing the entity to be regulated, it is not that easy. "The blockchain is a transnational, multijurisdictional peer-to-peer network. There are many actors, established in many places."

The researcher calls these targets "regulatory access points" — bodies that are more practical for government authorities to regulate in the crypto and ICO ecosystem. For instance, one access point is the internet service provider (ISP). "They are in a position to comply with regulators," she said. They also can determine which networks are connected to the blockchain, look deep into blockchain packets or applications, and they can sometimes distinguish between lawful and illegal activity. Indeed, most bitcoin nodes are hosted on only 13 ISPs. "Even though we see blockchain as decentralized, there's a way to centralize it."

> **"As regulators, we want to support innovation because it provides consumers access to better, cheaper, faster services — sometimes access to services they may not have had in the past."**
>
> –Kavita Jain

Another regulatory target could be miners. They are companies that validate blocks on the blockchain in return for compensation, usually in the form of cryptocurrency. To validate blocks, they perform complex calculations that use a lot of electricity. "When they are gathered in large mining pools, [we can] locate them through electricity consumption," the researcher said. They can be located because the electric utility might be run by the state. However, regulators risk unsettling the entire blockchain network and cause miners to flee to another country. Also, miners cannot distinguish between legal and unlawful activity, she said.

Authorities also could target intermediaries, such as cryptoasset exchanges, search engines, social networks and hardware manufacturers. With search engines, regulators could force them to stop listings that seem fraudulent. Social networks could be compelled to reject cryptocurrency or ICO ads. Hardware makers could be required to install "backdoors" into the system that regulators could access. The U.K.'s Investigatory Powers Act of 2016 allows such action, according to the researcher.

To be sure, there are drawbacks to targeting intermediaries as well. For example, South Korea has shifted anti-money laundering (AML) duties to banks from cryptoasset exchanges, the researcher said. "What does that mean from a competition and innovation perspective?" And then one could also argue the opposite: By removing AML compliance from crypto intermediaries, they are free to focus on innovation.

Target Exchanges

Coin Center's Valkenburgh thinks cryptoasset exchanges are the "logical" targets for regulation. "Those exchanges will always be centralized," he said. "We might see a decentralization of crypto to crypto exchanges, but if there are dollars involved, there will be a chokepoint, if you will. I think that is a sensible place to do your AML regulation, to do your investor protection regulation." Also, the exchanges would be easier to keep track of than the many startups. "It's going to be whack-a-mole to a certain extent."

> **"It's going to be whack-a-mole to a certain extent."**
>
> –Peter Van Valkenburgh

Monitoring the exchanges also is preferable to targeting the actual tech protocol or platform, such as regulating software development or network architecture of bitcoin or the Ethereum blockchain platform, said Valkenburgh. "Those plans would inevitably backfire. Alternative networks would appear, people would switch to those without backdoors, or that were not compromised in any way." What's more is that "these networks are made to avoid centralized control so it would be difficult to implement any meaningful policy through that layer," he added.

Similar disadvantages arise if authorities go after software developers, who could be required to program in "kill switches" or encryption "backdoors" for governments to use, the researcher said. If they balk at such regulation, developers could move to more friendly jurisdictions or work anonymously. Another wrinkle: Not all regulators like the idea of a "backdoor." She said the EU Security Commissioner believes it would weaken the overall security of the network within a blockchain context.

How about targeting the end users? For example, China has banned ICOs and encourages citizens to report on those who break the law. But the disadvantage is that the public might not understand what they are doing nor have the capacity to comprehend complex legislation, the researcher said. Also, the impact of shifting norms is an issue. "If a lot of people use it, it becomes much harder for regulators to enforce it," she said.

Instead of targeting a body to regulate, government could consider getting involved in decentralized networks. For example, they could participate in blockchain governance, software development, mining or running nodes. Also, they could create blockchains specifically designed to comply with regulatory constraints, or endorse projects that do so, the researcher said.

However, one conference participant argued that in a "world of decentralized applications ... you have to go after the internet itself because there's nowhere else." Indeed, it is quite possible for intermediaries to continue to disappear, another participant said. "With decentralized exchanges, more anonymous cryptocurrencies are coming online. At which point you have to go to the end users or the infrastructure itself" — or the ISP.

One lawyer noted that regulators have been thinking about the blockchain in terms of its being a technology rather than viewing it through an industry lens. "Blockchain tokens can represent anything," he said. "They can be my health care records. In the U.S., it will have regulatory implications." Another lawyer said that the difficulty is that a decentralized system by its nature wants to avoid the law. "They provide an alternative," he said. But is the decentralized system better than the rule of law? "This is like an open question. Is this something we should protect or ensure it develops? Or regulate and fight it?"

Whatever the approach, it behooves regulators to make sure they don't over-police. One industry participant said that a federal pre-emption of state laws would be helpful. He said there are 53 states and territories that regulate money transfers and licensing of exchanges. "It's ridiculous and absurd — that's a high compliance burden," he added. Getting to the 53rd background check and money transmission license will have "no effect on your likelihood of protecting consumers or not. It's just red tape."

How Many ICOs Are Scams?

Consumer protection is high on the list of regulators' goals in overseeing the industry. Concerns are rising, especially since ICOs have exploded in popularity seemingly from nothing. Indeed, the cryptocurrency craze has been compared to the Dutch tulip bubble in the 17th century. But are most ICOs really scams?

> **Based on one academic's research, at least 5% of ICOs are frauds and scams, and the figure could go as high as 25%.**

One academic from a leading university examined around 1,500 ICOs and 1,800 tokens from 2011 to 2018. Based on his research, he said that at least 5% are frauds and scams, and the figure could go as high as 25%. Some red flags: There is no white paper explaining the business model,

or if one exists, it is less technical than others, less polished and not professionally edited. The startup accepts credit cards and launched a website shortly before the offering with scant information about its founders.

Fraudulent ICOs also tend to engage in bad practices such as "bounty" programs, where they ask the community to talk up their ICO online and in social media in exchange for rewards. They also don't have an escrow account — a place to park investors' money until the offering is completed, after which funds are distributed to the startup in stages. Also, it's not a good sign if the startup doesn't have a codebase for the public to see.

What investors also don't seem to reward are startups with ICO advisors. Their presence means the startup's ICO is more likely to be listed on an exchange, perhaps due to the advisor's connections, but the offering is not likely to do well, the academic said. "There is a cottage industry of advisors on ICOs," he said. "They jump from ICO to ICO."

The good news is that the market seems to be able to discern good from bad actors, the academic said. More capital flows to startups whose white papers are more technical and which exhibit best practices like vesting and escrow. Those that do not promote dividend payouts and bounty programs get more money than those that do. Also, startups led by a team with more credentials and tech expertise are favored by investors.

"The most reassuring part of that is many of those you can spot with some major red flags," the academic said. "They are not as sophisticated yet." But of course, the danger is that as their expertise grows, so could their ability to dupe the public.
