# A Road Map For A Cryptocurrency Crackdown: Part 1

By **John Reed Stark** (August 1, 2019)

John Reed Stark

In a thunderous tweet storm on July 11 at 8:15 p.m., President Donald Trump officially lambasted Bitcoin and all other cryptocurrencies, stating:

**Donald J. Trump**
@realDonaldTrump

I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behavior, including drug trade and other illegal activity....

72.4K 8:15 PM - Jul 11, 2019

39.3K people are talking about this

**Donald J. Trump**
@realDonaldTrump

Replying to @realDonaldTrump

....Similarly, Facebook Libra's "virtual currency" will have little standing or dependability. If Facebook and other companies want to become a bank, they must seek a new Banking Charter and become subject to all Banking Regulations, just like other Banks, both National...

46.9K 8:15 PM - Jul 11, 2019

12.8K people are talking about this

**Donald J. Trump**
@realDonaldTrump

Replying to @realDonaldTrump

...and International. We have only one real currency in the USA, and it is stronger than ever, both dependable and reliable. It is by far the most dominant currency anywhere in the World, and it will always stay that way. It is called the United States Dollar!

50.7K 8:15 PM - Jul 11, 2019

16.5K people are talking about this

Not surprisingly, the cryptocurrency market, which tends to feed on attention, celebrated Trump's tweets. In fact, many in the cryptocurrency community brazenly spun Trump's tweets as validation that cryptocurrencies have finally arrived as a staple of global finance.

Brian Armstrong, CEO at digital currency exchange Coinbase Inc., tweeted to his more than 300,000 followers:


Meanwhile, the Bitcoin marketplace bought into Armstrong's spin, and Bitcoin's price, which had surged during the month prior, did not fall, but rather rose more than 2% to $11,636 after the president's tweets.

Few media outlets reported the president's first-ever crypto tirade, yet the statements were actually quite newsworthy. First off, Trump's position aligns him most closely with an array of loud and active cryptocurrency critics and skeptics, who also happen to be some of the most virulent anti-Trump Democrats, including Rep. Maxine Waters, D-Calif., Sen. Elizabeth Warren, D-Mass., and Rep. Brad Sherman, D-Calif.

Trump is also lining up against some of his own political appointees and advisers. Last year, Steve Bannon, former White House chief strategist, boasted that digital currencies "are the future," while Mick Mulvaney, acting White House chief of staff and director of the U.S. Office of Management and Budget, has also been vocal about his support of cryptocurrency and the benefits of blockchain.

Similarly, Commissioner Hester Peirce of the U.S. Securities and Exchange Commission would also likely disagree with the president. Digital currency supporters have dubbed the Trump appointee "Crypto Mom" after her now infamous dissent in an SEC decision to reject an exchange-traded fund offering bitcoin exposure.

Even more significant than the political oddities of Trump's crypto position are its ramifications on the cryptocurrency marketplace. What should the cryptocurrency industry and marketplace expect now that the White House has officially taken such a clear and unqualified anti-cryptocurrency position?

This three-part series drills down into some of the best strategic options to orchestrate a cryptocurrency sweep, including the utilization of gatekeeper theory to focus prosecutorial and regulatory efforts on the many cryptocurrency financial platforms, custodians and other intermediaries who control access to cryptocurrency markets.

In other words, by taking on the conduits and go-betweens cryptocurrency users pay to trade and convert the cryptocurrency obtained from their extortion schemes, murder plots and other nefarious activities, Trump could have a dramatic impact on the cryptocurrency marketplace.

Part one discusses:

- Background regarding the dangers of bitcoin and other cryptocurrencies, especially the recent spate of crippling ransomware attacks on municipalities; and
- Enforcing the range of anti-money laundering, know-your-customer and other federal financial compliance and licensure requirements that apply to the cryptocurrency marketplace.

Part two discusses:

- Enforcement of state and corresponding federal money transmitter registration requirements pertaining to cryptocurrency financial intermediaries;
- Prosecuting cryptocurrency trading firms that facilitate cryptocurrency transactions for violating U.S. economic and trade sanctions; and
- Subpoenaing cryptocurrency financial intermediaries — including public corporations who facilitate crypto-related transactions— to identify and prosecute those who have transacted in cryptocurrency and enjoyed crypto-related capital gains, but not paid capital gains tax.

Part three discusses:

- Prosecuting cryptocurrency trading platforms, token custodians, digital wallets and other financial intermediaries that violate SEC statutes, rules and regulations; and
- Some final thoughts for the road ahead.

**Spotlight: Ransomware Extortion Schemes and Municipalities**

Because transactions in cryptocurrencies like bitcoin are pseudo-anonymous, encrypted, decentralized and largely unregulated, one of the more prominent criminal uses of bitcoin to emerge involves ransomware schemes, and provides the most glaring example of how nefarious cryptocurrency has become.

Here is how a typical ransomware extortion scheme works:

- Ransomware attackers break into a corporate system and encrypt, or lock up, a corporate victim’s data. Most ransomware infections come from phishing attacks, in

which unwitting users are enticed to open a file or click on a link containing the ransomware malware.

- The ransomware attackers demand payment in cryptocurrency for the encryption key to enable the victim corporation to unlock the now inaccessible data.

- The ransomware victim pays the cryptocurrency ransom to the attacker.

- The ransomware attackers move on to their next victim.

Ransomware attackers can cripple significant portions, or even all, of a company's technologically facilitated operations. Hence ransomware's dirty little secret: Most corporations pay the ransom. How do most corporate victims of ransomware attacks pay the ransoms demanded?

Bitcoin: It's fast, reliable, verifiable, subject to little regulation and virtually untraceable — ideal for ransomware schemes. The attacker merely watches the public blockchain to know if and when a victim has paid up. Attackers can even create a unique payment address for each victim and automate the process of unlocking their files upon a confirmed bitcoin transaction to that unique address.

Unlike the sequence of events during a kidnapping scenario, where the exchange of money arguably places criminals in their most vulnerable position, ransomware attackers can collect with far less risk. Rarely is there an arrest, let alone a successful prosecution, of a ransomware attacker. Law enforcement remains virtually powerless, and has even fallen victim to ransomware extortion schemes.

In particular, ransomware attacks have begun to plague townships, counties, cities and other municipalities across the U.S. According to a recent report from Coveware, public-sector victims pay an average of $338,700 in ransom per incident. In June and July alone, at least three Florida cities became victims of ransomware attacks, after similar attacks on larger cities such as Atlanta, Dallas and Baltimore.

In Lake City, Florida, more than 100 years' worth of municipal records — from ordinances to meeting minutes to resolutions and city council agendas — were locked in cyberspace for nearly a month, hijacked by unidentified hackers who encrypted the city's computer systems and demanded 42 bitcoins — more than $460,000 at the time — to pay the ransom.

Riviera Beach, in Florida's Palm Beach County, signed off on an extraordinary $600,000 payment around the same time, also in bitcoin. The Village of Key Biscayne, Florida, has not publicly disclosed whether it plans to pay the perpetrators of a recent ransomware attack, while earlier this year Jackson County, Georgia, paid $400,000. Atlanta's mayor testified recently to Congress that the city refused to pay $51,000 in extortion demands from an attack last year, costing Atlanta $7.2 million to date.

**Trump's Cryptocurrency Options**

Legal commentators often lament that the U.S. financial regulatory structure was not designed to tackle the technical complexities of cryptocurrency, harping on the dysfunction that results when no single federal agency wields comprehensive authority over its many varying elements. However, what these legal commentators are missing is that cryptocurrency's jurisdictional maze and lack of precedent is actually a strength, not a

weakness.

Even when there is an absence of fraud, some prosecutorial and regulatory agencies can charge cryptocurrency market intermediaries for failures relating to federal compliance and licensure requirements. These include:

- Criminal prosecutorial agencies like the U.S. Department of Justice;
- Civil enforcement agencies like the SEC; and
- Financial regulatory agencies like the U.S. Treasury Department and its incumbent Financial Crime Enforcement Network, the U.S. Office of Foreign Assets Control and the Internal Revenue Service.

Each of the above agencies can expend its jurisdictional reach to investigate and prosecute crypto-related crimes by enforcing a mix of the licensure-related statutory weaponry of existing laws, rules and regulations.

In other words, even though he can't prove that an unsafe and dangerous car has been involved in a hit-and-run, Trump still has the tools to take that car off the road.

**Gatekeeper Theory**

For starters, Trump should steal a page from the playbook of Judge Stanley Sporkin, former director of the SEC Division of Enforcement. Judge Sporkin championed the principle of gatekeeper liability, premised upon what he referred to as the access theory of regulation and enforcement. With access theory, instead of pursuing every bad actor, Judge Sporkin opted instead to achieve more effective results in the long run by pursuing those who control access to our capital markets.

In the cryptocurrency marketplace, the most obvious targets for a gatekeeper assault include:

- Cryptocurrency platforms that provide cryptocurrency trading and the conversion of bitcoin and other cryptocurrencies into dollars;
- Crypto custodial services that provide digital wallet and other storage solutions for customers to safeguard and warehouse their cryptocurrency; and
- Corporate crypto facilitators that manage crypto transactions for companies seeking to accept cryptocurrency as payment for goods or services.

The best reason for gatekeeper theory? In stark contrast to the hackers and other cybercriminals who go to extreme efforts to conceal their identities, crypto gatekeepers actually want to be found. Crypto intermediaries market their services aggressively, especially via social media, which makes them easier to surveil, track and ultimately catch.

This may yet prove to be the most profound change brought by the internet on the field of law enforcement and financial regulation. Far from tying the hands of investigators and prosecutors, the internet has become the virtual rope that crypto gatekeepers use to hang

themselves.

**AML and KYC**

Two highly effective statutory tools for enforcement against crypto gatekeepers are the anti-money laundering and know-your-customer statutes, rules and regulations.

Pursuant to the Bank Secrecy Act, transactions involving traditional financial firms — such as banks, brokerages and money service businesses, or MSBs — are subject to strict federal and state anti-money laundering laws and regulations aimed at detecting and reporting suspicious activity, including money laundering and terrorist financing, as well as securities fraud and market manipulation.

MSBs have been required to register with FinCEN since 1999, when MSB regulations first went into effect. An entity acting as an MSB that fails to register is subject to civil money penalties and possible criminal prosecution.

MSBs are broadly defined, and have historically been recognized by FinCEN to include: (1) currency dealers or exchanges; (2) check cashers;(3) issuers of traveler's checks, money orders or stored value; (4) sellers or redeemers of traveler's checks, money orders or stored value; and (5) money transmitters.

The BSA requires an MSB to develop, implement and maintain an effective written AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. Since cryptocurrency financial intermediaries provide financial services, they are also required to verify their customers' identities before offering their services, also known as KYC.

Many financial institutions often blur the lines between KYC and AML processes. KYC mandates that customers provide verifiable and credible identification credentials in order to use a cryptocurrency company's service. Customer due diligence is a basic KYC process where customers' data, such as proof of identity and address, is gathered and used to evaluate their risk profile. Enhanced due diligence is an advanced KYC procedure, including transaction monitoring for high-risk customers prone to money laundering and financing of terrorism.

AML programs typically include a system of internal controls to ensure ongoing BSA compliance; independent testing of BSA/AML compliance; a designated BSA compliance officer to oversee compliance efforts; training for appropriate personnel; and a customer identification program.

**Cryptocurrency Firms, AML and KYC**

Given the identification and verification challenges associated with the global locations, pseudo-anonymity, encryption, decentralization and historically criminal tendencies of typical cryptocurrency users, a federal sweep of cryptocurrency intermediaries will likely identify a plethora of AML, KYC and other BSA violations.

Not only do cryptocurrency firms typically lack the sophisticated technological compliance infrastructure of traditional U.S. financial institutions, but they are also often misguided when it comes to their AML/KYC compliance responsibilities, contravening FinCEN's guidance on the application of FinCEN's regulations to persons administering, exchanging or using virtual currencies.

For instance, the New York Attorney General's Office asked 14 popular crypto trading platforms to respond to a questionnaire covering a range of topics, from trading fees to AML policies to methods for keeping customer assets secure. Ten chose to comply, and the September 2018 report of their responses illuminates the shadowy inner workings of cryptocurrency trading platforms, raising serious questions regarding the growing connection between cryptocurrency and money laundering, as well as a range of market manipulation concerns.

U.S. law enforcement agencies have already vowed to prosecute cryptocurrency custodian and conversion firms that serve criminals, even those operating outside the United States. The DOJ, acting in cooperation with FinCEN, has become increasingly active in policing criminals exploiting cryptocurrencies, leveraging AML statutes and regulations.

Some states have already taken the lead in prosecuting AML-related violations at cryptocurrency firms. Clearly, the noxious mix of AML and MSB federal and state regulatory requirements not only creates a foggy, deadly compliance labyrinth for any cryptocurrency firm, but is also replete with risk for anyone — or any U.S. state — doing business with them.

**Trump, AML and KYC**

Trump could announce a federal cryptocurrency sweep and direct cryptocurrency firms to be subject to on-site audits and scrutiny of individual transaction activity for AML compliance, which in turn could lead to institutional and management civil liability, penalties, fines, license revocation and even potential criminal exposure for individuals caught intentionally circumventing AML obligations.

For gatekeepers, like cryptocurrency firms, meeting their AML and KYC responsibilities is a Herculean task, making charging decisions easier and providing endless prosecutorial fodder, like shooting in a barrel.

Identifying the source of cryptocurrency — or in the least, confirming that a cryptocurrency is not somehow tainted by unlawful conduct — can be especially challenging. Like accepting a $50,000 roll of $100 bills, the cash's very existence raises questions pertaining to its purity. Moreover, merely because a $50,000 roll of $100 bills does not have blood stains on it, does not alleviate the obvious suspicion about its origin.

---

*John Reed Stark is president of John Reed Stark Consulting LLC. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as chief of its Office of Internet Enforcement.*