October 22, 2019

Being Smart About Your Smart Contract

Barry Seeman

Susan Joseph

Now is the time for the digital asset and cryptocurrency space to work with global regulators to widely adopt this emerging technology and ecosystem. We need only look at the regulatory activity to see that a robust digital asset and cryptocurrency world is being established; it is far better to work with than against the regulators so that innovation can be realized.

Work With, Not Against, Your Regulators!

Timing is everything! And now is the time for the digital asset and cryptocurrency space to work with global regulators to widely adopt this emerging technology and ecosystem. Regulators have issued a number of new statements and cautions, and taken actions, since we published our article on Oct. 2, 2019, “Being Secure About Your Security Token Offering (https://tabbforum.com/opinions/being-secure-about-your-security-token-offering/).”

In this article, we are bringing forward some additional information, observations and suggestions to the digital asset space, focusing on some of the recent statements and actions taken by U.S. and global regulators. In particular, we will discuss aspects of perceived financial markets stability, Know Your Customer (KYC) protocols, Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) protocols, and Tax Reporting. These issues are critical to understand and act upon, whether designing your first Security Token or opening your first crypto wallet.

This article is based upon the experiences and observations of an experienced financial professional, Barry Seeman, and a crypto-seasoned attorney, Susan Joseph. Contact details for both are found at the end of the article.

As with all articles like this one, we must disclose that we are not providing legal advice, we are not your attorneys, nor your accountants, and therefore, this article is for informational purposes only and not for the purpose of providing legal and/or accounting advice. You should contact your own legal counsel and/or accountant to obtain advice with respect to any particular issue or problem raised in this paper. Furthermore, all service providers acknowledged or highlighted in this paper are there for discussion purposes and should not be construed as an explicit endorsement of their services. Any service provider should be engaged solely after you have performed and resolved adequate due diligence and have agreed to contracted services.

Regulating the Known and the Unknown

Since the beginning of October 2019, there have been a number of guidance statements from global regulators that should give cryptopreneurs, investors, lawyers, enterprise managers, executives and blockchain programmers pause. Some industry participants have argued that regulators have been slow to exhibit a deep understanding of digital or crypto assets, and as such, have created an uncertain regulatory environment that leaves innovators with no clear path forward. But we would argue that those times are behind us.

We need only to look at the regulatory activity to see that a robust digital asset and cryptocurrency world is being established, and it is far better to work with than against the regulators so that innovation can be realized. All security/banking/markets regulators are tasked with understanding the potential systemic risks associated with an activity or product, and issue rules that can act to reduce or eliminate those risks to global markets. Global regulators have been prudent and diligent in education of their staff and the constituents or marketplaces that they serve. Some have set rules specific to digital assets and cryptocurrency. Many have offered “sandboxes” or “local office hours” as outreach and to encourage innovation. These statements, offerings, and ultimate rules are meant to create a level playing field, while also acting to set the bar describing certain illegal or frowned upon activities.

In our last article (“Being Secure About Your Security Token Offering (https://tabbforum.com/opinions/being-secure-about-your-security-token-offering/)”), we highlighted foundational considerations when issuing a new Security Token (a particular class of crypto-asset). Specifically, we stated:

> *“Financial regulatory authorities across the globe are beginning to pass rules pertaining to the issuance and sale of Security Tokens. These rules will evolve over time as the digital shares become more accepted. But you must be conscious of what security laws and tax laws are applicable to your investment and your investors and seek the appropriate advice from engaged counsel. … This highlights the important point that a Security*

Token represents an investment made by an investor, with the expectation of an increase in the value of said investment. Therefore, most securities regulators consider Security Tokens to fall under their purview and will require issuers to adhere to the regulatory rule-set that applies to whatever underlies the Security Token and how it is being sold."

It is now coming to pass that regulators are issuing statements and rulings to curtail certain activities that crypto-assets may afford. We recommend, as we did in the previous article, that you become equally sophisticated in the expressed concerns of regulators and act to remedy the structure and operations of your digital asset, protect your operation from restricted investors and money laundering possibilities, and take that "belt and suspenders" approach of "Being Smart About Your Smart Contract."

STATEMENT 1: "Potential financial stability issues from global stablecoins," FSB Chair's letter to G20 Finance Ministers and Central Bank Governors (https://www.fsb.org/wp-content/uploads/P131019.pdf), Oct. 13, 2019.

OK, this wasn't a text from your kid brother, telling you that Mom and Dad are watching the clock because your about to break curfew.

On Oct. 13, 2019, the Chairman of the Financial Stability Board (FSB) sent an alarming letter to G20 Finance Ministers and Central Bank Governors discussing stablecoins.

As a reminder, the FSB was formed through a mandate by the Group of 20 in April 2009, post-Financial Crisis. Its charter is to propose and guide "the development of critical reform initiatives in a number of areas" and work with "international standard-setting bodies and international organizations to build a more resilient financial system, addressing the fault lines that caused the global financial crisis." (*source:* FSB Chair's Letter to G20 Finance Ministers and Central Bank Governors). The sole decision-making body of the FSB is the Plenary consisting of representatives of all central banks and monetary authorities of the Member Countries. The current Plenary has 59 representative members from 25 jurisdictions, six representatives from four international financial institutions and eight representatives from six international standard-setting, regulatory, supervisory and central bank bodies. (https://www.fsb.org/organisation-and-governance/ (https://www.fsb.org/organisation-and-governance/))

The Chairman's letter did not pass judgement upon all crypto-assets, but rather singled out the potential for stablecoins to be a source of instability to global markets. It states:

"The introduction of 'global stablecoins' could pose a host of challenges to the regulatory community, not least because they have the potential to become systemically important, including through the substitution of domestic currencies. These include challenges for financial stability; consumer and investor protection; data privacy and protection; financial integrity including AML/CFT and know-your-customer compliance; mitigation of tax evasion; fair competition and anti-trust policy; market integrity; sound and efficient governance; cyber security and operational risks; and an appropriate legal basis."

On the surface, this appears to be a direct assault on the potential development and release of the Libra Stablecoin, Facebook's attempt to revolutionize global payments and money accounts. Libra's mission is (https://libra.org/en-US/) to be "A simple global currency and financial infrastructure that empowers billions of people. Reinvent money. Transform the global economy. So people everywhere can live better lives." Reserve assets backing this stablecoin will be the U.S. Dollar, Euro, Japanese Yen, British Pound and Singapore Dollar.

It certainly sounds like an altruistic approach to creating value for the underserved, and yet Mark Zuckerberg's planned upcoming testimony in front of the U.S. House Financial Services Committee (on Oct. 23) may further sway lawmakers and regulators away from expressing support for this endeavor. Randal Quarles, FSB Chairman, states in the letter:

"Stablecoin projects of potentially global reach and magnitude must meet the highest regulatory standards and be subject to prudential supervision and oversight. Possible regulatory gaps should be assessed and addressed as a matter of priority. … The FSB is assessing how the existing regulatory framework applies to 'global stablecoins' and whether any regulatory gaps need to be filled. In any case, it is essential to apply the principle of 'same activity – same rules', independent of the underlying technology."

We note that Libra publicly and consistently says it wants to work with regulators and will not launch prior to receiving regulatory approval in Europe and the USA. Both David Marcus, the Facebook/Calibra leader, and newly elected Libra board member, and Dante Disparte, head of policy and communications at Libra, have specifically and repeatedly stated this position:

- "Facebook admits digital currency doubts as regulatory hurdles loom (https://www.ft.com/content/be6a7756-eea2-11e9-ad1e-4367d8281195)," Financial Times, Oct. 14, 2019
- Hearing Before the United States Senate Committee on Banking, Housing, And Urban Affairs (https://www.banking.senate.gov/imo/media/doc/Marcus%20Testimony%207-16-19.pdf), July 16, 2019

For an in-depth analysis of the Libra Stablecoin, please refer to a report, authored by Susan Joseph, Executive Director of Diversity in Blockchain, and her co-founders, Anna Ashurov, Michelle Gitliz, Shawnna Hoffman, and Josh Klayman, which can be found at: https://diversityinblockchain.com/news/2019/7/17/project-libra-and-diversity-in-blockchain (https://diversityinblockchain.com/news/2019/7/17/project-libra-and-diversity-in-blockchain). This report is also available on the Congressional Record.

In essence, the ground rules have been laid, meaning that Libra, and any other stablecoin, will need to meet and follow the same regulatory regime of the US Dollar, Euro, etc. This includes all aspects of money transfer restrictions, regulatory reporting, sanction adherences, anti-money laundering protocols, etc. The phrase, "Subject to prudential supervision and oversight," signifies that regulatory bodies will need to move quickly in order to instill rules into the use and trading of Libra. And the phrase, "same activity – same rules," points to the premise that digital assets, coins and tokens must follow the same ruleset established for underlying assets, currencies or services they are attempting to disrupt.

[Related: "Will Libra Catalyze a Token Revolution in Finance (https://tabbforum.com/opinions/will-libra-catalyze-a-token-revolution-in-finance/)?"]

Over the past several weeks, we have witnessed the departures of key supporters from the Libra Association, such as PayPal, EBay, Stripe, Mastercard and Visa. It is unclear if this was a move in concert, or as a result of governmental pressure on these large corporate players in payment transfer and technology. There were letters of deep concern (https://www.schatz.senate.gov/imo/media/doc/Signed%20Letters%20re%20Libra%20to%20Patrick%20Collison,%20Ajaypal%20Banga,%20and%20Alfred sent by Senators Sherrod Brown and Brian Schatz to Stripe, Mastercard and Visa.

Either way, there is a substantial amount of scrutiny and oversight which will ultimately impact the development of Libra and other potential stablecoins.

STATEMENT 2: Leaders of CFTC, FinCEN, and SEC Issue Joint Statement (https://www.cftc.gov/PressRoom/SpeechesTestimony/cftcfincensecjointstatement101119) on Activities Involving Digital Assets

This joint statement of major U.S. Regulators was released from Heath Tarbert, Chairman, U.S. Commodity Futures Trading Commission (CFTC); Kenneth A. Blanco, Director, Financial Crimes Enforcement Network (FinCEN); and Jay Clayton, Chairman, U.S. Securities and Exchange Commission (SEC), on Oct. 11.

Once again, this wasn't a little tweet or a postcard in the mail. Regulators are paying attention to this business sector and you should be paying attention to the regulators. We have received a significant warning from key U.S. regulators, who are concerned and together acted "to remind persons engaged in activities involving digital assets of their anti-money laundering and countering the financing of terrorism (AML/CFT) obligations under the Bank Secrecy Act (BSA)."

Consider the following:

1. If you are working on, or considering an investment in cryptocurrency, such as Bitcoin, you likely fall under the purview of the CFTC, because of its prudential oversight of market contracts like futures and certain currency trading;
2. If you are working on, or considering an investment in a Security Token, or some other crypto-asset, you likely fall under the purview of the SEC, because of its prudential oversight of the securities and investments markets; and,
3. Regardless of whether you are working on a cryptocurrency or crypto-asset, you likely are under the purview of the FinCEN!
4. While we are not specifically tackling state regulations in this article, state regulatory schemes may be implicated as well. Yes, you can be governed by more than one regulator at the same time.

TAKE HEED! The Financial Crimes Enforcement Network is becoming a powerful voice in the rulemaking and oversight of the digital asset world. We highlight that this agency has not been a typical voice that is often quoted in the financial press, and when presented in the joint statement with the CFTC and the SEC, it must be taken with more emphasis. So we will reiterate: TAKE HEED! Regulatory bodies are resolving much of the rule ambiguity covering digital assets, and the fear that crypto-assets are ripe for abuses of money laundering and other nefarious activities is forcing a vocal focus from FinCEN.

Early adopters and investors in digital assets may have unwittingly believed that these investable or tradable tokens were not subject to rules of regulators, because of the altered terminology enjoined to the characteristics and operations of the tokens. This statement calls out the fact that:

> *"Market participants refer to digital assets using many different labels. The label or terminology used to describe a digital asset or a person engaging in or providing financial activities or services involving a digital asset, however, may not necessarily align with how that asset, activity or service is defined under the BSA, or under the laws and rules administered by the CFTC and the SEC."*

Do not be misled with a false understanding that regulators will give you a pass on activities and products such as “crowdfunding” and “utility tokens.” The CFTC, FinCEN and SEC just gave the world the overt “if it quacks like a duck” warning. Crypto-assets, ryptocurrencies and stablecoins will all fall under some rules and regulations of these and other governmental bodies across the globe. We emphasize that developers, issuers, lawyers, enterprise managers, executives, and investors must be aware of the regulations pertaining to their activities in their domiciliation.

Let’s return to the message of the statement, reminding participants that they are subject to “anti-money laundering and countering the financing of terrorism (AML/CFT) obligations under the Bank Secrecy Act (BSA).” The BSA was enacted (https://occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html) to deter and detect money laundering, terrorist financing, other criminal activities, and the misuse of U.S. financial institutions. This is a wide-ranging mandate which gives FinCEN the ability to scrutinize the full breadth of crypto activities.

Crypto-assets may present substantial innovation opportunities and represent the great democratizer of financial and security activities, allowing for instantaneous and trusted transactions, fractional ownership and various other blockchain miracles. They may allow for more transparency! All true. We welcome, support and are encouraged by the innovation that is both at the door and on the horizon. But we recognize that blockchain technology creates an environment which can circumvent all the safeguards legislated for KYC/AML/CFT obligations. To successfully mainstream innovation and encourage digital asset sector growth, all activities must remain compliant. And so, we support compliant innovation. Let’s discuss various aspects of these obligations.

Under Know Your Customer, or KYC, U.S. financial institutions must adhere to rules set forth by FinCEN, entitled “Customer Due Diligence Requirements for Financial Institutions (https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf),” or the CDD Rule. Let’s break down the rule into four musts:

1. Identify and verify the identity of any customer or investor;
2. If the customer or investor is a company, then identify and verify the identity of the beneficial owner of the company;
3. Understand the nature of the customer or investor relationship in order to develop a customer risk profile; and
4. Continuously monitor customers for suspicious activities and/or transactions.

Many smart contracts today have built into the coding the capabilities to capture the required information from the contract holder or investor. This includes obvious fields such as name, address, Social Security number, and other attributes required under the CDD Rule. But capturing the information is only one aspect of the protocol, and many contracts seem to fall short of the verification step, as well as the constant monitoring. If all aspects could be captured and implemented, such automation may make compliance easier and less costly, which would certainly be an improvement over some of today’s processes.

The irony is that the majority of token networks are built upon “trusted” blockchain networks; however, the network has not necessarily been populated with trusted information. Therefore, smart contracts must verify collected owner or investor data with external vendors that specialize in KYC-compliant background checks, such as LexisNexis Risk Solutions (http://www.risk.lexisnexis.com/) and service provider in the crypto-space, PrimeTrust (http://www.primetrust.com/).

Regulators have feared from the inception of blockchain token technology that these networks would be a gathering place for undesirable participants – i.e., criminals, terrorists and tax evaders. Therefore, adherence to the KYC protocols will require more than just safekeeping of key data. It will also require the belt-and-suspenders approach to utilizing external service providers to process and verify the information, provide verification of identify, flag and restrict problematic participants, and continuously monitor these components.

Further, the statement also emphasized the need to be diligent against money laundering and the financing of terrorism. Indeed, much of this approach starts with the KYC protocols, but you must realize that the flexibility and automation of smart contracts can also be a source of tainted funds or funds to be used for nefarious purposes.

The benefits of cryptocurrencies can also represent the greatest threats to their use. This is often the case with innovative products and processes. Thus, innovation that complies with regulation offers the best chance of taking root and flourishing. For example, it is possible to establish an anonymous wallet for holding cryptocurrencies and STOs. Generally, most wallets are not considered completely anonymous because they contain a private and a public key; a public key can typically be traced back to a specific server, which could identify the user. However, the problem is that it is entirely possible to set up an entirely anonymous wallet by taking some low-tech steps: 1) use a TOR browser (browser for maintaining anonymity) in order to set up a software wallet, and 2) use a burner email (temporary and fake email account) in order to finalize the wallet setup. You now have a public key which is not affiliated with an identifiable email or server. How does that entirely anonymous wallet square with the regulatory environment? And how does that cryptocurrency capability encourage adoption when it acts as its own worst regulatory enemy?

You can also transact in a clandestine fashion by avoiding the popular coin exchanges and purchasing cryptocurrencies directly from a holder in a private transaction, or even through bitcoin ATMs! If you have set up several anonymous wallets, you can proceed to mix coins across several accounts, which will break the informational capture of sender and receiver of the coins despite the FATF “travel rule” recommendations (https://www.fatf-

gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html) earlier this year, which requires exchanges to collect, share, and store personal information about transactions. Certain aspects of the technology as applied can now make the actual transaction harder and harder to trace.

With this reality, Anti-Money Laundering protocols become difficult to execute. Wallets can be maintained away from the scrutiny of compliance staff at financial institutions. Money/coin transfers can happen with little traceability. All of a sudden, you do not know the true source of the cryptocurrency that you have in your wallet.

It begs a sensible next question that should be considered if you're involved in any Security Token Offering or other transaction where you are preparing to accept cryptocurrencies: Should you accept an investment/subscription payment in Bitcoin or Ether, and/or pay dividends in the same? We would argue that hesitation in this space is warranted. We have typically advised Security Tokens to be offered in U.S. Dollars, and for dividends/distributions to be paid in U.S. Dollars, thus avoiding the possibility of transacting in tainted cryptocurrencies. The statement from the three regulators puts the onus for enacting and maintaining AML safeguards on the STO issuers and associated service providers. Belt and suspenders again!

[Related video: "Cryptocurrencies' Messy Legal Framework Might Surprise You: Katherine Cooper, Murphy & McGonigle (https://tabbforum.com/videos/cryptocurrencies-messy-legal-framework-might-surprise-you-katherine-cooper-murphy-mcgonigle/)"]

STATEMENT 3: IRS issues additional guidance (https://www.irs.gov/newsroom/virtual-currency-irs-issues-additional-guidance-on-tax-treatment-and-reminds-taxpayers-of-reporting-obligations) on tax treatment and reminds taxpayers of reporting obligations

If we trade in virtual currencies, do we need to report and pay virtual taxes? We're just asking …

On Oct. 9, 2019, the U.S. Internal Revenue Service (IRS) announced: *"As part of a wider effort to assist taxpayers and to enforce the tax laws in a rapidly changing area, the Internal Revenue Service today issued two new pieces of guidance for taxpayers who engage in transactions involving virtual currency."*

In particular, the IRS stated that cryptocurrencies are treated as property, and therefore, general tax principles applicable to property transactions apply accordingly. Well, this seems to make sense, and it involves the tax impact upon realization of gains and/or losses, with a conversion back into U.S. Dollars.

Furthermore, they specify that if you are paid in cryptocurrencies, then income is income. And it is a burden of the recipient to calculate the fair market value of cryptocurrency paid as wages, measured in U.S. dollars at the date of receipt.

They also gave clarification on hard fork events, when a:

> *"crypto-currency undergoes a protocol change resulting in a permanent diversion from the legacy distributed ledger. This may result in the creation of a new crypto-currency on a new distributed ledger in addition to the legacy crypto-currency on the legacy distributed ledger. If your crypto-currency went through a hard fork, but you did not receive any new crypto-currency, whether through an airdrop (a distribution of crypto-currency to multiple taxpayers' distributed ledger addresses) or some other kind of transfer, you don't have taxable income."*

Whew!

If you do receive new crypto-currencies as a result of a hard fork (regardless of an airdrop or not), then the IRS considers that you have two distinct assets, which requires you to recognize a closing transaction on the first cryptocurrency, thus generating a gain or a loss.

Most important, the IRS left us with a message to ponder, regarding the reporting of the above mentioned activities:

> *"The IRS is aware that some taxpayers with virtual currency transactions may have failed to report income and pay the resulting tax or did not report their transactions properly. The IRS is actively addressing potential non-compliance in this area through a variety of efforts, ranging from taxpayer education to audits to criminal investigations."*

We believe the IRS adding crypto disclosure to its tax form shows the inroads crypto and digital assets have made to the general public.

Finally …

We do not believe that the crypto-asset world is finished seeing new rules and statements from regulators. It is critical to stay on top of these developments and become adaptive to the changing landscape. Whether we are addressing anti-money laundering protocols or addressing the need for tighter controls around investor solicitations, we promote the “belt and suspenders” approach of “Being Smart About Your Smart Contract.”

This article previously appeared on Medium.com (https://medium.com/altcoin-magazine/being-smart-about-your-smart-contract-follow-up-to-being-secure-about-your-security-token-9d9ae19b2b30). For more information on these subjects, please contact:

- *Author: Barry Seeman at seeman@bearrunpartners.com (http://barry.seeman@bearrunpartners.com) / www.bearrunpartners.com (http://www.bearrunpartners.com)*
- *Co-Author: Susan Joseph at joseph1786@gmail.com (http://susan.joseph1786@gmail.com) / www.linkedin.com/in/susangjoseph/ (https://www.linkedin.com/in/susangjoseph/)*

© 2009-2019 by The TABB Group, LLC and contributors