

goodcryptoxDCA bot now on SOLANA

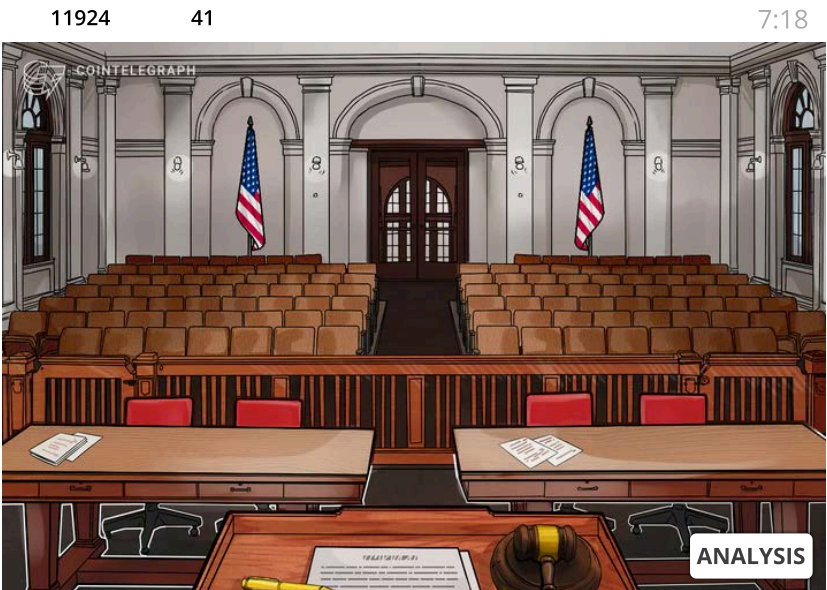
TRY NOW

 KIRILL BRYANOV

NOV 21, 2020


# The long arm of justice: How far can the DoJ really go in prosecuting foreign actors?

DoJ is now determined to hold the crypto industry to cross-border enforcement standards that have long applied to other sectors of finance.



COINTELEGRAPH IN YOUR SOCIAL FEED

Join ourSubscribe on



In early October, the U.S. Department of Justice revealed its Cryptocurrency Enforcement Framework, a report laying bare the government’s vision for emerging threats and enforcement strategies in the cryptocurrency space. The document is an important source of insight into how the laws governing digital finance will be soon implemented on the ground.

One of the fundamental principles that the government asserts in the document is its broad extraterritorial jurisdiction over foreign-based actors who use virtual assets in ways that harm U.S. residents or businesses. The guidance sets an extremely low bar for perpetrators of cross-border crime to clear before they face prosecution.

According to the framework, it can be enough for a crypto transaction to “touch financial, data storage, or other computer systems within the United States” to provoke enforcement action. Is the stringency of this approach unprecedented across other domains of financial crimes enforcement? What actual tools does the U.S. government have to counter criminals acting from overseas?

### **Business as usual**

The idea that U.S. law enforcement is justified in prosecuting criminal actors beyond the nation’s borders if their activity has adversely affected individuals, companies, or infrastructure at home is nothing new, especially when it comes to cyber and financial crimes.

Arlo Devlin-Brown, a partner in the white-collar practice of law firm Covington & Burling, commented to Cointelegraph:

“The DOJ has consistently taken the position that U.S. criminal jurisdiction extends to activity with minimal ties to the U.S., and U.S. courts have in many cases embraced the DOJ's expansive interpretation of its authority. Cryptocurrency businesses that operate outside the U.S. but have any ties to this country — bank accounts, customers, marketing activity — are at risk of enforcement action.”

Dan Newcomb, attorney at law firm Shearman & Sterling, said that there is nothing particularly extraordinary about the extraterritorial approach enshrined in the Cryptocurrency Enforcement Guidelines, as the DoJ has previously used a “wide variety of tools to hold foreign-based actors responsible for crimes punishable under U.S. law.”


The authors of the report note that the U.S. has used anti-money laundering measures against foreign actors dealing in fiat currencies for decades. Asserting similar jurisdiction over those who use digital

currencies appears to be a defensible extension of the principle already at work.

### Not new for crypto, either

The U.S. government has, on many occasions, gone after foreign persons and entities implicated in cryptocurrency-related crimes. Gail Fuller, a vice president at K2 Integrity, said that she considers the extensive extraterritorial jurisdiction asserted in the DoJ framework as “broadly consistent with the overall U.S. financial crimes compliance regime,” which is designed to protect the integrity of the U.S. financial system. Fuller commented:

“We’ve seen U.S. enforcement actions for sanctions violations and money laundering that have targeted foreign individuals or entities in cases in which their transactions touched the United States or its banks. In fact, we’ve already seen it in the cryptocurrency context, including with the 2017 indictment of foreign cryptocurrency exchange BTC-e and its Russian executive, Alexander Vinnik.”

 Ad 

Join eToro and trade cryptoassets without the hassle of wallets or private keys

[Visit eToro](#)

In Fuller’s view, the BTC-e case is particularly interesting because on top of money laundering charges, the Department of Justice charged the exchange platform with failing to register as a money services provider in the United States, based on the volume of U.S.-connected transactions it facilitated.

James Farrell, deputy general counsel at trading solutions provider Apify, sees the enforcement guidelines as the reminder to the crypto industry about something that has been well-known to the traditional finance for over a decade: If an act of financial misconduct has a substantial effect in the U.S., the SEC and DoJ can and will go after those responsible. “Stating that a single U.S. server is enough just highlights how thin a reed the DOJ needs to assert jurisdiction,” Farrell added.

To Farrell, the novel – and striking – part of the report is invocation of “protective jurisdiction” – effectively worldwide criminal

enforcement power - if the DOJ believes that the activity involving crypto may have national security implications. Farrell said:

“You see this concept enshrined in international treaties related to the taking of hostages, terrorist bombings and financing of terrorism. To hear that the same basis may be applied to the cryptocurrency industry was jarring and a marker of how seriously the DOJ is taking potential criminal misuse of this transformative and developing technology.”

### **Enforcement tools at DoJ's service**

Proclaiming jurisdiction over persons and entities that may be physically located thousands of miles away from U.S. shores is merely a symbolic move if there are no actual means for holding them accountable. U.S. law enforcement, however, commands quite an arsenal.

One heavy weapon is the degree of control that the United States' financial authorities exercise over the traditional global monetary system. Shearman & Sterling's Dan Newcomb observed to Cointelegraph:

“The key enforcement tool the U.S. has is the dominant role the U.S. dollar plays in international commerce and the fear conventional financial institutions have of being excluded from U.S. dollar transactions. Most holders of digital assets still need and want to convert those assets at some point into conventional currencies at financial institutions. Barring a digital player from access to conventional financial institutions is a powerful tool.”

Covington & Burling's Devlin-Brown said that the Justice Department can rely on a number of powerful statutes that can be used to prosecute foreign-based cryptocurrency actors:

“For example, the U.S. money laundering statute can reach almost any dollar-denominated transaction that U.S. authorities can establish as linked to many types of criminal activity. Even a dollar-denominated payment from, say, Germany to Argentina is covered because the transaction would likely involve a U.S. bank as an intermediary.”

Michael Yaeger, a white-collar crime attorney at law firm Carlton Fields and formerly an assistant U.S. attorney for the Eastern District of New York, told Cointelegraph that the DoJ report does not reveal any new instruments for prosecuting foreign-based actors.

However, Yaeger noted, the collection of past cases showcased in the document provides “useful examples of its powers, and perhaps signals which instruments will be used more in the future.”

One thing that caught Yaeger’s eye is the fact that the report seems to mention forfeiture efforts more than past DoJ reports on cyber crime:

“When forfeiture is combined with pre-judgment seizure of assets it is not only a powerful remedy, but an unusually fast one. The US has multiple cooperation agreements with other countries including data sharing agreements with foreign law enforcement and intelligence agencies, and has entered specific agreements related to forfeiture and the sharing of financial information.”

There is little doubt that the government is poised to leverage these and other international agreements in enacting its newly itemized enforcement strategy. Promoting cooperation with foreign governments and intergovernmental organizations like the FATF is listed among the crypto framework’s focal points.

The DoJ framework’s language on extraterritorial jurisdiction and cross-border enforcement may sound harsh to some. Yet, in fact the government is not articulating any principles dramatically different from those that are already being invoked in some high-profile crypto-related cases. Stating that these standards will be applied more systematically is only logical considering the expansion and maturation of the borderless realm of digital finance.

#Law #Government #Bitcoin Regulation #Police #US Government

#United States #Crimes #Department of Justice

 Add reaction

READ MORE



Crypto isn't 'run from garages' anymore: MEXC's Tracy Jin on IPO boom



Global crypto exchange weaves Web3 magic into LALIGA spectacle



Trump discloses \$57M crypto windfall from World Liberty Financial



KOLLEN POST

NOV 20, 2020

## Law Decoded: Green lights of the SEC, black flags of Binance, Nov. 13-20

Libel laws and new faces at the U.S. securities regulator lead the week's news.

48594

45

5:56



COINTELEGRAPH IN YOUR SOCIAL FEED

Subscribe on

Subscribe on



### Editor's note

Amid a political news cycle that has been stuck in a nauseating loop, covering crypto is often refreshing. Partisan forces have yet to dig out the trenches. A lot of the current task is just getting working definitions in play.

Meanwhile, the technology advances at a mind-boggling rate, and there are still enough outrageous scams, absurd tomfoolery and indeed general skulduggery to keep everything from getting dull.

Speaking of skulduggery, I will begin this week with a comment on a challenge to journalism in the crypto industry that has wide-spanning implications. Not many people think about the relationship between the law and journalism. At its best, journalism is egalitarian in whose toes it steps on — whether they're bigwigs in government or private industry, with obvious bonus points for size. Just so long as you're exposing what those people want to keep hidden.

The concept of the strategic lawsuit against public participation, or SLAPP suit, is that you don't need to win to shut someone up — whether that's a public whistleblower or, often, a journalist. It's a nasty legal invention that depends on an entity having more resources to burn on a lawsuit than the defendant has to defend him or herself. With that bit of prologue, we're starting with a defamation lawsuit from one of the biggest names in crypto.

[Explore more articles like this](#)

**Subscribe to the Law Decoded newsletter**

Arm yourself with the latest on crypto laws and guidelines to make smart choices for your crypto ventures. Delivered every Monday



**Subscribe**

By subscribing, you agree to our  
[Terms of Services and Privacy Policy](#)

## **Binance sues Forbes in the U.S. for accusing exchange of operating in the U.S.**

Binance Holdings, the parent company of the global exchange but, they claim, not of Binance.US, is [suing journalists](#) Michael del Castillo and Jason Brett and publication Forbes for libel.

The pair wrote a piece accusing Binance of using a scheme of concealed corporate ownership to get funds from operations in the U.S. back to the mothership. Binance's plight in this case would likely



be more sympathetic if the firm didn't have a record of concealing its ownership and registration location. It's a lack of transparency that means nobody is quite sure where the largest crypto exchange in the world is based and whose laws it answers to. In a positive light, it's sort of like pirate radio back in the '60s UK, going offshore to broadcast the Who to unsuspecting Britons. In a negative light, it's more like regular old pirates, coming to shore only when they want to do some pillaging.

The case, filed in New Jersey's district court, seems unlikely to turn out in Binance's favor, but that's hardly the point. CEO Changpeng Zhao has a longstanding contentious relationship with reporting on the company. In the past year, he has used Twitter to threaten to hit TheBlock with a similar libel suit, and once casually referred to Cointelegraph's staff as "evil journalists."

Trying to intimidate journalists, as mentioned above, is nothing new. SLAPP lawsuits have become part of the game, and with companies operating across such a wide range of jurisdictions, many do a fair bit of jurisdiction shopping. Fortunately for del Castillo, Brett and Forbes, New Jersey is fairly protective of its journalists. Such suits, however, have a chilling effect on efforts to shine light on opaque businesses like Binance.

### **SEC signs off on third token as not a security**

The U.S. Securities and Exchange Commission sent out only its third no-action letter to a token issuer, allowing social media platform IMVU to sell and buy its VCOIN to and from users.

The SEC has long been a major stumbling block for firms looking to issue crypto tokens. Many in the industry chafe at the lack of solid guidance as to what the SEC does not consider a security. As firms like Telegram and Facebook found out, such definitions are important.

The two earlier no-action letters from the SEC were for projects that were extremely limited in scope. The SEC was providing pretty flimsy support for tokens on tiny platforms with single uses that, critically, did not allow users to turn those tokens back into fiat currency.

Per this week's no-action letter, VCOIN will not be available to trade on any outside platform and will stay at a fixed price that IMVU has committed to buy and sell at, providing an unlimited supply. The idea here is to avoid the "expectation of profit" prong of the Howey



Test, which the SEC uses to determine investment contracts. Which is all par for the course.

IMVU's wide user base AND the ability of those users to transact VCOIN among themselves before selling them back to platform in exchange for fiat currency is a huge leap forward for the SEC's comfort with crypto. Maybe, as the guard is changing, the people in charge are trying to open the gate. Speaking of which...

### **The guard is changing at the SEC**

This week, the SEC also announced that Jay Clayton, who has been chairman of the commission since 2017, will step down by the end of the year. Coming just a week after Bill Hinman, director of the Division of Corporate Finance, made a similar announcement, the SEC's leadership is poised for a major turnover.

Such a turnover is not a complete surprise. Clayton has been known to be looking to leave the SEC for some time. He in fact fell into a somewhat scandalous situation when President Trump and Attorney General Barr tried to jam through his nomination to serve as prosecutor in the Southern District of New York after an apparently chummy golf outing between Trump and Clayton.

Moreover, regulatory staffs often track alongside shifts in presidential administrations. Trump and Senate Republicans have been charging through a roster of nominations in what may be the clearest indicator that they don't actually believe Trump won this month's election. Clayton's timed departure, however, should put nomination of the SEC's new leadership firmly in the hands of a Biden administration. Given that the Senate will be deadlocked or with a slight Republican majority, it's likely going to be a fairly moderate candidate, but certainly one not as laissez-faire as Clayton.

### **Further reads**

The Electronic Frontier Foundation has put out a new project to educate the public on browser fingerprinting and tracking.

Legal analysts for Bloomberg Law analyze the charges against BitMEX and the exchange's leadership in the context of AML requirements for crypto.

Lawyers for Pilsbury write on the developing role of blockchain and tokenization in fractional real estate ownership and trading.

#Law #Government #SEC #Bitcoin Regulation #US Government  
#Cryptocurrency Exchange #Binance

😊 Add reaction

READ MORE





Crypto isn't 'run from garages' anymore: MEXC's Tracy Jin on IPO boom



Global crypto exchange weaves Web3 magic into LALIGA spectacle



Trump discloses \$57M crypto windfall from World Liberty Financial



Losing access isn't bad luck.  
It's bad setup. **Go offline.**

Ad

BUY NOW

Save 10% with  
CORTELEGRAPH code



JOSH O'SULLIVAN

JUN 13, 2025

Why do we fall for crypto scams? Understanding human vulnerability in the digital age

How overconfidence, FOMO, and emotional manipulation can lead to losing \$850,000 in crypto. What can we learn from these real-life cases to protect ourselves from falling for similar scams?

3412

6:12



Presented by **Crystal**

- 1. Introduction**
- 2. FOMO — 'It's too good to be true'**
- 3. The trust trap — 'Betrayal from within'**
- 4. The power disadvantage — 'There is no other option'**
- 5. Picking ourselves up: Learning from others' mistakes**

## 1

### Introduction

The world of crypto is unpredictable, and many people experience similar falls before they learn to protect themselves. Scammers prey on emotional and psychological weaknesses, manipulating greed, fear, and misplaced trust—tactics that affect everyone, even seasoned experts.

Why do people fall for these scams, and what psychological triggers lead them astray? By understanding how these schemes work, we can rise from each fall and be better prepared to protect ourselves from future threats.

## 2

### FOMO — 'It's too good to be true'

Scammers can often establish a sense of immediate urgency around a seemingly lucrative opportunity before exploiting a victim's fear of missing out (FOMO).

There is an interesting type of scam that preys on victims' greed, tricking them into believing they can steal someone else's money while, in reality, they end up sending their own money to scammers. It typically begins when the victim "accidentally" receives a message stating, "Your account has been created," accompanied by a link to an exchange platform and login credentials. Out of curiosity, the victim logs in and discovers a substantial balance — let's say \$10,000 — sitting in the account.

Lured by the prospect of easy money and driven by greed, the victim tries to withdraw the funds. However, they are told there's a withdrawal limit and that they need to top up the account with, say, \$1,000 to unlock the full \$11,000. After sending this money, they discover (or sometimes don't) that the website is fake, and instead of gaining any funds, they have sent their own money to scammers, losing both the money they deposited and the fake funds they were hoping to withdraw.

**Why we fall:** The desire for opportunity, paired with FOMO, drives impulsive decisions that override caution, making even the most prudent individuals susceptible to greed and scams.

### 3

#### The trust trap — 'Betrayal from within'

Fraudsters frequently take advantage of positions of authority and hide in plain sight to carry out their scams.

Take, for example, a company that decided to handle its own crypto payment processing in-house, relying on the expertise of its talented engineers. Confident in their ability to bypass expensive third-party services, they stored funds directly in a company wallet. Months later, a vigilant financial controller noticed something troubling: while ad sales had surged, the expected revenue was nowhere to be found.

An internal investigation revealed that a subtle tweak in the payment system had funneled millions in crypto to an unknown destination. Despite their best efforts, the company never recovered the lost funds — and never found out who was responsible.

**Why we fall:** We naturally trust those we are close to - like family, friends and colleagues. This gives us the sense that we would never be betrayed - a vulnerability that can easily be exploited.

### 4

## **The power disadvantage — ‘There is no other option’**

Targeted exploitation is a common method used by scammers. They take advantage of their victims when they're most financially or emotionally vulnerable — using desperation, greed or even hope against them. They use privileged information to strategically choose their victims, making this a form of calculated manipulation.

In a disturbing example of such exploitation, Russian-speaking ransomware gang REvil hackers specifically targeted companies insured against ransomware attacks. After infiltrating a US-based insurance firm, they accessed a list of clients covered for such incidents and deliberately went after those companies, knowing they were more likely to pay the ransom.

Why it worked: Power disadvantage. The scammers held full power, knowing their targets would rather pay up than allow their data to go public, which would have further expensive repercussions. There was simply no other option for the victims.

## **5**

### **Picking ourselves up: Learning from others' mistakes**

Participants in the crypto ecosystem can strengthen their security practices and make them habitual by learning from others.

One striking case involved Dutch law enforcement's takedown of the Hansa darknet market. After arresting the two German operators and seizing the servers from Lithuania, they didn't shut the market down immediately. Instead, they allowed it to continue operating for another month, silently monitoring over 1,000 daily transactions.

This covert strategy allowed authorities to collect critical data on more than 10,000 users and their addresses. When the market was finally taken offline, the operation had provided a treasure trove of intelligence, which was shared with Europol. This led to widespread arrests and a significant blow to the darknet underworld.

This case highlights how proactive observation, continuous education and a well-executed strategy can turn the tide against even the most elusive scammers. Falling for a crypto scam doesn't mean someone is unintelligent or foolish — it means they're human. Scammers thrive on exploiting vulnerabilities, from overconfidence to emotional desperation.

However, understanding the psychological tactics they use is key to preventing future attacks.

Understanding the psychological triggers scammers use to manipulate funds from users' wallets to theirs is key to understanding how to prevent becoming a future victim.

How we rise: Learning from the experiences of others, staying educated and practicing vigilance are the most powerful tools for protecting ourselves from scams. By developing stronger habits, enhancing our awareness and using available tools, we can turn potential downfalls into opportunities for growth and security in the digital asset world.

Companies like Crystal, a blockchain intelligence company, help governments, crypto businesses, and financial institutions investigate cryptocurrency crimes. Using real-time blockchain intelligence tools, like transaction monitoring and aggregated transaction visualization, Crystal helps law enforcement agencies and companies make quick, informed decisions against crypto-related threats.

### Find out more about Crystal

**Disclaimer.** Cointelegraph does not endorse any content or product on this page. While we aim at providing you with all important information that we could obtain in this sponsored article, readers should do their own research before taking any actions related to the company and carry full responsibility for their decisions, nor can this article be considered as investment advice.

#Blockchain #Cryptocurrencies #Fraud #Adoption #Scams

## READ MORE



Circle's NYSE debut marks start of crypto IPO season: Are Kraken, Gemini and Bullish next?



Global crypto exchange weaves Web3 magic into LALIGA spectacle



Walmart, Amazon consider issuing own stablecoins: WSJ







## Poloniex exchange goes down on the brink of new Bitcoin all-time high

When all eyes are on Bitcoin, exchanges sometimes suffer difficulties.

21329

59

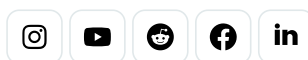
1:10



COINTELEGRAPH IN YOUR SOCIAL FEED

Follow our

Subscribe on



With a new all-time price high in sight for Bitcoin, crypto exchange Poloniex recently went offline.

“Poloniex is currently unavailable due to an unexpected issue,” the exchange’s customer support Twitter page said on Friday. “We are investigating the issue and will keep you updated here throughout.”

Bitcoin has yielded exuberant upward price action in recent weeks, as well as catching growing attention. When traffic becomes dense on exchanges, their systems sometimes go down, locking out traders. This has happened with other exchanges in the past as well, including BitMEX and Coinbase.

“Poloniex is now out of maintenance mode,” Poloniex posted in a follow-up tweet. “Our spot and margin markets are in post-only mode and withdrawals are temporarily unavailable.” A subsequent update stated the return of futures contract trading on the platform.



Meanwhile, Bitcoin remains painfully close to its all-time price high near \$20,000. This year has seen a significant amount of mainstream financial attention on the asset. Paul Tudor Jones, Jack Dorsey's Square and MicroStrategy have all jumped on board, buying big positions in the digital coin.

Cointelegraph reached out to Poloniex for additional details, but received no response as of press time. This article will be updated accordingly should a response come in.

UPDATE Nov. 20, 22:03 UTC: This article has been updated, reflecting Cointelegraph's request for comment.

#Business #Bitcoin Price #Cryptocurrency Exchange #Poloniex  
#Trading

 Add reaction

## READ MORE



Saylor says Bitcoin could fix Apple's stock buybacks:  
Finance Redefined



Global crypto exchange weaves Web3 magic into  
LALIGA spectacle



How to use Grok for real-time crypto trading signals



Are you a journalist or an editor?

Join us



#### MOBILE APPS



#### COINTELEGRAPH NEWSLETTER

Email

Subscribe

Cointelegraph covers fintech, blockchain and Bitcoin bringing you the latest crypto news and analyses on the future of money.

[Terms of services](#) and [Privacy policy](#)

© Cointelegraph 2013 - 2025

Cointelegraph is committed to providing independent, high-quality journalism across the crypto, blockchain, AI, fintech, and iGaming industries. To support the free use of our website and sustain our editorial operations, some of the links published on our site may be affiliate links. This means we may receive a commission if you click through and take action—such as signing up for a service or making a purchase. These commissions come at no additional cost to you. Our affiliate relationships help us maintain an open-access platform, but they do not influence our editorial decisions. All news, reviews, and analysis are produced with journalistic independence and integrity. Thank you for supporting responsible and accessible reporting.