4800 Hampden Lane, Suite 200, Bethesda, Maryland 20814
www.johnreedstark.com

Crypto Task Force Roundtable (West Coast Mini Edition), Enforcement Forum West
John Reed Stark, President, John Reed Stark Consulting LLC
May 16th, 2025

"White Paper and Receipts: A Stark Response Regarding Crypto-Crime (Which is Mammoth) and Judicial Decisions Declaring Digital Assets to be Securities (Which are Myriad and Definitive)"

That was then, this is now.

Once upon a time, decades ago, the world experienced the genesis of a new database worksheet based upon a blockchain, a shared, immutable ledger, which can facilitate the process of recording transactions and tracking assets in a computer network. The emergence of blockchains, later spawned a new breed of equations – so-called cryptocurrencies -- and a new legion of entrepreneurs – so-called crypto-bros -- who peddled cryptocurrency to the masses.

These crypto-bros pledged a *Fourth Industrial Revolution*, delighting the masses with promises that blockchain and crypto-tokenization would transform the planet, reinventing financial systems, revolutionizing the efficiency of transactions, democratizing wealth, creating a newfangled, self-governing private currency and doing whatever else the crypto-entrepreneurs could conjure up, even curing cancer.

Given crypto's inherent limitations, rather than inventing ways to use crypto technology for a product or service, the crypto-bros instead used crypto technology as a means to raise cash from investors (fiat currency) by selling their computer-generated crypto tokens (mathematical equations of computer code) in "initial coin offerings" (ICOs) which they described in so-called "White Papers."

Crypto-bros promised investors *get-rich-quick* profits and built online trading facilities for their ICOs to trade, calling these platforms "exchanges," where investors could buy-and-sell their tokens 24-7, and where investors could prosper without the interference and oppression of the

heavy hand of government. The crypto-bros targeted especially the unbanked and disenfranchised, guaranteeing a new frontier of investor empowerment.

Unlike actual initial public offerings or "IPOs," the crypto-bros did not register their tokens, nor file their White Papers, in compliance with U.S. federal securities laws. Instead, the crypto-bros bypassed traditional market regulation, proudly selling their crypto tokens directly to the public. This meant that crypto-bros did not provide audited, comprehensive and detailed disclosures to crypto-investors, thereby circumventing and undermining the entirety of U.S. federal securities regulation.

At the same time, the crypto-trading "exchanges," similarly ignored U.S. securities laws and were not subjected to rigorous inspection, audit or examination, robust record-keeping obligations, critical net capital requirements, mandatory cybersecurity safeguards, strict licensing of salespeople and so many other crucial investor protections.

Issuing an ICO or running a crypto-exchange was as care-free as a backyard garage sale – and the crypto bros loved it. Above all else, the ICO projects underscored the remarkable ease with which crypto bros could unilaterally raise substantial capital from enthusiastic retail investors by pitching billions of units of computer code that incurred negligible costs to create. ICO projects had somehow miraculously converted computer code into billions of dollars through sales transactions (all without the cost and burden of adhering to U.S. securities laws).

Crypto typically had no cash flow, no yield, no employees, no management, no balance sheet, no product, no service, no history operations, no earnings reports, no proven track record of adoption or reliance, and the list goes on (and on). This boundless regulatory and data vacuum prohibited any financial analyst, let alone any everyday investor, from conducting a proper valuation.

The cryptoverse soon grew exponentially, as the crypto-bros adopted a unique and extremely effective modus operandi. Specifically, crypto-bros transformed victims into victimizers, incentivizing legions of crypto investors to further spread the gospel of crypto to other future victims. The process was twofold: first, they hijacked the earnest libertarian ethos of their victims and then, they metastasized that ethos into a cancerous morass of mathematical computational code ideal for speculation and even more ideal for crime (especially ransomware attacks), terrorism (especially nuclear weapons development of rogue nations) and predatory inclusion (especially exploitations of people of color).

In just a few years, the crypto-bros grew up, becoming overnight millionaires (even billionaires), while rebranding their crypto as "digital assets" and rebranding themselves as "global digital asset financiers."

It was the dawning of a new era of business and economics, replacing a hundred years of traditional and heavily regulated financial markets with a *Walking Dead-like* post-apocalyptic anarchical commercial free-for-all.

Not surprisingly, "many, many ICOs turned out to be complete vaporware, either frauds or functionally indistinguishable from frauds," and the crypto-marketplace instantaneously presented a *drivers-ed film* of flagrant violations of the securities laws, especially registration failures, market manipulation violations and a litany of other kinds of fraud and deceit.

The newly created cryptoverse would have flourished ad infinitum but for one independent federal agency, the U.S. Securities and Exchange Commission (SEC), the governmental arm that is primarily charged with protecting investors and enforcing the securities laws. The SEC understood that despite the innocent aspirations of many earnest crypto-investors, the cryptoverse's blatant disregard for a century of investor protection was not good for anyone, anywhere.

To the SEC staff, they had no choice but to act in the face of this conduct. Without the SEC's vigorous enforcement, these digital financial behemoths would continue to operate in the shadows, with no transparency, no consumer protections and no accountability, putting both investors and markets at risk.

Fortunately, the SEC was undeterred by the crypto-financiers and their FOMO hype of blockchain and tokenization. Since 1934, SEC enforcement has addressed emerging issues with common sense and flexibility, and without the benefit, or the hindrance, of detailed prescriptions, including for policing foreign bribery payments, municipal securities fraud, derivatives scams, unlawful insider trading, fictional prime bank instruments, subprime grifts, non-existent eel farms, bogus ostrich farms and the list goes on.

So-called digital asset investors were betting on the efforts of the promoters and originators of these digital assets. That triggered the '33 Act.

So-called digital asset trading platforms were coopting the nomenclature of the securities industry, calling themselves "exchanges," "brokers," and "market-makers," creating a counterfeit veneer of investment-related assurances, integrity, expertise and regulatory supervision. That triggered the '34 Act.

To combat crypto-related securities violations, the SEC created the *Crypto Assets and Cyber Unit*, a specialized group of enforcement staff who initiated a regulatory onslaught against crypto-issuers and trading platforms, filing over 200 crypto-related enforcement actions, charging crypto-financiers for failing to register their projects and operations with the SEC (and winning just about all of their enforcement actions) .

Although crypto-financiers did everything they could to bypass the securities laws and evade SEC scrutiny, including reinventing, revamping and recalibrating their ICOs into different variations, such as "Simple Agreements for Future Tokens" (SAFTS), crypto-lending programs, crypto-staking programs and a slew of other crypto-concoctions and iterations, the crypto-financiers kept losing in court, time and time again. The SEC's crypto-enforcement program soon became a gargantuan prosecution machine, churning out new cases and new victories almost weekly.

But that was then, and this is now.

Despite the obvious dangers of digital assets, the SEC has now, suddenly, opted to demolish its crypto-enforcement program, dismissing or "pausing" a broad swath of crypto-related enforcement litigation, appeals and investigations, including those involving Coinbase, Binance, OpenSea, Uniswap, Consensys, Cumberland, Kraken, Gemini, Tron and Ripple (and a slew of other major SEC crypto-related actions will soon likely follow).

At the same time, acting SEC Chair Mark Uyeda cancelled the SEC Crypto Unit, secretly "disappeared" one of its co-chiefs, and gutted its ranks while simultaneously rebranding the unit as the "Cyber and Emerging Technologies Unit," sardonically referred to internally by SEC staff as "C2." (Apparently, it's "Back to the Future" in the SEC Enforcement Division. It was 27 years ago that the SEC, under the leadership of then-enforcement director Richard H. Walker, created the "Office of Internet Enforcement," to do pretty much the same thing as "C2.")

So, what happened? How could the SEC suddenly embrace such a profound and radical 180 degree crypto-turnabout?

Well, it turns out that the crypto-industry did not like the idea of SEC registration – they would be forced to answer tough questions about why investors should invest in their tokens and forced to allow the SEC to examine, inspect and audit their books, records and operations. So, in 2023, crypto-financiers decided that instead of paying millions to their lawyers to lose every court battle (throwing good money after bad), the crypto-financiers opted for a new forum and a new playing field to battle the SEC – elections. Along these lines, the crypto-financiers donated hundreds of millions of dollars to political candidates who supported the "innovation" of crypto and who were willing to add their voices to the growing chorus of voices vilifying a rogue and antiquated SEC.

For the crypto-financiers, their strategy paid off handsomely at the ballot box and they won bigtime, successfully buying an election. Rarely in American politics has a new industry spent so much money with such success, in such a short amount of time, as the cryptocurrency financiers did. Indeed, "Big Crypto," became the most sophisticated, effective and successful lobbying cartel in history – and the talk of the town in D.C. political circles.

Since the 2024 election, the SEC has summarily embraced the Big Crypto viewpoint, working side-by-side with crypto-firms, in partnership, resolutely decreeing that previous SEC leadership (both Republican and Democratic Chairs):

- *Suppressed innovation and ceded America's technological leadership by failing to provide the digital asset industry with "regulatory clarity;*

- *Violated the "Due Process" rights of legitimate firms by failing to provide "Fair Notice" that certain digital asset transactions and business models violate the law; and*

- *Exceeded its authority and was an irresponsible and runaway regulator led by the sinister SEC Chair Gary Gensler, who practiced "Regulation by Enforcement" and restricted technological progress and investor empowerment.*

SEC Chair Gensler resigned at 11:59 AM on January 20, 2025 and within almost minutes, newly anointed Acting SEC Chair Mark Uyeda proudly proclaimed that the crypto-days of yesteryear were no more. Chair Uyeda decreed that Gensler's SEC had exploited the SEC's catalogue of antiquated statutes to stifle innovation, to strip individuals of their fundamental entrepreneurial rights and to wreak havoc upon crypto's rightful vision of technological transformation.

To further his vision, today we begin fidelity to Chair Uyeda's new SEC crypto specialized group, the antithesis of the SEC Crypto Enforcement Unit -- *The SEC Crypto Task Force,* which, instead of prosecuting Big Crypto, was created to forge an alliance with Big Crypto —inviting crypto financiers to create the terms of their own regulation.

As far as I can tell, the goal of this revolutionary merger of government and industry is to construct a new crypto-regulatory framework; to cure the SEC sins of the past; and to eradicate any remnants, fragments or artifacts of the injustices of the Gary Gensler era. Not surprisingly, I have some serious concerns about this sudden and abrupt SEC transformation:

- First off, the SEC seems to be ignoring/dismissing the extraordinary success the SEC's crypto-enforcement efforts, which is the most winning enforcement program in SEC history, prevailing in court in most (arguably all, including the Ripple case) of the 200+ crypto-related enforcement actions the SEC has ever filed. Per the SEC, these volumes of crypto-related decisions, thoughtfully handed down by a broad range of Article III judges, must now be systematically ignored, unilaterally rendering federal securities compliance both optional and obsolete.

- Second, the cryptoverse is not merely unsafe, disorderly, anarchic, chaotic and lawless but crypto also enables a plague of horrific and dire externalities (such as ransomware, terrorism, human trafficking, child pornography and other horrendous crimes) while also creating a new epoch of global financial systemic risk. Contrary to the SEC's current posture, crypto-regulation does not neatly fit under a rubric of caveat emptor; crypto's externalities and systemic risk belie and discredit such a simplistic and naïve regulatory paradigm.

- Third, the hypocrisy of the SEC's crypto-legal position cannot be overstated. On the one hand, the SEC promises a new generation of crypto-regulators, who will champion the future of finance and money and enable a digitally transformative technological *Fourth Industrial Revolution.* Yet, in an oddly dystopian twist, the SEC defiantly asserts that selling digital assets is just like selling Pokémon cards, American Girl dolls or Beanie Babies.

- Finally, the new SEC taglines of crypto-innovation and emancipation are not only a red herring, but they are also the hallmarks of an affinity fraud, a type of securities swindle

> that the SEC has ironically fought against for the past 90 years. An affinity fraud is an investment scam in which a con artist targets members of an identifiable group based on personal affinities such as race, age and religion. With crypto, the SEC is tapping into the largest affinity group of all — freedom-loving Americans. The SEC's pitch misappropriates fundamental American beliefs of liberty and the right to be left alone, which effectively sidetrack and dissemble crypto's plain truth — *that the crypto-emperor has no clothes*.

My take is that by masquerading a mixed metaphor of grift, illusion and regulatory annulment as some sort of ground-breaking embrace of financial innovation, the SEC may not only be abdicating its historic mission of investor protection but may also be enabling crypto-financiers to laugh all the way to the bank (to deposit their fiat).

Notwithstanding, there is always room for the improvement of securities regulation, and some SEC regulatory renovations might certainly make sense, which is why I participated in both the SEC East Coast Crypto Roundtable and the Enforcement Forum's West Coast Crypto Roundtable (Mini-Edition). Specifically, last Thursday, I had the pleasure of debating Teresa Goody Guillen about crypto/securities laws/crypto-crime/etc. during Bruce Carton's 2025 sold-out Enforcement Forum West conference. Watch at:
https://youtu.be/5qSn9qySRqM?si=X2SxTPfAYYXRimBO

Teresa, whom I like and admire, vehemently disputed most of what I stated, especially the following 2 axioms:

1) That crypto has facilitated fraud, money-laundering and other flavors of financial crime on a gargantuan scale; and

2) That court after court has decreed, time and again, in clear and certain terms, that digital assets are securities.

Unfortunately, time constraints did not allow me to respond thoughtfully to Teresa's litany of objections. Along those lines, I have prepared this White Paper (with receipts) to meticulously and exhaustively respond with the four critical axioms below, which I not only expressed during the debate, but for which I have also *brought receipts*:

1. There is Now an Extraordinary and Robust Volume of Federal Judicial Decisions Holding That Digital Assets Are Securities;

2. Crypto Has Become a Killer App for Criminals;

3. Actual Crypto-Crime Traceability is a Myth; and

4. Blockchain Hype is Mostly Bunk.

I. THERE IS NOW AN EXTRAORDINARY AND ROBUST VOLUME OF FEDERAL JUDICIAL DECISIONS HOLDING THAT DIGITAL ASSETS ARE SECURITIES

Whether an investment product acts as a stock token, is priced off of the value of securities and operates like derivative, is a stable value token backed by securities, or any other virtual product that provides synthetic exposure to underlying securities, the SEC has insisted that those promoting, enabling or otherwise facilitating that investment must all comply with U.S. securities laws.

Not surprisingly, time and again, the courts have consistently affirmed the SEC's position and along the way, have dramatically highlighted the cryptocurrency industry's shortcomings. To date, the SEC has now brought 200 or so crypto-related enforcement actions for violations involving a litany of crypto-concoctions – including enforcement actions against perpetrators of initial coin offerings, simple agreements for future tokens ("SAFTS"), crypto-lending programs, celebrity crypto endorsements, crypto-staking programs, and crypto-intermediaries such as Kraken, Coinbase, Binance, Beaxy, Bittrex and others.

This laundry list of notorious defendants has continued to grow each quarter during the last few years. In fact, up until January 20, 2025, it was easier to list the crypto companies that ***weren't*** being sued by the SEC than the ones that were operating lawfully.

Along these lines, below is an exhaustive discussion of some of the most recent and important judicial decisions supporting the assertion that just about any variant of digital asset offering is a security that triggers SEC jurisdiction and compliance.

SEC v. Green United

This SEC crypto-enforcement action began on March 8, 2023, when the SEC charged

Thurston and Green United, LLC, d/b/a "Green" or "Set Power Free," with the unregistered offer and sale of investments called "Green Boxes" or "Green Nodes," leading investors to believe that those products mined a digital token they called GREEN on a purported "Green Blockchain."

The SEC Complaint

As alleged in the SEC complaint, investors were led to believe that the value of GREEN could increase if Green United succeeded in creating a "public global decentralized power grid." In reality, as alleged in the complaint, the Green Boxes purchased by investors did not mine GREEN, but rather mined Bitcoin, which was not transferred to investors. Likewise, Green Nodes did not mine GREEN but, as alleged in the complaint, were a basic software that in no way generated GREEN. As alleged in the complaint, Thurston created the total supply of GREEN tokens in October 2018 through a smart contract on the Ethereum blockchain, and Green United distributed those GREEN tokens to investors wallets at Thurston's direction in order, as alleged, to create the appearance that GREEN was being mined.

Additionally, the SEC complaint alleged that from April through October 2018, SEC recidivist Krohn, whom Thurston recruited and paid commissions to promote and sell Green Boxes and

whom the SEC alleges acted as an unregistered securities broker, made numerous misrepresentations to investors about the present value of the GREEN token and returns on investment that investors could anticipate.

The defendants filed a motion to dismiss arguing that the alleged Green Box investment scheme was not a security, and that the SEC was a rogue regulator, regulating by enforcement, unlawfully coopting powers from Congress and *"inviting the court to assent to its jurisdictional abduction."*

Green United's strategy initially arguably worked when in March 2023, the court partially granted their first motion to dismiss with leave for the SEC to amend. But the victory was short-lived, because on February 21, 2024, the SEC filed an amended complaint with additional details on the fraud allegations. Then, not surprisingly, last March, Thurston and Krohn filed renewed motions to dismiss, arguing the amended complaint still failed to properly allege an "investment contract" security existed or sufficiently plead securities fraud with particularity as required -- only this time the defendant's motion to dismiss was flatly denied.

A Compelling Denial: The SEC Was Simply Doing Its Job

Per Judge Ann Marie McIff Allen of the Central Division of Utah Federal Court:

> *"In short, at this stage, this action does not present any novel attempt at regulation by the SEC. Rather, the SEC, by this action, pursues the regulatory goals Congress set for it ninety years ago. Thus, Defendants identify no constitutional infirmity relevant to the Court's analysis."*

Favorite Excerpt (a Tenth Circuit quote oft cited in the dozens of motion to dismiss denials of other SEC crypto-enforcement actions)

> *"As to Defendants' third and final argument– that the SEC's suit violates the Due Process Clause and separation of powers set forth in the United States Constitution – the Court finds no constitutional violation . . . The Tenth Circuit's review of the intent of the Securities Acts is instructive here: "Congress enacted the Securities Acts in response to serious abuses in a largely unregulated securities market, and for the purpose of regulating investments, in whatever form they are made and by whatever name they are called.* ***Congress painted with a broad brush in defining a security in recognition of the virtually limitless scope of human ingenuity, especially in the creation of countless and variable schemes devised by those who seek the use of the money of others on the promise of profits.*** *To that end, as the [Supreme] Court explained, Congress determined that the best way to achieve its goal of protecting investors was to define the term security in sufficiently broad and general terms so as to include within that definition the many types of instruments that in our commercial world fall within the ordinary concept of a security. In furtherance of that goal, Congress did not attempt precisely to cabin the scope of the Securities Acts but instead enacted a definition of security sufficiently broad to encompass virtually any instrument that might be sold as an investment*." *(Emphasis added)*

SEC v. Opporty

In a stunning 69-page decision, Judge Eric Komitee of the Eastern District of New York provides yet another meticulously detailed analysis as to why digital assets are securities under the Howey Test (and why the SEC was spot-on in its arguments relating to digital assets).

In a September 24, 2024, memorandum, Judge Komitee said the SEC had proved enough of its claim that Opporty International and its owner Sergii Grybniak had unlawfully offered the sale of unregistered securities in the US. Specifically, Judge Komitee wrote that under the Howey test, outlined in the 1946 Supreme Court decision SEC v. W.J. Howey Co., the digital tokens the defendants sold in their offering are investment contracts within the meaning of federal securities laws and, therefore, needed to be registered.

Some Background

The SEC announced on January 21, 2020, that it was taking legal action against Opporty and Grybniak, accusing the company of failing to register a fraudulent initial coin offering (ICO) by offering the sale of "unregistered digital asset securities."

As alleged in the SEC's complaint, Sergii "Sergey" Grybniak and his company Opporty International, Inc. raised approximately $600,000 from nearly 200 investors in an ICO of Opporty's unregistered digital asset securities called "OPP Tokens." Grybniak and Opporty allegedly made multiple false and misleading statements to investors, including exaggerating the number of actual and potential users of its business platform and falsely claiming that the ICO was "SEC regulated," "SEC compliant," and "SEC registered."

The SEC's complaint further alleged that Grybniak and Opporty engaged in other deceptive acts, including misappropriating third-party content without approval or attribution, to create the false impression that actual users of Opporty's platform had created such content.

Opporty marketed itself as providing a "blockchain-based ecosystem for small businesses and their customers," primarily in the US. The platform was meant to be a place where small businesses could list their services and enter into agreements via smart contracts.

A Compelling Decision from Judge Komitee

Like every SEC crypto-defendant has proclaimed, the Opporty defendants asserted a due process defense against the SEC claim, arguing that the SEC's guidance about crypto offerings has been so vague and arbitrary that investors have not had sufficiently definite warning about how the Howey test might apply. The defendants also argued that the SEC acted arbitrarily in bringing the current action. But Judge Komitee disagreed, stating unequivocally:

"Although the application of the Howey test to new facts can raise interpretive questions, that is inherent in the application of existing law to any new technology. The fact that a body of law involves an 'inherently individualized and fact-specific inquiry' does not render it

constitutionally vague *. . . More importantly, the Second Circuit has foreclosed the defendants' vagueness challenge: confronted with the argument that the term' investment contract' is void for vagueness, it held (albeit in a footnote) that 'position to be untenable.'" (Emphasis added)*

SEC v. Rivetz

Like Opporty, the SEC charged Rivetz Corp., Rivetz International SEZC, and Steven K. Sprague, the President of Rivetz and CEO of Rivetz International, with conducting an illegal, unregistered offering of securities through an initial coin offering. Sprague is the CEO of Cayman Islands company Rivetz International and its parent. Sprague was accused by the SEC of promoting his ICO for RvT tokens despite their lack of a functional use at the time.

Some Background

According to the SEC's complaint, between July and September 2017, the Rivetz defendants offered and sold digital assets designated as "RvT tokens" to the public, including U.S. investors, for the purpose of capitalizing Rivetz's business.

The complaint alleges that Sprague marketed RvT as an investment opportunity by promoting the value of RvT to investors; highlighting that RvT would be made available to trade on digital asset trading platforms; describing where RvT could be resold; touting Sprague's abilities and managerial skills, including his experience as a former officer and director of a public company; and claiming RvT would increase in value as a result of Rivetz's efforts. According to the complaint, the RvT tokens could not be used to purchase any good or service at the time they were sold.

As alleged, the defendants' offers and sales of RvT, which raised the equivalent of $18 million in digital assets from investors, were not registered with the SEC and did not qualify for any exemption from registration.

The SEC's complaint, filed in the District of Massachusetts, charges the defendants with violating the securities registration provisions of Section 5 of the Securities Act of 1933. The SEC sought injunctive relief, the return of allegedly ill-gotten gains plus prejudgment interest, and a civil penalty.

The Rivetz Decision

In a blunt, scathing and merciless September 30, 2024 order, Massachusetts federal court judge Mark Mastroianni agreed with the SEC that Sprague, through Rivetz, sold unregistered securities by offering the Ethereum-based Rivetz, or RvT, token to US persons. Specifically, Judge Mastroianni awarded the SEC’s summary judgment against the Rivetz defendants. This means that the Judge has unilaterally declared the SEC victorious and that there is no need for a trial – and Judge Masstroianni has ordered the SEC to confer with the defendants and file a proposed judgment for injunctive and monetary relief on or before October 22, 2024.

Like every crypto firm before him, Sprague (who represented himself) claimed his token was a software product and not an investment contract under the securities-defining Howey test. But

Judge Mastroianni disagreed and held that, ". . . from the first announcement of the ICO through its completion, Rivetz and Sprague made statements to potential purchasers that clearly tied the value of RvT tokens to Rivetz's goal of creating a security ecosystem for mobile devices."

Judge Masstroianni explained that the value of the RvT token "was directly dependent on Rivetz's entrepreneurial efforts" and that the tokens were also billed "as a functional part of the Rivetz security ecosystem," and their value "was dependent on future demand and usability." The order went on to say that the ICO's White Paper told potential purchasers that Rivetz had a viable security product ready to fill significant market demand and the product's success would drive demand for RvT tokens, propelling its value.

This case also reinforces the application of the economic reality test (a favorite of the SEC's briefs) in that the SEC has argues that a court should look at the totality of the circumstances of a digital asset when applying the Howey Test. Judge Masstroianni disagreed, rejecting Sprague's argument that disclaimers in the offering meant there was a lack of common enterprise, or an expectation of profits derived from the efforts of the promoter.

Judge Masstroianni wrote:

"His argument might be meritorious were the court required to credit contractual formalities and limiting language included in documents provided to purchasers participating in the [initial coin offering]; however, the opposite is true. ***This court must look at the economic realities of the transaction, especially the language used to encourage potential purchasers****." (Emphasis added)*

SEC v. Kraken

In a devastating 29-page decision, a California federal judge denied a motion from crypto-trading platform Payward Inc. and Payward Ventures (DBA as "Kraken") to dismiss an SEC enforcement action, finding the that the SEC plausibly alleged that digital currency transactions on Kraken's online platform could constitute investment contracts and are subject to securities laws.

Trading platforms like Kraken allow their customers to deposit fiat (legal tender issued and approved by a country) into bank accounts and crypto assets into wallets controlled by the platform, and then to purchase and sell those assets for fiat or other crypto assets. These exchanges may be conducted on- or off-chain. The crypto assets offered on the Kraken Trading Platform are available for sale to an individual or institution who creates an account with Kraken.

The SEC's suit against Kraken parents Payward Inc. and Payward Ventures alleges that the platform failed to register as a broker, dealer and exchange for "crypto asset securities." In its motion to dismiss the case, Kraken argued the transactions it enables on its platform are not securities.

The SEC alleges that Kraken, through the Kraken Trading Platform and Kraken Services, made available for trading crypto assets that are offered and sold as investment contracts, and thus as securities. These include, but are not limited to, crypto assets labeled with the following trading symbols: ADA, ALGO, ATOM, FIL, FLOW, ICP, MANA, MATIC, NEAR, OMG, and SOL. Because all the SEC must do is plausibly allege that at least one of these crypto assets is being traded as an investment contract to make its claims feasible, Judge Orrick focused on the SEC's factual allegations regarding two crypto assets: ALGO and SOL – and held that both could be securities.

The SEC's allegations against Kraken concern crypto assets that were originally issued by third-party cryptocurrency networks. Although Kraken agrees that the initial offering of the digital assets involved an investment of money, Kraken argued that when the asset hits the resale market on its platform, the investment contract doesn't follow, failing the so-called Howey Test, which is a test the U.S. Supreme Court created for lower courts to use when determining if an investment product is a security. Kraken went so far as to label the SEC's argument as a "perversion" of the Howey test.

But Judge William H. Orrick, who presides over the matter, strongly disagreed:

> *"The court in Howey said nothing about an investment of money requiring privity between the issuer and the investor, nor has Congress ever drawn such boundaries around what constitutes an investment contract . . .* ***It defies common sense to suggest that when someone purchases crypto assets from a reseller or another investor, that person or entity does not understand themselves to be investing money in the asset****." (Emphasis added)*

The SEC Case Against Kraken Protected Investors

The SEC charged that Kraken turned a blind eye to its legal responsibilities and engaged in its securities intermediary conduct without registering with the SEC, depriving investors of the disclosures and protections that registration entails.

The SEC argued that by failing to prevent known conflicts of interest and commingling its investors' assets with its own, Kraken demonstrates why registration and the investor protections that come with regulatory oversight are critical to the soundness of U.S. capital markets.

U.S. SEC registration of financial intermediaries: (1) mandates that investor funds and securities be handled appropriately without conflicts of interest; (2) ensures that investors understand the risks involved in purchasing the often illiquid and speculative securities that are traded on a cryptocurrency platform; (3) makes buyers aware of the last prices on securities traded over a cryptocurrency platform; and (4) provides adequate disclosures regarding their trading policies, practices and procedures.

Overall, entities providing financial services must carefully handle access to, and control of, investor funds, and provide all users with adequate protection and fortification.

With traditional SEC-registered financial firms, the SEC has unlimited and instantaneous visibility into every aspect of operations. With crypto trading platforms, the SEC lacks any sort

of oversight and access — and has scant ability to detect, investigate and deter fraudulent conduct.

By failing to register with the SEC, the SEC charged that Kraken has placed their own financial interests ahead of the legal obligations they owe to customers as securities intermediaries, failing to register as an exchange, a broker, a dealer, and a clearing agency without registration in violation of Exchange Act Sections 5, 15(a), and 17A(b) [15 U.S.C. §§ 78e, 78o(a), and 78q1(b)].

The SEC sought a final judgment: 1) Permanently enjoining Kraken from violating the federal securities laws; 2) Ordering Kraken to disgorge their ill-gotten gains, on a joint and several basis, and to pay prejudgment interest thereon; 3) Permanently enjoining Kraken from acting as an unregistered exchange, broker, dealer, or clearing agency; and 4) Imposing civil money penalties on Kraken.

Why This Decision was Yet Another Home Run for the SEC's Crypto-Enforcement Efforts
Like so many of the crypto-enforcement action "motions to dismiss" and "motions for summary judgment" decisions, the defense spent tens of millions in legal fees to litigate their failed position and the end result has been pretty much the same: SEC victory.

However, what has always intrigued me most are not the outcomes of the decisions, but rather the intensive time and effort judges routinely take in drafting their decisions on these exhaustive dispositive crypto-related motions. Along these lines, below are five especially compelling excerpts of Judge Orrick's compelling Kraken Order:

Excerpt #1: Judges must look at the totality of the circumstances when applying the Howey Test to crypto-products:

"Howey and its progeny require any court considering whether a secondary market transaction constitutes an offer or sale of an investment contract to apply the same analysis that it would if that transaction were to occur on a primary market. The determinative factor does not involve the nature of the platform upon which the asset is transacted, ***but rather the reasonable expectations of the individual initiating the transaction. That analysis considers the totality of the circumstances and the economic reality of transaction****." (Emphasis Added)* **Excerpt #2:**

There is no need for post-sale obligations to trigger the Howey Test:

"Kraken argues that an investment contract requires "post-sale obligations" from the issuer to the receiver; the SEC insists that it does not. ***The weight of authority, both recent and well-established, favors the SEC*** *. . . In short, the blue-sky laws from which Howey drew inspiration may have involved more formal contracts, but the Court in Howey, the Ninth Circuit in Hocking, and numerous courts since have made clear that contractual formalities are not required for something to qualify as an investment contract, and therefore a security. What counts is the totality of the circumstances surrounding a sale, trade, or exchange, and the expectations of the investor. Kraken's argument would improperly constrain Howey." (Emphasis Added)*

Excerpt #3: Whether a crypto asset is offered in the primary market or the secondary market, the analysis is the same:

"The parties disagree about the degree to which Kraken's nature as a secondary market for cryptocurrency transactions changes the way the transactions are considered when determining whether the SEC has plausibly alleged that they constitute investment contracts. Ultimately, the resolution is simple: The Howey test applies wherever a court seeks to determine whether a transaction involves an investment contract, regardless of whether that transaction is on a primary or secondary market . . . In short, binding authority requires the court to evaluate whether an investment contract is formed in a secondary market to consider the features of that secondary market transaction. It does not require that the court ignore anything that happened in a primary market transaction; if a reasonable investor would understand representations made during the primary market transactions to carry forward into the secondary market, then those representations may be considered. ***What matters are the reasonable expectations of the investor.*** *That a transaction does not involve the asset's primary issuer does not foreclose the possibility that the primary issuer's representations follow the asset through to the secondary market . . . Kraken agrees that the initial offering of the Kraken-Traded digital assets involve an investment of money. But it argues that once the asset hits the resale market on Kraken's platform, that investment does not follow the asset, meaning that an asset that may have originally met the first Howey prong no longer does upon resale. Kraken's perspective is too narrow." (Emphasis Added)*

Excerpt #4: Why the Ripple Decision (as precisely proclaimed by the deciding Judge herself in the Ripple decision) has little, if any, value as legal precedent for any U.S. Court:

"Kraken compares this case to Ripple Labs I, where the court held on summary judgment that purchasers on digital asset trading platforms (including Kraken) had no reasonable expectation of profits. It determined that the "economic reality" showed that the third Howey prong was unsatisfied where there was no relationship between the alleged issuer and the purchasers on digital asset platforms. . .. It explicitly declined to address whether secondary market sales of the crypto asset in question constituted offers and sales of investment contracts because the question was not before her. ***The court's opinion is carefully constrained to the facts of the case and predicated on findings from a fully developed record****. Again, "[w]hether a secondary market sale constitutes an offer or sale of an investment contract would depend on the totality of circumstances and the economic reality of that specific contract, transaction, or scheme." As discussed, the way the court foreshadowed how a court would have to consider secondary market sales of crypto assets is consistent with the Ninth Circuit's holding in Hocking. See Hocking, 885 F.2d at 1462 (declining to recognize an absolute rule about when secondary market transactions involve a security and noting that Howey requires the examination of the "economic reality" of each secondary market transaction, including analysis of how assets are promoted to investors, and what the investor's intentions and expectations were when they invested). The SEC has plausibly alleged that investors in crypto assets offered on Kraken possessed an expectation of profits from the efforts of others that they derived from the*

promoters' representations that Kraken republished and reasserted on its platform. Whether or not the record ultimately supports that allegation will be revealed through discovery." (Emphasis Added)

Excerpt #5: Why the major questions doctrine argument is a losing one (and why I have stopped counting the times that judges have said so):

"Kraken, and its numerous amici, insist that the question posed in this case is the kind reserved for Congress, because resolution of the dispute in the SEC's favor would expand its regulatory power. Other courts have already considered whether similar claims brought by the SEC violate the major questions doctrine and found that they do not. The same is true here. The major questions doctrine originates from the idea that Congress does not delegate extraordinary powers that transform an agency's authority without making its intent clear. . . This is not such a case. The cryptocurrency industry "falls far short of being a 'portion of the American economy' bearing 'vast economic and political significance . . . Moreover, the SEC is not asserting a "transformative expansion in its regulatory authority" or a "highly consequential power beyond what Congress could reasonably be understood to have granted it." . . . ***While cryptocurrency itself is a relatively novel financial instrument, the principles driving the SEC's attempt to assert regulatory authority over it are not new.*** *" (Emphasis Added)*

SEC v. Binance

In a powerful opinion, the bulk of the SEC's enforcement action against Binance, and its cofounder Changpeng Zhao was judicially ordered to proceed. The SEC sued Binance and Zhao for mishandling customer funds, misleading investors and regulators, failing to register certain securities and failing to register as an exchange, broker-dealer and clearing firm. Binance and Zhao contested the SEC's claims and filed a motion to dismiss.

Out of 13 counts, 10 will proceed in their entirety and two partially, while one is dismissed, according to the order issued by Judge Amy Berman Jackson, in the U.S. District Court for the District of Columbia.

Some Highlights

Perhaps the most crucial and impactful quote from Judge Jackson's decision relates to Judge Jackson's application of the U.S. Supreme Court's 1946 so-called "Howey Test" to digital assets, which she addresses head-on:

"In addressing this concept, the Supreme Court has repeatedly emphasized that the statutory definition in general, and the term "investment contract" in particular, must be read broadly to address the variety of investment vehicles and money-making schemes that could not possibly have been foreseen in 1934 when the Securities Act was passed. In the Securities Act, the term 'security' was defined to include by name or description many documents in which there is common trading for speculation or investment. Some, such as notes, bonds, and stocks, are pretty

much standardized and the name alone carries well settled meaning. Others are of more variable character and were necessarily designated by more descriptive terms, such as 'transferable share,' 'investment contract,' and 'in general any interest or instrument commonly known as a security.' We cannot read out of the statute these general descriptive designations merely because more specific ones have been used to reach some kinds of documents. . .. [T]he reach of the Act does not stop with the obvious and commonplace. Novel, uncommon, or irregular devices, whatever they appear to be, are also reached if it be proved as matter of fact that they were widely offered or dealt in under terms or courses of dealing which established their character in commerce as 'investment contracts,' or as 'any interest or instrument commonly known as a 'security.' SEC v. C.M. Joiner Leasing Corp., 320 U.S. 344, 351 (1943)."

Judge Jackson also specifically addresses the digital asset industry's typical laundry list of defenses and, consistent with a series of cited SEC-crypto-related decisions, denied them all seriatim. Three examples:

Example #1: Binance argued that the digital asset industry lacked fair notice of the SEC's crypto-enforcement efforts. The Court's response:

"Defendants focus on the SEC's failure to issue regulations on crypto assets and its inconsistent statements and approaches to regulating the sale of digital assets as investment contracts . . . But this suit is consistent with the other enforcement actions that the agency has brought alleging that the sales of crypto assets are "investment contracts" within the meaning of Howey . . . Moreover, the agency put the industry on notice even before 2019. In July 2017, the SEC issued a report advising "those who would use . . . distributed ledger or blockchain-enabled means for capital raising to take appropriate steps to ensure compliance with the U.S. federal securities laws."

Example #2: Binance argued that the SEC's actions constituted unlawful and rogue SEC regulation by enforcement. The Court's response:

"With respect to the 'power grab' argument, the SEC's enforcement action here does not reflect "enormous and transformative expansion in [the agency's] regulatory authority without clear congressional authorization" . . . Rather, the SEC asks the Court to rule whether defendants' crypto assets are "securities" within the meaning of the Securities Act of 1933 and the Securities Exchange Act of 1934, an application of enforcement powers that the agency has exercised since at least 1946, when the Supreme Court held in Howey that the contracts at issue in that case "under the circumstances . . . together constitute[d] an 'investment contract' within the meaning of the federal securities laws."

Example #3: Binance argued that the SEC's efforts constituted a violation of the Major Questions Doctrine. The Court's response:

"The Court has not been given grounds to find that the industry, while important, has the broad reach that has motivated courts to apply the [major questions] doctrine to other industries . . .

Further, a ruling that certain of defendants' sales of crypto assets are investment contracts, and therefore securities, would not have the economic reach that other regulatory actions found to be subject to the [major questions] doctrine would have had."

The Secondary Market for Digital Assets

Judge Jackson renders some interesting case-specific findings concerning whether digital assets trading in the secondary market are securities, focusing on the mindset of the investor.

First off, in the secondary market, Judge Jackson affirmed that no contractual relationship is required between the investor and issuer, stating:

". . . it is the economic reality of the particular transaction, based on the entire set of contracts, expectations, and understandings of the parties, that controls."

However, Judge Jackson focuses on whether secondary market investors have purchased a digital asset for its utility (such as to gain a discount on trading) or for the expectation of profit (such as to generate an investment return like with a stock purchase). Judge Jackson seems to be saying that, in the secondary market, the mindset of the investor is a crucial determinant of the classification of a digital asset as a security and must be pled with particularity.

I would bet that the SEC will take discovery from a slew of secondary market investors in Binance-related tokens and present evidence about the hope of the investors to earn a profit from buying those Binance-related tokens. Also, expect the SEC to add investor statements/affidavits to some future crypto-related pleadings, which will emphasize the hope to "get-rich-quick" from purchasing digital assets.

Along the same lines, Judge Jackson dismisses the SEC's claims for Binance's failure to register its stablecoin, BUSD (now pretty much defunct), asserting:

"Absent from all of this is any suggestion that purchasers were informed that the proceeds from BUSD sales were to be deployed, through the issuers' managerial and entrepreneurial efforts, to generate a return for their benefit. While the complaint emphasizes with respect to BNB that potential buyers were told that proceeds from the offering would be used to strengthen the platform that would in turn give the tokens their value, for BUSD it simply states that the proceeds were to be spent on "profit-generating opportunities for the benefit of both Trust Company A and Binance." Compl. ¶ 317. There are no facts alleged to support an inference that this advanced the fortunes of those who bought the BUSD tokens, or that they reasonably expected to share in the companies' profits in the form of a return on their investment."

Staking

Not surprisingly, Judge Jackson held that the SEC plausibly alleges that Binance's Staking product is an investment in a common enterprise with the expectation of profit due to the managerial or entrepreneurial efforts of others. The Staking investors' assets are pooled and controlled by BAM Trading, and their fortunes rise and fall with BAM Trading's success as a validator - clearly constituting a security.

One More Favorite Quote

Judge Jackson gives equal time to criticizing the SEC's arguments and criticizing Binance's arguments — adding occasionally subtle snarky gems in her opinion rejecting the Ripple decision discussed a bit more by later on (and will be the subject of an exclusive posting as well), below, such as this one:

"The defendants insist that the plain text of the provision and the history behind it require that an "investment contract" must involve some sort of contractual relationship or arrangement between the offeror and the purchaser . . . But their argument has been foreclosed by Supreme Court and Circuit precedent, and indignation alone cannot open that door."

SEC v. Coinbase

On June 6, 2023, the SEC filed a complaint against Coinbase, Inc., alleging that Coinbase was operating its crypto asset trading platform as an unregistered national securities exchange, broker, and clearing agency and also that Coinbase had failed to register the offer and sale of its crypto asset staking-as-a-service program. In an 84-page order, the U.S. District Court for the Southern District of New York has denied Coinbase's motion to dismiss the SEC's case against Coinbase. The decision, written by U.S. District Judge Katherine Failla, allowed the SEC to pursue its lawsuit against Coinbase.

Some Excerpts:

"The very concept of enforcement actions evidences the Commission's ability to develop the law by accretion. The SEC has a long history of proceeding through such actions to regulate emerging technologies and associated financial instruments within the ambit of its authority as defined by cases like Howey — a test that has existed for nearly eight decades. See, e.g., SEC v. SG Ltd., 265 F.3d 42, 44 (1st Cir. 2001) (applying federal securities laws to "virtual shares in an enterprise existing only in cyberspace"). Using enforcement actions to address crypto-assets is simply the latest chapter in a long history of giving meaning to the securities laws through iterative application to new situations."

"The Court finds the SEC has sufficiently pleaded that Coinbase operates as an exchange, as a broker, and as a clearing agency under the federal securities laws, and through its Staking Program engages in the unregistered offer and sale of securities."

"As explained herein, the 'crypto' nomenclature may be of recent vintage, but the challenged transactions fall comfortably within the framework that courts have used to identify securities for nearly eighty years." Said the SEC in an email to CoinDesk:

"We're pleased that yet another court has confirmed that, while the term 'crypto' may be relatively new, the framework that courts have used to identify securities for nearly 80 years still applies. It's the economic realities of a transaction, not the labels, that determine whether a particular offering constitutes a security."

First off, this is an 84-page decision, and Judge Failla presents her conclusions with meticulous detail. The judge is obviously sending a signal to the parties of what the law is regarding digital assets and the regulation of exchanges, broker-dealers, and clearing firms.

Second, these are strict liability, violations, so no particular state of mind can mitigate liability. In other words, it doesn't matter what anyone advised Coinbase to do, the law is the law, and they are likely to have violated it.

Third, to me, there does not seem to be any possibility of any new facts that could arise during discovery that would somehow change the judge's perspective. This means that Coinbase's motion for summary judgment after discovery will likely be similarly denied.

Fourth, there are no allegations of fraud, but the allegations that the SEC makes go to the essence of Coinbase operations, so if the SEC were to prevail, which seems highly likely (unless the new Administration dismisses the case), the vast majority of Coinbase's, non-bitcoin related operations will have to stop until Coinbase registers as an exchange, as a broker-dealer, and as a clearing firm.

Finally, at the conclusion of discovery and the hearing of all dispositive motions, there will not be much left for the jury to decide in a trial, because the violations may very well be established as a matter of law.

SEC v. KIK

In Kik, the SEC's complaint, filed in the U.S. District Court for the Southern District of New York on June 4, 2019, alleged that Kik sold digital asset securities to U.S. investors without registering their offer and sale as required by the U.S. securities laws. Kik argued that the SEC's lawsuit against it should be considered " void for vagueness." Kik lost.

The court granted the SEC's motion for summary judgment on September 30, 2020, finding that undisputed facts established that Kik's sales of "Kin" tokens were sales of investment contracts (and therefore of securities) and that Kik violated the federal securities laws when it conducted an unregistered offering of securities that did not qualify for any exemption from registration requirements. The court further found that Kik's private and public token sales were a single integrated offering, and that Kik's Fair Notice defense failed, stating:

*"First, the law regarding the definition of investment contract gives a reasonable opportunity to understand what conduct and devices it covers. Howey provides a clearly expressed test for determining what constitutes an investment contract, and an extensive body of case law provides guidance on how to apply that test to a variety of factual scenarios. See United States v. Smith, 985 F. Supp. 2d 547,588 (S.D.N.Y. 2014) ("[I]t is not only the language of a statute that can provide the requisite fair notice; judicial decisions interpreting that statute can do so as well."). That is constitutionally sufficient. See United States v. Zaslavskiy, No. 17 CR 647 (RID), 2018 WL 4346339, at *9 (E.D.N.Y. Sept. 11, 2018) ("[T]he abundance of caselaw interpreting and applying Howey at all levels of the judiciary, as well as related guidance issued by the SEC as to*

the scope of its regulatory authority and enforcement power, provide all the notice that is constitutionally required.").

Second, for similar reasons, the law provides sufficiently clear standards to eliminate the risk of arbitrary enforcement. Howey is an objective test that provides the flexibility necessary for the assessment of a wide range of investment vehicles. Kik focuses much of its argument on the SEC's failure to issue guidance on securities enforcement related specifically to cryptocurrencies, SEC officials' inconsistent public statements on the issue, and the SEC's failure to bring enforcement actions against other issuers of digital tokens. However, the law does not require the Government to reach out and warn all potential violators on an individual or industry level. See Dickerson v. Napolitano, 604 F.3d 732, 745-46 (2d Cir. 2010) ("Courts ask whether the law presents an ordinary person with sufficient notice of or the opportunity to understand what conduct is prohibited or proscribed, not whether a particular [party] actually received a warning that alerted him or her to the danger of being held to account for the behavior in question." (internal quotation marks and citations omitted)). Kik cites one case where the Second Circuit, in assessing an as-applied vagueness challenged, took account of uncertainty in the SEC's interpretation of a provision. See Upton v. SEC, 75 F.3d 92, 98 (2d Cir. 1996). In Upton, the SEC had been inconsistent in its enforcement of a rule as applied to the same practice occurring consistently across the industry for years. Id. at 98. By contrast, as Kik acknowledges, every cryptocurrency, along with the issuance thereof, is different and requires a fact-specific analysis. Furthermore, the vagueness inquiry does not call for a factual investigation into whether a statute has led to arbitrary enforcement; it asks, objectively, whether the statute "authorizes or even encourages arbitrary and discriminatory enforcement." Copeland, 893 F.3d at 114. The statute at issue here does not."

The final judgment permanently enjoined Kik from violating the registration provisions of Sections 5(a) and 5(c) of the Securities Act of 1933. For the next three years, Kik is further required to provide notice to the Commission before engaging in enumerated future issuances, offers, sales, and transfers of digital assets. Kik was also ordered to pay a $5 million penalty.

SEC v. Telegram

In Telegram, the SEC filed a complaint on October 11, 2019, alleging that the company had raised capital to finance its business by selling approximately 2.9 billion "Grams" to 171 initial purchasers worldwide. The SEC sought to preliminarily enjoin Telegram from delivering the Grams it sold, which the SEC alleged were securities that had been offered and sold in violation of the registration requirements of the federal securities laws.

Telegram argued that the SEC has "engaged in improper 'regulation by enforcement' in this nascent area of the law, failed to provide clear guidance and fair notice of its views as to what conduct constitutes a violation of the federal securities laws, and has now adopted an ad hoc legal position that is contrary to judicial precedent and the publicly expressed views of its own high-ranking officials." But Telegram lost and the Judge did not even make mention of any Due Process arguments in his opinion.

Specifically, on March 24, 2020, the U.S. District Court for the Southern District of New York issued a preliminary injunction barring the delivery of Grams and finding that the SEC had shown a substantial likelihood of proving that Telegram's sales were part of a larger scheme to distribute the Grams to the secondary public market unlawfully.

Without admitting or denying the allegations in the SEC's complaint, the defendants consented to the entry of a final judgment enjoining them from violating the registration provisions of Sections 5(a) and 5(c) of the Securities Act of 1933. The judgment ordered the defendants to disgorge, on a joint and several basis, $1,224,000,000 in ill-gotten gains from the sale of Grams, with credit for the amounts Telegram pays back to initial purchasers of Grams. It also ordered Telegram Group Inc. to pay a civil penalty of $18,500,000. For the next three years, Telegram is further required to give notice to the SEC staff before participating in the issuance of any digital assets.

SEC v. LBRY

In November, 2022, the Fair Notice issue presented itself in an SEC enforcement action against **LBRY, Inc.,** a software firm that issued crypto asset securities called "LBRY Credits" or "LBC," and Judge Peter Barbadoro of the United States District Court for the District of New Hampshire addressed the Fair Notice defense head-on – and rejected it.

The SEC charged LBRY for selling unregistered securities, but LBRY claimed it did not receive "fair notice" of the application of securities laws to the LBC offer/sale. The decision is considered "a major blow" to crypto issuers, many of whom have argued to RBE promoters.

In LBRY, Inc., filed on March 29, 2022, the crypto-defense (and now war-cry) of "lack of regulatory clarity" and "regulation by enforcement" was specifically and unambiguously addressed – and summarily rejected.

Specifically, Judge Paul Barbadoro of New Hampshire federal court granted the SEC's summary judgment motion against LBRY. LBRY had argued that the SEC's attempt to treat LBC as a security violated its right to due process because the agency did not give LBRY fair notice that its offerings of LBC were subject to the securities laws. But LBRY lost.

In the first part of the ruling, the court held that LBRY offered/sold LBC as a security (LBRY had argued that LBC functioned as a digital currency that is an essential component of the LBRY Blockchain). This part of the decision was unprecedented because it was the first time a judge had determined that a coin that was not distributed through an ICO, was a security. Also, in its final point on its Howey analysis, the court rejected LBRY's argument that LBC could not be a security because it was a utility token with demonstrated purchases for consumptive, not investment, use.

The court noted that "[n]othing in the case law suggests that a token with both consumptive and speculative uses cannot be sold as an investment contract." The court summarized its holding: "[w]hile some unknown number of purchasers may have acquired LBC in part for consumptive purposes, this does not change the fact that the objective economic realities of LBRY's offerings of LBC establish that it was offering it as a security."

In the second part of the ruling, the Court held that LBRY did not have a defense that it lacked fair notice of the application of securities laws to the LBC offer/sale, resoundingly rejecting the so-called Fair Notice defense, which has become a critical page of the crypto-defense "regulatory clarity" playbook.

Judge Barbadoro stated:

"LBRY relies on the 2nd Circuit's decision in Upton v. SEC for the proposition that the SEC may not impose a sanction for violating the securities laws 'pursuant to a substantial change in its enforcement policy that was not reasonably communicated to the public.' But the facts of Upton bear no resemblance to the present case.

Upton involved an attempt by the SEC to sanction the CFO of a brokerage firm for violating an SEC rule that established a formula for setting the amount of money that the brokerage was required to maintain in a customer reserve account. Although it was undisputed that the brokerage had at all times complied with the "literal terms" of the rule, an ALJ relied on a novel interpretation of the rule by the SEC to conclude that the CFO could be sanctioned. Because the SEC did not give public notice of its new interpretation until after the brokerage had ended its offensive practice, the Second Circuit vacated the sanction imposed by the Commission. The present case is obviously quite different from the problem the court confronted in Upton.

The SEC has not based its enforcement action here on a novel interpretation of a rule that by its terms does not expressly prohibit the relevant conduct. ***Instead, the SEC has based its claim on a straightforward application of a venerable Supreme Court precedent that has been applied by hundreds of federal courts across the country over more than 70 years . . .*** *"* (Emphasis added)

As some experts have now explained, in rejecting LBRY's contention that the SEC's suit constituted a "substantial change in its enforcement policy that was not reasonably communicated to the public" because LBRY did not conduct an ICO, "the court held that the SEC's theory fit comfortably within the bounds of prior caselaw." The Court noted specifically that LBRY had no basis for asserting it was unaware of Howey's guidelines, even if it sold LBC tokens in a non-ICO context.

SEC v. Terra

In a decision from SDNY Judge Jed Rakoff in the SEC enforcement action against Terraform Labs Pte. Ltd. and Do Hyeong Kwon, Judge Rakoff addressed the Fair Notice defense head-on – and rejected it. Judge Rakoff writes:

"Next, defendants argue that the SEC violated their due process rights by bringing this enforcement action against them without first providing them "fair notice" that their crypto-assets would be treated as securities. See FCC v. Fox Television Stations Inc., 567 U.S. 239, 253-54 (2012) (ruling that the Due Process Clause requires that agencies bringing an enforcement action "provide," through written guidance, regulations, or other activity, "a person of ordinary intelligence fair notice" that the regulated conduct was "prohibited").

According to the defendants, the SEC has long maintained that cryptocurrencies are not securities, but here, they claim it has for the first time taken the position that all cryptocurrencies are securities and enforced this understanding against the defendants without any prior indication that it had changed its view. This sudden about-face, the defendants say, deprived them of their constitutional right to "fair notice" and, by implication, the opportunity to conform their behavior to the SEC's regulations. In response, the SEC argues that it has never taken either of the black-and-white positions that the defendants ascribe to it. Indeed, rather than state that all crypto-currencies are securities or that none of them are, the SEC insists that it has broadcast the same position on this issue all along: that some crypto-currencies, depending on their particular characteristics, may qualify as securities.

*Prior to its bringing this case, moreover, the SEC asserted the exact same position it has taken in this case in several enforcement actions brought against other crypto-currency companies for allegedly fraudulent conduct in the offer and sale of their crypto-assets. See, e.g., SEC v. PlexCorps, 2018 WL 4299983, at *2-3 (E.D.N.Y. Aug. 9, 2018); SEC v. Zaslavskiy, 2018 WL 4346339, at *8-9 (E.D.N.Y. Sept. 11, 2018). These relatively high-profile lawsuits -- which involved substantially similar allegations and millions of dollars in allegedly fraudulent cryptocurrency transactions -- would have apprised a reasonable person working in the crypto-currency industry that the SEC considered some crypto-currencies to be securities and that the agency would enforce perceived violations of the securities laws through the development, marketing, and sale of these crypto- currencies.*

Following this prior litigation, moreover, a department of the SEC issued written guidance in April 2019 that admonished those "engaging in the offer, sale, or distribution of a digital asset" to consider "whether the digital asset is a security" that would trigger the application of "federal securities laws." Sec. & Exchange Comm., Framework for "Investment Contract" Analysis of Digital Assets (April 2019). Within this document, the SEC also provided "a framework for analyzing whether a digital asset is an investment contract" and a list of characteristics that, if present in a given digital asset, would make the SEC more likely to view the given crypto-asset as a "security." Id. The instant lawsuit, in sum, is just one example of the SEC's longstanding view that some cryptocurrencies may fall within the regulatory ambit of federal securities laws.

None of the statements cited by the defendant, moreover, suggests that the SEC ever operated under a contrary assumption. For instance, the statement of an SEC staff member that a "token ... all by itself is not a security, just as the orange groves in Howey were not," Defs.' Br. at 13, does not amount to a concession that all cryptocurrencies are not securities. It does not, in other words, preclude the SEC from asserting, as it has here, that a token constitutes an investment contract when it is joined with a promise of future profits or the like to be generated by the offerors. The SEC's most recent representation that digital assets "may or may not meet the definition of a 'security' under the [f]ederal securities laws" is even more obviously aligned with its position in this case. Securities & Exchange Comm., Release No. IA-6240, at 16 n.25 (Feb. 15, 2023).

In short, defendants' attempt to manufacture a "fair notice" problem here comes down to asserting the SEC's position in this litigation is inconsistent with a position that the SEC never adopted. So long as the SEC has -- through its regulations, written guidance, litigation, or other actions -- provided a reasonable person operating within the defendant's industry fair notice that their conduct may prompt an enforcement action by the SEC, it has satisfied its obligations under the Due Process Clause . . . (Here, the Court makes explicit what has long been implied in the "fair notice" inquiry, at least as applied to agencies like the SEC that are charged with regulating highly technical entities. The question whether "fair notice" has been provided should be assessed from the perspective of a reasonable person in the defendant's industry rather than from that of a member of the general public. It would make little sense to construe the Due Process Clause to require that agencies like the SEC provide "fair notice" to everyday citizens, most of whom have no interaction with the industries that the SEC is tasked with regulating.)

It follows from the foregoing that the APA also does not foreclose the SEC's interpretation of federal securities laws to encompass the regulation of the defendants' crypto-assets. While it may be true that, where an agency intends to promulgate "a new industry-wide policy," notice-and comment rulemaking -- not case- by-case adjudication -- offers a "better, fairer, and more effective" method of doing so, Cmty Television v. Gottfried, 459 U.S. 498, 511 (1983), here, as detailed above, the SEC is not announcing a new policy in this case, but merely enforcing its previously stated view that certain crypto-assets can be regulated as securities if they meet the characteristics of an "investment contract" under the Howey case (described below). Far from representing a "radical departure" from the SEC's stated views on the law, this enforcement action is simply a "fact-intensive application of a statutory standard," a category of agency action that has traditionally been exempt from the procedural requirements of notice-and comment rulemaking.

To conclude, no doctrine -- whether grounded in interpretive canons, statute, or the federal Constitution -- bars the SEC from, as a preliminary matter, asserting that the defendants' crypto assets are "investment contracts" that are subject to federal securities laws."

SEC v. Ripple

In the infamous summary judgment holding from Judge Analisa Torres in the SEC matter charging Ripple Labs, Inc., Bradley Garlinghouse, And Christian A. Larsen, Judge Torres addressed the issue of the sale of digital assets, at least with respect to institutional sales – and rejected it.

Specifically, the Court held that, at least with respect to the institutional sales, Ripple had fair notice that doing its offering without registration was illegal, rejecting Ripple's due process defense, stating:

"The Court rejects Defendants' fair notice and vagueness defenses as to the Institutional Sales. First, the caselaw that defines an investment contract provides a person of ordinary intelligence

*a reasonable opportunity to understand what conduct it covers . . . Howey sets forth a clear test for determining what constitutes an investment contract, and Howey's progeny provides guidance on how to apply that test to a variety of factual scenarios . . . That is constitutionally sufficient to satisfy due process. See United States v. Zaslavskiy, No. 17 Cr. 647, 2018 WL 4346339, at *9 (E.D.N.Y. Sept. 11, 2018) ("[T]he abundance of caselaw interpreting and applying Howey at all levels of the judiciary, as well as related guidance issued by the SEC as to the scope of its regulatory authority and enforcement power, provide all the notice that is constitutionally required."). Second, the caselaw articulates sufficiently clear standards to eliminate the risk of arbitrary enforcement. Howey is an objective test that provides the flexibility necessary for the assessment of a wide range of contracts, transactions, and schemes. Defendants focus on the SEC's failure to issue guidance on digital assets and its inconsistent statements and approaches to regulating the sale of digital assets as investment contracts . . . But the SEC's approach to enforcement, at least as to the Institutional Sales, is consistent with the enforcement actions that the agency has brought relating to the sale of other digital assets to buyers pursuant to written contracts and for the purpose of fundraising. See, e.g., Telegram, 448 F. Supp. 3d 352; Kik, 492 F. Supp. 3d 169. Moreover, the law does not require the SEC to warn all potential violators on an individual or industry level . . . "*

As to the remaining aspects of Judge Torres's decision, this is hardly a victory for a slew of reasons, all of which I exhaustively discuss in a recent an X article.

Ultimately, Ripple Labs Inc. was ordered to pay a civil penalty of $125 million for violating the securities laws by selling its XRP token to institutional investors, a fraction of what US regulators had sought in a long legal battle. Both Ripple and the SEC appealed the decision.

SEC v. Consensys

Back in April, Consensys Software, Inc. had gone forum-shopping and sued the SEC in Texas after it received an SEC Wells Notice over its products and dealings in Ethereum (they also sued the SEC Commissioners, including its Chairman at the time, Gary Gensler). A Texas federal judge dismissed the lawsuit.

By way of background, an SEC Wells Notice is a formal notification issued by an SEC Enforcement staffer to inform a company/individual that the SEC staff intends to recommend to the SEC Commissioners that the SEC initiate an enforcement action against that Well's Notice recipient. The Wells Notice gives the recipient an opportunity to provide a written explanation or argument (a "Wells submission") as to why the SEC Commissioners should decline the staff's recommendation. A Wells Submission can be in writing or video. The Wells Submission is nonpublic, unless the recipient opts to make it public, an option rarely exercised for obvious reasons. Consensys responded to the Wells by essentially asking the Texas federal court to launch a judicial "preemptive strike:" 1) Declaring that ether transactions are not securities; 2) Barring the SEC from suing firms over their use of ether; and 3) Declaring Consensys' MetaMask software on the right side of the law.

IMHO, Consensys's lawsuit did not pass the straight face test, because, as any first-year law student can attest, the SEC's threat of enforcement via a Wells Notice and any subsequent SEC

enforcement action are not final actions a court can review. In other words, Consensys's case lacked "ripeness," a fundamental federal civil procedure requirement.

Meanwhile, in June, per some reports, the SEC notified Consensys that it had closed its investigation into Ethereum 2.0. However, the SEC ended up suing Consensys in New York, alleging that Consensys engaged "in the unregistered offer and sale of securities through a service it calls MetaMask Staking and with operating as an unregistered broker through MetaMask Staking and another service it calls MetaMask Swaps."

More Decisions

In a remarkably short period of time, U.S. federal judges have drafted a century's worth of case law answering the question of whether a digital asset is a security with a resounding "yes." Some other recent cases worthy of note:

SEC v. Shavers, No. 4:13-CV-416, 2013 WL 4028182 (E.D. Tex. Aug. 6, 2013)

SEC v. REcoin Grp. Found., LLC, No. 1:17-cv-05725, 2017 WL 4329876

(E.D.N.Y. Sept. 29, 2017).

SEC v. Grybniak, 2024 WL 4287222 (E.D.N.Y. Sept. 24, 2024)

*SEC v. Payward, Inc., 2024 WL 4511499, at *8-9, *17-18 (N.D. Cal. Aug. 23, 2024)*

*SEC v. Balina, 2024 WL 2332965, at *8-11 (W.D. Tex. May 22, 2024) appeal docketed 24-50725 (5th Cir.)*

*SEC v. Teshauter, 2024 WL 1348432, at *4-6 (S.D. Tex. Mar. 29, 2024)*

SEC v. Genesis Global, 2024 WL 1116877 (S.D.N.Y. Mar. 13, 2024)

*SEC v. Wahi, 2024 WL 896148, at *6 (W.D. Wash. Mar. 1, 2024)*

SEC v. Arbitrade, 668 F. Supp. 3d 1290 (S.D. Fla. 2023)

SEC v. NAC Foundation, 512 F. Supp. 3d 988, 995 (N.D. Cal. 2021)

*SEC v. Blockvest, 2019 WL 625163, at *9, *11 (S.D. Cal. Feb. 14, 2019)*

*United States v. Zaslavskiy, 2018 WL 4346339, at *7, *9 (E.D.N.Y. Sept. 11, 2018)*

See also: *Hodl Law v. SEC, 2024 WL 3898607 (9th Cir. Aug. 22, 2024)*

The Wave of SEC Crypto-Victories is Not Surprising (At All)

It is of no consequence that: 1) Digital assets are not any sort of tangible item – digital assets are mere computer code that operate on blockchain technology; and 2) Digital Assets do not

necessarily memorialize any contractual relationship with any particular company or issuer or other party, and in and of themselves do not inherently constitute securities.

As famed Bloomberg legal commentator Matt Levine explains:

"Courts have consistently found that the "object" of an investment contract is distinguishable from the investment contract—each digital asset "all by itself is not a security, just as the orange groves in Howey were not." See, e.g., SEC *v.* ETS Payphones, Inc.*, 408 F.3d 727, 732–33 (11th Cir. 2005) (scheme involving sale-leaseback of payphones was an investment contract, without suggesting that the payphones were securities);* Kemmerer *v.* Weaver*, 445 F.2d 76, 79–80 (7th Cir. 1971) (sales of "live breeding beavers" plus service agreements for their care was an investment contract, without suggesting that the beavers themselves were securities). Thus, digital assets implicate the securities laws only when sold as part of an ongoing "investment contract, transaction or scheme ..."*

To argue that token issuers are not selling tokens as a fund-raising tool (i.e. as an investment) does not pass the straight face test. The tokens are clearly just like *stock*. The token issuer takes in fiat cash, uses the money to build some sort of project or enterprise (and enrich themselves in the process) and an investor receives a token, which represents some sort of ownership interest in that project.

There are two fundamental securities laws in the US that were created to avoid a financial meltdown like the one that occurred in 1929 -- the '33 Act and the '34 Act:

- The '33 Act — The Securities Act of 1933 — regulates the *issuance* of securities: If you want to raise money for your business by selling stocks or bonds, you have to register your sales with the SEC and give buyers a prospectus with disclosure about your business, which among other things, presents a fair and accurate depiction of the financial condition of your company, its operations, management, etc. The registration statement is also "audited" by an independent accounting firm who verifies the accuracy of the company's representations contained therein; and

- The '34 Act — The Securities Exchange Act of 1934 — regulates the *trading* of securities: It has rules for stock exchanges and brokers, rules against fraud in stock trading, rules for continuing disclosure by companies with publicly traded stock and rules requiring that the regulated is subject to an inspection, audit and examination anytime the SEC feels like it.

Matt Levine explains this notion further:

"The form of economic ownership is not exactly the same as it is in the case of stock, but it is closely analogous. If you buy a token and the project becomes popular, the token will be worth more. The token might pay dividends (in the form of staking rewards), or its price might be propped up by buybacks (burning) paid for out of the revenues of the project, just as in the case of corporate stock. It might have some sort of voting or governance rights, or a right to validate

transactions in the project. But in any case it will go up and down with the popularity of the project, of the business; it will remain a speculative investment in the project."

Big Crypto's Arguments Are Fatally Flawed

To counter Matt Levine's argument above, digital asset financiers paradoxically point to the many different types of digital asset offerings that the SEC has charged for failing to register without specifying them as such beforehand. But this argument fails on its face, and fatefully proves the contrary, i.e. that securities laws are indeed adaptable to new technology. But as U.S. District Court Judge Katherine Polk Failla recently wrote in her 84-page Coinbase order (discussed above):

"[T]he "crypto" nomenclature may be of recent vintage, but the challenged transactions fall comfortably within the framework that courts have used to identify securities for nearly eighty years."

In short, crypto-case law now speaks volumes, and a broad range of Article III judges have now definitively stated that crypto assets are subject to federal securities laws as a matter of law. In fact, there now exists a robust, extensive, ubiquitous and extraordinary library of judicial crypto decisions -- all glaringly presented in plain view, for all securities lawyers to incorporate into their corporate legal counseling practices.

The Stark reality is that a proven, effective and unambiguous legal framework to regulate crypto assets exists, and courts have unqualifiedly affirmed its applicability over and over again. Crypto-financiers may not like the judicial outcomes of SEC enforcement policing, and the SEC may opt to ignore their existence – but these SEC crypto-victories are now resolutely rooted in judicial doctrine and cannot be "disappeared" like an SEC crypto unit chief or an SEC crypto trial lawyer.

II. CRYPTO HAS BECOME A KILLER APP FOR CRIMINALS

The dire externalities of crime and mayhem enabled by blockchain's most prominent uses – digital assets and DeFi - cannot be overstated.

For criminals, the regulatory vacuum and anonymizing features of digital assets enables the committing of treacherous crimes like never before and all around the world. Along these lines, crypto has evolved into a killer app for criminals, which is perilous for everyone everywhere.

Crypto and Ransomware

Take for example the crypto-crime of ransomware. Perpetrators of ransomware attacks demand crypto to unlock corporate IT systems and data that the attackers have surreptitiously encrypted.

Collecting crypto (typically bitcoin) in extortion transactions allows ransomware attackers not only to conceal their tracks and identities, but also to conduct their schemes from anywhere in the world.

Ransomware attacks have grown exponentially since the advent of bitcoin in particular, and but for bitcoin, ransomware would not exist.

For instance, FinCEN announced in November, 2022, that US financial institutions spent nearly $1.2B on ransomware payouts in 2021 more than double from 2020, and three quarters of the 1,251 ransomware payments pertained to ransomware were apparently paid to Russian gangs. If crypto were so easy to trace, then the identities, whereabouts and details of the ransomware payment collectors would become known -- and prosecutions would follow. But that rarely, if ever, actually happens.

In 2023, ransomware actors intensified their operations, targeting high-profile institutions and critical infrastructure, including hospitals, schools, and government agencies. Major ransomware supply chain attacks were carried out exploiting the ubiquitous file transfer software MOVEit, impacting companies ranging from the BBC to British Airways. As a result of these attacks and others, ransomware gangs reached an unprecedented milestone, surpassing $1 billion in extorted cryptocurrency payments from victims (not counting the many ransomware attacks and payments that go unreported.

Indeed, ransomware attacks rose by 13 percent in the last five years, with the average ransom thus far is $2.73 million, almost an increase of $1 million from 2023.

If crypto were so easy to track, then the tens of thousands of ransomware attackers would all get caught. But the reality is that only a minuscule few are ever even identified, let alone apprehended, charged, extradited and brought to justice. Too many crypto-related tools exist to obscure, mask, disguise, camouflage and secrete crypto-transactions.

Going forward, statistics reveal that a ransomware attack will occur every 2 seconds by 2031, which will have a devastating impact on people, companies and the entirety of the global capital marketplace.

Crypto And Other Crimes

Traditional crimes have also increased exponentially because of crypto, including:

Drug-dealing, Terrorism financing, human sex trafficking, child pornography, money laundering, sanction evasion by countries like Russia, North Korea and Iran, who use crypto to transfer funds outside financial systems, assassins and other killers seeking payment for murder-for-hire services and a slew of other financial crimes.

North Korea is a particularly egregious criminal application of crypto and money laundering. North Korea's crypto hackers are paving the road to nuclear Armageddon. North Korea has quietly become a cryptocurrency superpower, stealing billions in bitcoin and ether and is funneling profits to fund its nuclear weapons program.

In fact, just a few weeks ago, the cryptoverse experienced a new record-shattering North Korean hack of the cryptocurrency exchange Bybit. Bybit is less known in the United States, as it is not permitted to serve US customers, but Bybit is the second-largest exchange globally, ahead of

Coinbase and behind Binance. On February 21, attackers stole more than 400,000 ETH (priced at around $1.5 *billion*) from one of the company's so-called "cold wallets." This was the largest financial theft in the history of the world – and it appears that the robbery was a total success.

This is not just devastating for Bybit's customers, it's also a national security emergency. Analysts have linked the attack to North Korea's Lazarus Group, known for exploiting cryptosecurity vulnerabilities to finance North Korea's regime and bankroll nuclear weapons programs.

What sets the Bybit hack apart is not only the amount stolen but also the extraordinary pace of post-hack money laundering. Within less than 24 hours after the hack, $160 million had already been funneled through illicit channels, an amount that would have been unimaginable to move this quickly just a year ago. As one commentator noted, the scale and speed of this laundering operation "mark a dangerous evolution in how nation-state hackers can exploit the crypto ecosystem."

The Lesson? Twofold. First off, the Bybit heist is just another day in the shadowy and chaotic global capital marketplace of the cryptoverse. It isn't that the fox is guarding the chicken coop – it's that no one is guarding the chicken coop.

Second, and even more importantly, the Bybit hack shows that when intermediaries don't register, it's not just investors who get hurt. The tumultuous and frenzied business model of the cryptoverse has ushered in both a new era of global financial systemic risk and novel national security hazards, which are threats to everyone, everywhere.

DOJ and Catching Crypto Thieves

Yes, U.S. Department of Justice (DOJ) occasionally catches someone (e.g. discovering their crypto in a laptop under a blanket in a popcorn tin in a bathroom) but those apprehensions and interdictions are few and far between.

For instance, according to DOJ, the cross-border nature of digital asset technologies requires collaboration with foreign law enforcement partners to locate and gather electronic records and digital evidence involving off-shore digital asset issuers, trading platforms, service providers and other online infrastructure; to seize and prevent further distribution of digital assets linked to crime; and to identify and hold responsible criminal actors who exploit pseudonymity features of Defi and blockchain technologies to avoid detection, identification and prosecution.

Along the same lines, from ransomware payments demanded in cryptocurrencies to state actors using digital assets to circumvent sanctions and other restrictions, DOJ is raising the alert that crypto is expanding into every area the agency is exploring.

The Fictitious Right to (Secretly) Transact in Crypto

For crypto-enthusiasts, one reason that crypto was created was to restrain governmental intrusion into financial privacy. In fact, in response to my postings, crypto-enthusiasts (albeit sometimes

rudely and impolitely) often praise the pseudo-anonymity of crypto-payments, proudly citing their own personal fundamental democratic and libertarian cravings for privacy of financial transactions.

Unfortunately, this brand of cognitive dissonance sorely misses the point. Though concealment of financial transactions may have libertarian appeal, the U.S. Congress has already determined that affording anonymity in financial transactions is not worth the cost of the global spread of terrorism, crime and economic chaos.

In the U.S., individuals do not have a right to keep their financial transactions secret from the government. There exists a slew of critical and historically significant regulations along these lines.

For instance, the Bank Secrecy Act (BSA) establishes program, record-keeping and reporting requirements for national banks, federal savings associations, federal branches and agencies of foreign banks. The BSA, amended to incorporate the provisions of the USA PATRIOT Act, also requires every bank to adopt a customer identification program as part of its BSA compliance program.

In addition, U.S. law generally prohibits making payments to those who are enemies of the U.S, such as terrorist organizations. Hence, in the U.S., a person must also know the identity of anyone to whom they make payments. The U.S. Treasury Department's Office of Foreign Asset Controls (OFAC) supervises the enforcement of these sanctions laws, such as The Trading with the Enemy Act and the International Emergency Economic Powers Act.

Finally, there also exist an array of broad and sweeping U.S. federal reporting requirements to the U.S. Financial Crimes Enforcement Network (FinCEN), the U.S. Internal Revenue Service (IRS) and other government regulators and law enforcement institutions relating to financial transactions by banks, broker-dealers, money service businesses and a litany of other financial firms.

It's critical to understand that money laundering is the process of making illegally-gained proceeds (i.e. "dirty money") appear legal (i.e. "clean"). Typically, it involves three steps: placement, layering and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean." Money laundering can facilitate crimes such as drug dealing, child sex trafficking, terrorism and sanctions evasion and can also adversely impact the global economy.

In its mission to "safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activity," the Financial Crimes Enforcement Network acts as the designated administrator of the Bank Secrecy Act (BSA). The BSA was established in 1970 and has become one of the most important tools in the fight against money laundering. Since then, numerous other laws have enhanced and amended the BSA to provide law enforcement and regulatory agencies with the most effective tools to combat money

laundering. (An index of anti-money laundering laws since 1970 with their respective requirements and goals in chronological order can be found here.)

Other than the staunchest of crypto's libertarians, few politicians actually believe that the cryptoverse should be exempt from, or receive special treatment under, well-established anti-money laundering laws.

Along these lines, the U.S. Congress has already decided that it is worth sacrificing some financial privacy to make sure there's no future 9/11. The true believers of crypto have never understood that — their very mantra is giving people a means to shield themselves from government oversight. And as for pro-crypto politicians, their hype and bluster are not just misguided and exploitive, it's also just plain hypocritical.

AML laws serve an important purpose in protecting U.S. citizens from terrorism and other crimes. It's a challenging balancing act – individual rights versus the proliferation of terrorism.

But under any circumstance, while crypto-enthusiasm's quest for building a money system outside of government control may be a worthwhile objective, it currently flies in the face of a broad range of standard and well-established U.S. laws. In short, the cryptoverse should start blaming Congress, not the SEC, FinCEN, IRS, etc. for its frustration and consternation and take any libertarian conflict to Congress and not to the courts (because you will lose, these laws are ironclad).

Now do Fiat

I get it, legions of criminals have committed crimes using fiat currency (I should know, I spent almost 20 years investigating and prosecuting financial crimes). But crypto has evolved into the killer app for criminals, ushering in a crypto-crime wave of epic proportions. It is axiomatic that the scale of crime in crypto is orders of magnitude greater than what it is in traditional finance and is vastly underestimated.

Merely because some mythical engineer has discovered a potentially revolutionary manner to engage in and verify commercial transactions (e.g. replacing a traditional corporate entry recorded in an intermediary institution's centralized ledger with a virtual entry recorded on a blockchain's decentralized distributed ledger), does not mean that criminals should be permitted to create their own form of anonymizing legal tender to commit robbery, theft, drug dealing, sex trafficking, extortion, terrorism, etc.

Along the same lines, just compare banks with crypto firms to see if the "now do fiat" argument actually holds up. Banks are heavily regulated, and depositors generally have protections. In glaring contrast, with crypto firms there is no required insurance, no regulatory oversight, no consumer protections, no traditional examinations, auditing or inspections, no licensure, no mandated cybersecurity standards, no fiduciaries, no segregation of customer assets, no rules against insider trading or market manipulation — barely any traditional protections of any kind -- which renders the entirety of the crypto-ecosystem not just unsafe and dangerous but also easily susceptible to fraud, grift and chicanery.

Of course, it should go without saying that U.S. TradeFi is rife with bad actors and can be dangerous -- and is a system that has a lot of flaws -- and some really dire oppressive tendencies. I get it, I spent almost 20 years investigating and prosecuting financial crimes but the risks of transacting with U.S. registered financial institutions like banks and brokerages obviously pale in comparison to the risks of engaging in transactions with digital asset platforms and stablecoins.

Banks, as opposed to crypto-firms, are heavily regulated and depositors generally have protections. The stark reality is that with crypto firms there is no insurance, no regulatory oversight, no consumer protections, no examinations, no auditing, no licensure, no mandated cybersecurity standards, no fiduciaries, no segregation of customer assets, no rules against insider trading or market manipulation — no traditional protections of any kind -- which renders the entirety of the crypto-ecosystem not just unsafe and dangerous but also easily susceptible to fraud, crime and chicanery.

Additional Sources

-- This U.S. Treasury Department Report, is entitled, "Illicit Finance Risk Assessment in Decentralized Finance," and provides an unbiased and thoughtful review of crypto-crime data and trends.

-- This article explains how Hamas and other terrorist organizations evolve and transmogrify, changing their crypto financing techniques to evade capture.

-- This testimony from a former U.S. Department of Justice (DOJ) prosecutor (which is somewhat supportive/agnostic of blockchain) explains in plain language the challenges for law enforcement when terrorists use crypto.

-- This DOJ report responding to President's Biden's Crypto-Executive Order highlights how criminals and terrorists continue to use crypto and other digital assets for money laundering, weapons purchases, facilitating tax evasion, and evading sanctions.

-- This U.S. General Accounting Office Report explains how the increasing use of advanced obfuscation techniques makes blockchain analysis difficult and resource intensive for US agencies.

-- This recent panel discussion between the SEC's current and former Crypto Unit chiefs covers how the lack of crypto traceability makes detection of market manipulation an impossibility for any investor.

-- This DOJ Report explains how the cross-border nature of digital asset technologies requires collaboration with foreign law enforcement, which presents extraordinarily complex and sometimes impossible challenges for the identifying, arresting, extraditing and prosecuting crypto-criminals.

III. ACTUAL CRYPTO-CRIME TRACEABILITY IS A MYTH

At present, most criminals who utilize cryptocurrency to facilitate their criminal activities are highly unlikely to be apprehended, and their illicitly acquired cryptocurrency is virtually impossible to recover. This conclusion is unequivocal, and to assert otherwise is not only irresponsible but also demonstrably false.

Indeed, even in the best cases of crypto-tracking (which are rare, take a lot of effort and only work in some instances), the identity of the actual holder is typically found using subpoenas, search warrants, arrest, etc. Not an easy task when the individuals and entities reside in countries outside the U.S., who will not only fight U.S. law enforcement efforts but will even go so far as to refuse to accept delivery of service. (See e.g. SEC/Terraform case, where Terraform and its founder continue to fight SEC subpoenas despite a detailed ruling compelling them to do so.)

Crypto is Extraordinarily Challenging (and Can Be Impossible) to Trace

The spreading the myth that crypto-transactions are easy to trace is perhaps the most frustrating and misleading of all crypto-enthusiast retort. While crypto payments (if not obscured or properly laundered) might in some instances provide a glimpse into the chain of where crypto is going, the chain does not identify who the crypto is going to.

Consider ransomware attacks as an example. If crypto were so easy to track, then the tens of thousands of ransomware attackers would all get caught. But the reality is that only a minuscule few are ever even identified, let alone apprehended, charged, extradited and brought to justice. Too many crypto-related tools exist to obscure, mask, disguise, camouflage and secrete crypto-transactions.

The amount of ransom payments actually made to ransomware attackers can never be know – but with respect to reported ransomware payments, FinCEN announced in November, 2022, that US financial institutions spent nearly $1.2B on ransomware payouts in 2021 more than double from 2020, and three quarters of the 1,251 ransomware payments pertained to ransomware were apparently paid to Russian gangs. In 2023, the total amount of money received by ransomware actors amounted to 1.1 billion U.S. dollars, up by over 140 percent from 457 U.S. dollars in the year prior, and estimates in 2024 were slightly lower, despite yet another barrage of catastrophic ransomware attacks.

Again, if crypto were so easy to trace, then the identities, whereabouts and details of the ransomware payment collectors would become known -- and prosecutions would follow. But that rarely, if ever, has actually happened.

Second, while crypto payments (if not obscured or properly laundered) might in some instances provide a glimpse into the chain of where crypto is going, the chain does not identify who the crypto is going to.

Finally, even in the best cases of crypto-tracking (which are rare, take a lot of effort and only work in some instances), the identity of the actual holder is typically found using subpoenas, search warrants, arrest, etc. Not an easy task when the individuals and entities reside in countries

outside the U.S., who will not only fight U.S. law enforcement efforts but will go so far as to refuse to accept delivery of service. (See e.g. SEC/Terraform case, where Terraform and its founder continue to fight SEC subpoenas despite a detailed ruling compelling them to do so.)

Along these lines, the U.S. Treasury Department, in an April 6, 2023, Report entitled, "Illicit Finance Risk Assessment in Decentralized Finance" stated ominously:

> *"[T]here are some limitations to relying on public blockchain information and tracing to mitigate illicit finance risks in the DeFi space. First, as noted above, the data on the public blockchain is pseudonymous. While regulators, law enforcement, and public blockchain companies can in some cases identify transaction participants, they may in other cases only have the participants' wallet addresses without additional identifying information. Additionally, users can obfuscate the tracing of transactions on the public blockchain through the use of mixers, cross-chain bridges, or anonymity-enhanced cryptocurrencies (AECs), which can create challenges for blockchain tracing. Second, blockchain tracing and analytics often require an initial identified illicit transaction or address as a starting point, although new tools are able to identify potentially suspicious activity based on blockchain data. Third, critical activities in a DeFi service can occur off-chain and there are challenges to locating and obtaining this data."*

What About Fiat? Tracing Fiat is Far More Challenging Than Tracing Crypto

Crypto enthusiasts often resort to the talking point that using fiat currency to commit crimes is far more common than using crypto to commit crimes and tracing crypto is a lot easier than tracing fiat currency. This is a maddening, misguided and feeble deflection.

I get it, legions of criminals have committed fraud using fiat currency. But crypto has created digital mayhem beyond imagination. For example, a criminal cannot use cash: to collect a $5 million ransomware payment; to raise $10 million for a terrorist attack; to pay $1M for a suitcase of heroin or to transfer $5K to the dark web to download child pornography. But crypto easily facilitates these crimes and many others and has increased crime exponentially.

Silk Road, Zhong and Bitfinex

By way of background, Silk Road was an early darknet market that operated from 2011 to 2013, primarily in the transaction of illicit drugs. Silk Road was closed in 2013 following raids by the FBI and other agencies. Silk Road founder Ross Ulbricht is currently serving **two life sentences in prison** after being found guilty of money laundering, computer hacking, and conspiracy to traffic narcotics.

During the sentencing of Ulbricht, Judge J. Paul Oetken of the U.S. District Court for the Southern District of New York held that all of the approximately 9.9 million bitcoin that passed through Silk Road was subject to forfeiture. Zhong allegedly defrauded Silk Road by rapidly executing transactions that fooled the online marketplace's payment system into depositing bitcoin into his account, exploiting a weak point in Silk Road's infrastructure in 2012 and from that, amassed about 53,500 bitcoin. For almost ten years, the whereabouts of this massive chunk of missing Bitcoin had ballooned into an over $3.3 billion mystery.

The DOJ seizure of a big part of the missing bitcoin (in addition to bitcoin surrendered to DOJ by Zhong himself) resulted when a law enforcement, pursuant to a search warrant, discovered a laptop that contained the previously elusive bitcoin.

Specifically, on November 9, 2021, law enforcement executed a search warrant on Zhong's home and located 50,491.06251844 bitcoin of the approximately 53,500 bitcoin crime proceeds (a) in an underground floor safe; and (b) on a single-board computer that was submerged under blankets in a popcorn tin stored in a bathroom closet.

In total, the Zhong-related bitcoin forfeitures included:

- 50,491.06251844 Bitcoin seized from Zhong's home on November 9, 2021;
- 825.38833159 Bitcoin provided by Zhong on March 25, 2022; and
- 35.4470080 Bitcoin provided by Zhong on May 25, 2022.

While blockchain tracing may have allowed law enforcement to go back years to track and trace the flow of Zhong's funds, what was critical was the 10+ years of police work that followed (such as search warrants and other legal processes), together with a lot of luck, which allowed DOJ, IRS and others to piece together a decade of money laundering.

A similar stroke of luck, circumstance and hard work yielded impressive results in a case involving Bitfinex. According to court documents, lya Lichtenstein, 34, and his wife, Heather Morgan, 31, both of New York City, allegedly conspired to launder the proceeds of 119,754 bitcoin that were stolen from Bitfinex's platform after a hacker breached Bitfinex's systems and initiated more than 2,000 unauthorized transactions. Those unauthorized transactions sent the stolen bitcoin to a digital wallet under Lichtenstein's control.

Over the course of five years, approximately 25,000 of those stolen bitcoin were transferred out of Lichtenstein's wallet via a complicated money laundering process that ended with some of the stolen funds being deposited into financial accounts controlled by Lichtenstein and Morgan. The remainder of the stolen funds, comprising more than 94,000 bitcoin, remained in the wallet used to receive and store the illegal proceeds from the hack. After the execution of court-authorized search warrants of online accounts controlled by Lichtenstein and Morgan, special agents obtained access to files within an online account controlled by Lichtenstein. Those files contained the private keys required to access the digital wallet that directly received the funds stolen from Bitfinex and allowed special agents to lawfully seize and recover more than 94,000 bitcoin that had been stolen from Bitfinex. The recovered bitcoin was valued at over $3.6 billion at the time of seizure.

In the Bitfinex prosecutions, the U.S. tracked down Lichtenstein and Morgan, who were not hiding, but were instead living the high life in New York City and had become celebrated Internet celebrities/influencers who showed off their wealth for all to see. But even given the near notoriety and fame, without the private key found during a search warrant, the seizure and identification efforts would have likely failed. The U.S. found the private key only because the defendants foolishly converted some of their bitcoin to gift cards using: 1) A gift card exchange

platform that respected U.S. search warrants; and 2) An email address that linked to a cloud account at a cloud service also willing to respect a U.S. search warrant (where the defendants had hidden their private keys and a treasure trove of other inculpatory evidence).

N.B. in Bitfinex: 1) DOJ took six years of investigating before making any arrests; 2) The investigation required massive coordination of resources, engaging an alphabet soup of federal agencies (DHS; FBI; DOJ-Criminal Division; DOJ-CCIPs; DOJ-OIA; US Attorney's Offices in DC, EDPa. and SDNY; and even the Ansbach Police Department in Germany); and 3) The defendants were living as crypto-celebrities in plain view in New York City splashing their activities all over social media. Had the defendants been residing outside of the United States, the outcome would likely have been very different.

It would be somewhat naïve to conclude from the Bitfinex or Zhong cases that tracing and recovering crypto assets is always easy—or even always possible. Even with the latest blockchain analytics, investigations will typically take years (even a decade) to complete. As one former DOJ prosecutor, Duke Law Professor Shane Stansbury, testified so eloquently:

"Frequently, the hardest part of a cyber-related prosecution is demonstrating what investigators sometimes refer to as "hands on the keyboard." Digital breadcrumbs left by criminals can prove invaluable to investigators. But ultimately prosecutors must demonstrate that an identifiable person is behind the criminal activity. And in a criminal case, that identity must be established beyond a reasonable doubt. That is, of course, as it should be, but in cryptocurrency-related cases prosecutors will often have the distinctive challenge of relying on a very complex series of digital patterns and transactions to meet their burden.

That crucial connection of a criminal's identity to their criminal conduct is one of the main challenges posed by cryptocurrency. A public blockchain can be helpful, but often it can get one only so far. Prosecutors can spend years trying to penetrate the layers of obfuscation by savvy criminals. Even if they succeed, they may still face obstacles due to the current state of the cryptocurrency market."

The difficulty for law enforcement in tracing crypto is also recently highlighted in U.S. DOJ's response to President Biden's March 9, 2022, Executive Order, which called for certain U.S. government agencies to examine the risks and benefits of cryptocurrency assets and report back.

Per DOJ's response:

"Criminals continue to use cryptocurrency and other digital assets for money laundering, facilitating tax evasion, and evading sanctions. Criminals have developed increasingly sophisticated obfuscation techniques— complex and rapid transactions, "chain- hopping" by converting funds from one cryptocurrency into another, use of AECs, and other measures— designed to make tracing difficult and to place stolen funds beyond recovery. Criminals can also use mixers and tumblers, including automated services that employ smart contracts to combine multiple users' coins together before sending out unrelated coins to each user's designated recipient, to obfuscate their transactions.

These techniques are made easier by the fact that many digital asset exchanges and platforms make little or no effort to comply with anti-money laundering regulations, such as know-your customer (KYC) requirements, or operate in jurisdictions without anti-money- laundering and countering-the-financing- of-terrorism (AML/CFT) requirements in line with the international standards."

Along the same lines, from ransomware payments demanded in cryptocurrencies to state actors using digital assets to circumvent sanctions and other restrictions, DOJ is raising the alert that crypto is expanding into every area the agency is exploring.

Acknowledging that U.S. DOJ has seen a tremendous increase in crypto related crime over the past several years, DOJ's former director of National Cryptocurrency Enforcement Team (NCET), Eun Young Choi stated during her tenure:

"We are seeing cryptocurrency and digital assets really touch every aspect of criminal activity we investigate . . . By its very nature the technology is built in order to not rely on intermediaries, cross-border transactions that are immutable and irreversible. Law enforcement can freeze conventional transactions, but they can't do that with digital asset transactions."

Crypto Cloaking Devices

What was also critical is that the conduct in Zhong and Bitfinex is that the defendants did not bother to use any sort of mixer, tumbler or other tools to conceal the origin/location of his bitcoin (he used a popcorn tin and a blanket instead), which is now commonly part-and-parcel to crypto-money laundering, ransomware attacks, terrorism, sanctions evasion, drug dealing and so many other crypto-crimes.

Indeed, according to DOJ, mixers and tumblers are designed specifically to conceal or disguise the nature, the location, the source, the ownership, or the control' of a financial transaction**.** Along these lines, an Ohio man pleaded guilty to a money laundering conspiracy arising from his operation of Helix, a Darknet-based cryptocurrency laundering service. According to court documents, Larry Dean Harmon, 38, of Akron, admitted that he operated Helix from 2014 to 2017. Helix functioned as a bitcoin mixer/tumbler, allowing customers, for a fee, to send bitcoin to designated recipients in a manner that was designed to conceal the source or owner of the bitcoin. Helix was linked to and associated with "Grams," a Darknet search engine also run by Harmon. Harmon advertised Helix to customers on the Darknet to conceal transactions from law enforcement.

Along these lines, the U.S. Department of Treasury has imposed sanctions on crypto mixing service Tornado Cash, which has been used to launder over $7B worth of crypto since 2019.

Tornado cash is a virtual currency mixer that operates on the Ethereum blockchain and indiscriminately facilitates anonymous transactions by obfuscating, their origin, destination, and counter parties, with no attempt to determine their origin. Tornado receives a variety of transactions and mixes them together before transmitting them to their individual recipients.

According to DOJ, while the purported purpose is to increase privacy, mixers, like Tornado, are commonly used by illicit actors to launder funds, especially those stolen during significant heists.

Beyond Mixers and Tumblers

Unfortunately, crypto money laundering tools beyond mixers and tumblers continue to evolve into new and more effective iterations, continue to grow in popularity, and continue to add exponentially to the crypto-concealing toolkit, including:

- *Nested and Unregulated Crypto-Exchanges*. The lack of U.S. regulatory oversight relating to digital asset trading platforms and the extraordinary threat to investors posed by these so-called Web3 trading services extends to money laundering. Criminals can maintain accounts with various popular crypto trading platforms, which allow customers to trade using those accounts. The nested exchange even offers immediate access to all features without KYC requirements, marketing directly to criminals. For example, per a recent CNBC report, a major way criminals in the crypto world launder money is by sending digital assets across blockchains, bypassing a centralized service that can trace and freeze transactions. They use so-called cross-chain bridges to make it happen, and the dollar amounts are getting large. One particular cross-chain bridge called RenBridge has been used to launder at least $540 million in crime-related crypto cash since 2020, according to new research from blockchain analytics firm Elliptic.

- *Privacy Coins* (such as Monero (XMR), Zcash (ZEC) and Dash (DASH)). For instance, Monero encrypts the recipient's address on the blockchain and generates fake addresses to obscure the real sender. It also obscures the amount of the transaction. According to the report by the U.S. Attorney General's Cyber Digital Task Force called *Cryptocurrency: An Enforcement Framework* released on Oct. 8, privacy coins can undermine existing AML and be used to finance terrorism.

- *Chain-Hopping*. DOJ warns that chain-hopping is "frequently used by individuals who are laundering proceeds of virtual currency thefts," and involves swapping one's crypto holdings for others operating on a different blockchain like Bitcoin and Ethereum. Indeed, recent research from blockchain analytics and crypto compliance firm Elliptic has revealed the extent to which cross-chain bridges and decentralized exchanges (DEXs) have removed barriers for cybercriminals. In an Oct. 4 report titled "The state of cross chain crime," Elliptic researchers Eray Arda Akartuna and Thibaud Madelin took a deep dive into what they described as "the new frontier of crypto laundering." The report summarized that the free flow of capital between crypto assets is now more unhindered due to the emergence of new technologies such as bridges and DEXs. Per Elliptic, cybercriminals have been using cross-chain bridges, DEXs and coin swaps to obfuscate at least $4 billion worth of illicit crypto proceeds since the beginning of 2020.

- *Peer-to-Peer (P2P) crypto networks.* P2P decentralized networks allow the users to exchange crypto without an exchange, where criminals used unsuspected users (money mules) to send funds to other addresses and finally to an exchange in a country with little AML standards. For example, Play-to-earn (P2E) crypto games are emerging as a popular

blockchain application that brings in a high risk for scams and money laundering. P2E crypto gaming offer tokens that can be easily sold outside of gaming environments. Gamers can then sell their crypto funds earned in obscure P2E crypto games for more liquid ERC-20 tokens that run on top of Ethereum, especially stablecoins, on centralized

or decentralized exchanges. Gamers then can convert their more popular tokens into the fiat currency of their choice.

- *Gambling Platforms.* Crypto-gambling casinos now flourish all over the world. Criminals can use online gambling sites to send crypto from one country to a wallet address controlled by a criminal in another country. As a result, a criminal may purchase chips with crypto, conduct a few transactions and then "cash" them out to a wallet address which is controlled by the same criminal, another associate or a "nested service provider" "Or, two associates, the buyer and the seller of illegal goods both hold a gambling account with the same provider. Then, they transfer between the gambling account as a player-to-player transfer. The seller then will "cash out" the money as gambling profits, where this is the profits for selling illegal goods. Along these lines, FinCEN is watching casinos that offer sports betting and crypto payment options for potential money laundering problems.

- *Non-Fungible Tokens (NFTs)*. NFTs can be bought and sold using cryptos on specialized marketplaces. A recent study by the US Treasure Department found that the booming NFT market could be a target for money laundering and terrorist financing who want to "clean" illegally obtained funds. NFTs can be instantly transferred from one party to another without any geographical boundaries or regulatory restrictions. "For example, a criminal can generate an anonymous NFT, list in for sale on the blockchain and then purchase it from himself through an anonymous and unregulated digital wallet which contains illegal funds in another jurisdiction. The NFT could at the end be sold to an unsuspected individual who will purchase the NFT with clean funds." Money laundering allegations relating to NFTs are widespread, even nefarious allegations relating to the NBA NFT marketplace.

- *Off-Chain*. The biggest myth in crypto is that all cryptocurrency transactions are recorded on the blockchain. In fact, per AML expert Alison Jimenez, "Just a small fraction of crypto transactions are permanently, immutably, de-centrally recorded on the blockchain. Most transactions occur off-chain, within exchanges, who keep private ledgers. History has shown us plenty examples of 'sloppy' or fraudulent recordkeeping by crypto companies." (See expanded discussion below, "A Final Note on the Myth of CryptoTraceability")

A Final Note on the Myth of Crypto-Traceability

Below are some more extraordinarily insightful conclusions regarding so-called "CryptoTraceability" from taken from a February 1, 2024, article written by Alison Jimenez and entitled,
"Cryptocurrency Traceability: Unraveling Underlying Assumptions."

"Just because…a crypto transaction occurred, does not mean that the transaction was recorded on the blockchain. The biggest myth in crypto is that "all crypto transactions are recorded on the blockchain." Most crypto transactions occur within exchanges. The exchange transactions occur on private ledgers and internally match buyers and sellers. These transactions are not posted on the blockchain. Therefore, there is no record of the internal crypto exchange transaction to trace on the blockchain.

Just because…a crypto transaction was recorded on the blockchain, does not mean that the cryptocurrency is traceable. Bad actors can use a variety of obfuscation techniques to thwart on-chain tracing. For example, decentralized exchanges, mixers, privacy coins, side-chains, chain hopping, moving cryptos in and out of exchanges or crypto casinos, all hinder tracing of on-chain transactions. Additionally, all blockchains are not created equal. Some blockchains have enhanced privacy which hinders traceability.

Just because…a cryptocurrency transaction is traceable, does not mean that the transaction has been attributed. Or that the attribution is correct. There is no universally agreed upon definition of blockchain "attribution." Some commentators define attribution as "links" or "ties" between an address and a real-world person or entity. While others more broadly link an address to an event.

The following may all be considered attribution in blockchain analytics:

-- A ransomware event where the bad actor is unknown

-- A hack event where the hacker is unknown

-- A ransomware event or hack undertaken by a known cybercrime group composed of unknown individuals

-- A wallet linked to a Twitter or Discord handle

-- An address linked to an offshore exchange with unknown ownership

-- A wallet linked to a mining pool composed of unknown individuals

-- A DEX or DAO with unknown individual controllers/managers

-- A darknet market with unknown owners"

Along the same lines, in November of 2023, Ms. Jimenez testified before House Sub-Committee on Digital Assets, Financial Technology, and Inclusion, Hearing: Crypto Crime in ContextBreaking Down the Illicit Activity in Digital Assets.

Unlike the other witnesses testifying at the extraordinarily memorable hearing, Alison Jimenez was not bought and paid for by crypto-firms. Ms. Jimenez is beholden to no one and bases her testimony solely on established facts and hard data. In fact, Ms. Jimenez has no bias whatsoever,

is 100% independent and objective and only seeks truth -- which makes her testimony all the more powerful and uniquely credible.

As Ms. Jimenez explains metaphorically in her chain-analysis takedown: *"If all cryptocurrency transactions were an iceberg, the crypto transactions subject to blockchain analytics is the small portion above the waterline."*

Suspicious Activity Reports (SARs)

The purpose of Suspicious Activity Reports (SARs) is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations of the Bank Secrecy Act (BSA). In many instances, SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases.

Information provided in SAR forms also presents the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) with a method of identifying emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions. Below are some key facts about crypto-related SARs pointed out by Ms. Jimenez:

- The number of SARs filed related to cryptocurrency is growing exponentially. Over 92,000 cryptocurrency SARs were filed in 2021 reflecting transactions worth over $96 billion dollars;

- Bad actors prefer to use cryptocurrency over many other financial products. When adjusted for percentage of U.S adults using a given financial product, crypto SAR filings dwarf SARs filed relating to investment products and are gaining ground on U.S currency SARs. For example, there were 2.74 SARs per 1,000 Users of Crypto versus 0.18 SARS per 1,000 Users of Stocks. Even without adjusting for consumer adoption, there were more cryptocurrency SARs filed in 2021 than for all securities/investment products from 2014 through 2020; and

- The dollar value of each cryptocurrency SAR hovers near $1 million dollars which is significantly greater than the dollar value of other products and industries; and

The Limits of Blockchain Transparency

Many bad actors have changed how they transact with cryptocurrency on the blockchain to limit exposure to blockchain analytics and tracing. Per Ms. Jimenez, on-chain obfuscation methods include:

- *Using mixers;*

- *Using De-Fi protocols as a mixer;*

- *Transacting on "layer 2" protocols such as the bitcoin Lightning Network;*
- *Hopping from one blockchain to another;*
- *Creating new 'clean' wallets or addresses for each on-chain transaction;*
- *Using privacy-enhanced cryptocurrencies; and*
- *Selecting blockchains with enhanced privacy features*.

Meanwhile, attribution of a wallet address to a specific person or entity is challenging, especially for the private sector who lack access to off-chain data available to law enforcement or intelligence agencies. Additionally, blockchain analytic firms do not always reach the same conclusions regarding attribution even when they are working from the same blockchain data. The data is skewed, the analysis varies, and the "analysts" employ different methodologies. Finally, the attribution and tracing methodology used by blockchain analytics firms is not only typically proprietary and unaudited but the blockchain analytics firms are actually owned and operated by crypto-firms who have an obvious interest in downplaying crypto-related crime.

Per Ms. Jimenez, most cryptocurrency transactions occur within crypto exchanges, who internally match buyers and sellers and act as market-makers, stepping in as a counterparty when a buyer/seller is unavailable. These off-chain transactions also escape traceability and blockchain analytics. Per Ms. Jimenez's well-footnoted research:

- *Researchers estimated that bitcoin transactions within exchanges to be ten times the volume of transactions executed on the blockchain: On-chain transactions, however, constitute only a small share of the universe of all Bitcoin trades, most of which are "off-chain" utilizing some form of exchange, some heavily regulated, some not so much;*
- *A crypto exchange's internal transactions are not recorded on the blockchain. Instead, these off-chain transactions are recorded on the exchange's internal ledger;*
- *Bad actors can use cryptocurrency but evade creating a blockchain record of transactions by simply conducting transactions within an exchange. As demonstrated by SAR filings by Virtual Asset Service Providers (VASPs), IC3 and CFPB complaints, and criminal indictments, this is in fact occurring; and*
- *Cryptocurrency exchanges have also engaged in market manipulation, wash trading, insider trading, and a host of other crimes. Perhaps even more concerning is that sanctioned countries are operating cryptocurrency exchanges."*

Why "Now do Fiat" Is a Farcical Retort

With common sense and diligent footnoting, Ms. Jimenez's testimony tackles head-on the cacophony of the "Now Do Fiat" whataboutism pivot/talking point from crypto-promoters, addressing their argument with facts, research and common sense. Ms. Jimenez states:

"Hopefully we can agree that the comparison below is nonsense: 'Alice drinks 2% milk. Bob puts 98% unleaded gasoline in his car. Bob's percentage is 49 times greater than Alice's!' Putting crypto crime into context is a worthwhile endeavor but making invalid comparisons only confuses the issue. Yet, statements like this are routinely used when discussing cryptocurrency's use in illicit finance versus traditional financial products. Commentators often erroneously compare a UN estimate of the value of illicit proceeds ranging 2% to 5% of global GDP to numbers published by blockchain analytics vendors that report transactions involving illicit address are less than 1% percent of all digital asset transaction volume. Some commentators extrapolate from the invalid comparison to suggest that "criminals don't like crypto." Here are a few reasons why this comparison is flawed:

- *The UN estimated the proceeds of crime, not the means of payment. The means of payment could have been real estate, oil, stock, jewelry, bartering of drugs for weapons, or government issued currency (fiat);*

- *Blockchain analytics illicit transactions only include "known" or "attributed" on-chain transactions while the UN's estimate was of all illicit proceeds, not just proceeds clearly "attributed" to criminals;*

- *Blockchain analytics vendors divide their illicit crypto transaction amount by all cryptocurrency transaction volume;*

- *Cryptocurrency transaction volume is inflated in several ways including: bad actors creating thousands of transactions to obscure fund movement, leveraged trading, rampant wash-trading, and moving cryptocurrency between wallets without any meaningful economic activity;*

- *Blockchain analytics calculations divides "known" illicit transactions by "all" cryptocurrency transactions. The denominator, "all crypto transactions", includes unidentified illicit activity, licit transactions, and unclassified transaction;*

- *Commentators often incorrectly interpret this data to only include the binary options of illicit or licit activity. Additionally, when transactions are attributed a regulated exchange, blockchain analytics often cannot determine if illicit crypto was involved; and*

- *Global GDP and "all cryptocurrency transaction volume" are not interchangeable and do not measure the same thing. Global "transaction volume" is orders of magnitude greater than Global GDP."*

What's most staggering is how crypto has almost instantaneously fueled a nascent and atrocious category of crime wave. Computers, phones, tablets and other networking devices have become the lawless continent on which criminals travel wherever they want, going into factories, stores and homes, stealing data in massive amounts to sell and use to enable more crime. "Criminals world-wide have been inspired by this near-instant, clandestine way to pay and accept money to ratchet up existing crimes and invent new ones."

Moreover, despite the law enforcement successes in Bitfinex, Zhong and a few other cases, the bottom line is that, at least for now, tracing crypto-transactions to catch criminals requires immense resources, years of doggedness and lots of luck – and prosecutorial success rarely happens. For example, at a meeting at FBI headquarters in Washington, D.C., with a dozen of the top cyber-agents and prosecutors from the FBI and DOJ, I asked them all, "How often is it that the FBI recovers ransomware payments?" As one senior FBI Agent and crypto-crime specialist responded quickly: "Never."

The Stark reality is that as Winston Smith says in the famed science fiction novel *1984* (and as I said in my 1982 high school graduation quote): "Freedom is the freedom to say that two plus two makes four. If that is granted, all else follows." Along these lines, the Crypto Task Force must acknowledge that for criminals who have incorporated crypto into their modus operandi, tracing their crypto transactions creates unprecedented challenges for law enforcement, regulators or anyone else.

IV. Blockchain Hype is Mostly Bunk

Despite its relentless hype and inexorable bluster, blockchain technology itself has extremely limited utility and is a solution to a problem that nobody has. Today, blockchain has one sole bonafide use case, which is powering cryptocurrency-- all other use cases are better served by a regular centralized database.

No doubt blockchain enthusiasts will taunt me with *OK Boomer* replies and insist that *I just don't get it*. But like one famed economist recently wrote, "*It really looks as if there never was an it to get."*

What is Blockchain?

What is blockchain? Put simply, a blockchain is a shared or *distributed* ledger that can store the complete transaction history of not just cryptocurrency but other kinds of records in an unchangeable and permanent record. Thus, users supposedly cannot manipulate data that's already in the blockchain. As such, blockchain attracted initial interest among some enterprises, especially those in banking and finance, who believe that blockchain can help to create new market infrastructure and drive efficiency in the trading of products across the globe.

However, the reality is that no matter how exciting and aspirational the venture capital blockchain propaganda, blockchain stubbornly remains a glorified, append-only, limited writer spreadsheet and immutable ledger -- which provides little utility for anyone.

The truth is that blockchain's technological DNA is laden with sluggishness, clunkiness, costliness, inefficiencies, security issues and a slew of other problems, which renders blockchain not just difficult to scale but also challenging to use. Hence, blockchain faces extraordinary obstacles and can never become the magical financial and societal panacea that its promoters have been promising for over 15 years.

Yet for reasons difficult to fathom, some professionals and some companies continue to cling to the dream of magical blockchain elixir. Consider a Goldman Sachs public relations blitz regarding their blockchain endeavors, specifically:

- A December 6, 2022 Wall Street Journal Op-Ed article entitled, *"Blockchain Is Much More Than Crypto," by Goldman's Chairman and CEO, David Solomon, stating, "Investors large and small stand to gain with blockchain innovations that are guided by established, experienced institutions;"* and

- A February 10, 2023, 20-minute video on CNBC Cryptoworld about their digital asset endeavors, which seemed uncomfortably choreographed, where a Goldman official proudly proclaimed that *"digital assets will bring about a paradigm shift in the financial market and beyond . . . The intersection between digital assets and ESG . . . [blockchain] technology really lends itself to that and allows for critical reduction of risks and cost savings. Key, profound [blockchain] foundations that can have a positive impact across financial markets."*

My take is that efforts by Goldman Sachs and anyone else's shilling of crypto's underlying technology of blockchain are less akin to technological innovation and more akin to marketing theater and transparently self-serving, frivolous propaganda.

And while not necessarily misleading, or otherwise unlawful, my opinion, as presented in this article and based on years of research and decades of experience, is that by enabling potentially perilous groupthink sophistry, blockchain euphoria threatens not just individual investors but could also impact the systemic stability of all global financial markets.

A New Word: *Blockchainification*

While laden with technobabble, blockchains are actually not a very complicated technology and have been around for decades. In fact, long before Nakamoto's white paper, famed technologist and cryptographer David Chaum, while studying at UCLA Berkeley in 1982, first outlined a blockchain database protocol in his dissertation, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups."

There were apparently decentralized databases before Chaum, but Chaum is most often cited as its inventor. Was Chaum's desertion too complicated for non-technologists to understand? Not really.

Anyone who has ever used a database or any other electronic repository of data stored in place -- from an excel spreadsheet to an Oracle SQL architecture --- can understand blockchain. Because blockchains are like any other database, except that all the data is public and copies of the

database are stored in many disparate places. Of course, the uses are extraordinarily limited. After all, not many databases in the world function well when everyone has access to it but no trusted person who can make changes to it.

Hence, *Blockchainification* --the art of injecting blockchain into any existing technology -- has now proven most often to fail miserably. Indeed, if blockchain disappeared tomorrow, the only ones hurt would be:

1. The litany of venture capitalists who have gambled on the potency of blockchain hype;

2. The cult of investors who have risked their life savings on the success of "greater fool theory economics;"

3. The cadre of marketing professionals who specialize in crypto and DeFi spin; and

4. The shameless legion of lawyers who woke up one morning and decided to change their bio to read: "Fintech Attorney."

Wall Street and Blockchain

What is most striking about blockchain propaganda is that although blockchain has been touted since 2008 as a game-changing revolution in how corporations handle and reconcile financial services, very little widespread blockchain utility has come to fruition.

In fact, Wall Street firms have been experimenting with blockchain projects for at least the past five years. Yet despite all the carnival barking, few have had a widespread impact on how financial transactions take place. Others have simply given up, like the group of European insurance companies who formed a consortium called B3i in 2016 to explore blockchain uses in their industry.

In July, 2022, the B3i consortium (which included Zurich, Swiss Re, Generali, Allianz, XL Innovate, SCOR, Aegon Blue Square, MAPFRE and Achmea) shut down after failing to raise new capital. A statement on the website reads:

> *"The directors, following consultation with the shareholders, have collectively concluded that there was not sufficient support to continue with the venture at this stage."*

In addition to transforming the insurance industry, blockchain promoters have promised how blockchain will streamline supply chains, upgrade payments infrastructure, accelerate clearing systems and make global trade more efficient and less dependent on third parties. But these claims now appear more like baseless flimflam and bravado masquerading as aspirational optimism.

But what blockchain promoters on Wall Street are really talking about are so-called "private blockchains" providing opportunities for enterprise applications. But there seems an obvious dearth of an actual application that at all impacts anyone's daily lives.

Moreover, ask any bona-fide, well-credentialed technologist (that isn't working for a crypto-firm or in a crypto-department) and they will likely conclude that blockchain most often seems more like a useless add-on than vital, transformational flywheel. Technologist Stephen Diehl explains this troubling blockchain phenomenon in a recent article:

"Indeed, the top-selling database solutions from companies like IBM, Oracle, and Microsoft have had all the selling points of private blockchains — immutability and auto-reconciliation — for more than 40 years. The so-called tokenization projects of banks . . . built on top of private blockchains to do intraday repo transactions or bond settlements are quite real, but the use of the word "blockchain" to describe any of this is pure innovation theatre. Tokenization is merely mundane "digitization" wrapped up in crypto language. And most securities markets have already been digitized since the 1980s."

What Diehl describes as "innovation theater" is not necessarily nefarious or problematic – all companies promote their wares and hype the innovation and invention of their operations.

The difference in blockchain, however, is that by promoting blockchain, Wall Street firms bestow an aura of legitimacy upon other crypto-related investments. In other words, crypto promoters leach on to Blockchain proclamations, amplify them exponentially and exploit them to dupe investors into buying crypto and buying into the myths (and deceit) of decentralized finance.

What these charlatans are doing with their blockchain promotion is using "blockchain" as an exhortation to describe what are otherwise routine back-office projects, with little impact on anyone except their clients, who may or may not be experiencing any benefits. For instance, that Wall Street firms portend to be bullish on crypto is a far cry from the reality – which, in my opinion is that Wall Street firms are merely selling digital bonds to other banks on a private database. Diehl explains:

"Blockchain technology is neither particularly innovative nor useful and has a terrible track record of success in the IT industry. In the best case, it is simply a buzzword describing mundane technologies that have existed for decades. In the worst case, it's a solution in search of a problem, a form of a technical fantasy that falsely promises to alchemize human trust through technology and is a symptom of the irrational exuberance and magical thinking arising out of cryptomania."

Reputation Laundering

Other than a likely flawed or misguided IT architectural initiative, the work Goldman Sachs and the rest of Wall Street are doing in and of itself not harmful in any way.

A financial firm can certainly run a bond settlement system using a private blockchain in the same way an automobile manufacturer can make a car with square wheels (and if you apply enough torque on the wheels the car will clunk forward). But to most technologists, jerry-rigging blockchain into an otherwise already efficient technological application is rarely an optimal solution. However, the problem is that efforts at blockchain self-promotion are actively co-opted as a deceptive form of "reputation laundering" for crypto investments.

For instance, a person with little experience in IT or banking who reads David Solomons' WSJ op-ed, could easily be tricked into thinking that Goldman is getting into crypto -- when the reality is that Goldman is merely upgrading their bond settlement system and wrapping it in some flavor-of-the-month buzzwords. Crypto promoters will spread this bogus narrative aggressively as a clever way to legitimize crypto i.e. "Hey everybody*, Goldman is getting into crypto, everyone else should too*." Even though such a characterization is not accurate and is grossly misleading – the blockchain buzzword adoption catapults blockchain groupthink and can make for a powerful pitch.

It should also go without saying that Goldman's blockchain efforts are not illegal in any way and may very well bear fruit for their clients someday (though that seems doubtful in my opinion). However, "tokenization" is not the same as "digitization" and Wall Street's marketing of it's likely inefficient, costly and cumbersome blockchain-use of bond settlement should not, in my opinion, provide a reason to run out and buy some crypto.

Technology Experts Agree: Blockchain is Wildly Over-Hyped

Meanwhile, as the burgeoning Big Crypto Cartel spent more money than the entire defense sector put together to foster and extend blockchain groupthink throughout the U.S. Congress and the groupthink brigade shilled blockchain as a futuristic game-changer and revolutionary equalizer, not every bought into the braggadocio.

In response, in a letter to U.S. Congressional leaders, the global tech community called out blockchain and all of web3 to be one big con, publishing their letter at concerned.tech.

The Concerned.tech Letter's over 1,500 signatories included professors, scientists and engineers from Amazon, ACM, Adobe, AMD, Apple, Box, Block, CMU, Cornell, Disney, Dropbox, eBay, Google, GitHub, IEEE, IBM, Microsoft, MIT, Meta, Mozilla, Pixar, Netflix, Oracle, Stanford, Shopify, Salesforce, Thoughtworks and VMWare.Signatories were not only programming language creators, scholars and legends of the tech industry but also everyday software engineers and coders. It was a unique and remarkable get-together of some of the greatest technical minds in the world. The Concerned.tech Letter:

- Tackles crypto groupthink head-on, centering around the premise that *facts are facts,* and explained the challenges to conjure up a single U.S. societal benefit (social, economic or otherwise) of crypto and the untraceable financial transactions it's use facilitates, and how in the U.S., there exists not a single task or process that crypto improves. Moreover, using crypto does not create greater security or safety for one's finances and is not convenient or free. In fact, the truth is precisely the opposite;

- Explains that, for the most part, the entire crypto ecosystem resided amid an unregulated, mysterious and often sinister environment, replete with fraud, trickery and manipulation; and

- Debunks blockchain groupthink with objective and independent technological expertise, concluding that when it comes to blockchain and all of web3, *there's no there there*.

In an interesting follow-up to the Concerned.tech Letter, next came yet another extraordinary study, this time of the top Google results for "blockchain production users" (and related queries), which analyzed 34 individual "real world blockchain" projects. One would expect some actual functioning projects that have an impact on every-day consumers — outside of cryptocurrency & NFTs. But looking into all 34, the researcher discovered that are already dead, 6 are only useful within the crypto & NFT ecosystems and not in the "real world" and 14 use Blockchain in a way where removing the blockchain would not impact functionality at all, or make the product better. The remaining project is Chainanalysis, which has real-world impact by helping law enforcement de-anonymizing blockchain users.

Along the same lines, famed cryptographer and security specialist Bruce Schneier, in an eerily prescient 2019 Wired article, explained so clearly why "there's no good reason to trust blockchain:"

"Private blockchains are completely uninteresting. (By this, I mean systems that use the blockchain data structure but don't have the above three elements.) In general, they have some external limitation on who can interact with the blockchain and its features. These are not anything new; they're distributed append-only data structures with a list of individuals authorized to add to it. Consensus protocols have been studied in distributed systems for more than 60 years. Append-only data structures have been similarly well covered. They're blockchains in name only, and—as far as I can tell—the only reason to operate one is to ride on the blockchain hype."

"To answer the question of whether the blockchain is needed, ask yourself: Does the blockchain change the system of trust in any meaningful way, or just shift it around? Does it just try to replace trust with verification? Does it strengthen existing trust relationships, or try to go against them? How can trust be abused in the new system, and is this better or worse than the potential abuses in the old system? And lastly: What would your system look like if you didn't use blockchain at all? If you ask yourself those questions, it's likely you'll choose solutions that don't use public blockchain. And that'll be a good thing—especially when the hype dissipates."

It's *Still* Still Not The Early Days

On January 14, 2022, technologist and software engineer Molly White authored a viral blog post entitled, "It's Not Still The Early Days," which details how blockchains are slow, do not scale well, and are expensive. White also noted how with blockchains, there is no "undo" button in order to try to achieve that trustless, censorship-resistant ideological goal. White concludes her article sardonically:

"How long can it possibly be "early days"? How long do we need to wait before someone comes up with an actual application of blockchain technologies that isn't a transparent attempt to retroactively justify a technology that is inefficient in every sense of the word? How much pollution must we justify pumping into our atmosphere while we wait to get out of the "early days" of proof-of-work blockchains? How many people must be scammed for all they're worth while technologists talk about just beginning to think about building safeguards into their platforms? How long must the laymen, who are so eagerly hustled into blockchain-based

projects that promise to make them millionaires, be scolded as though it is their fault when they are scammed as if they should be capable of auditing smart contracts themselves? The more you think about it, the more "it's early days!" begins to sound like the desperate protestations of people with too much money sunk into a pyramid scheme, hoping they can bag a few more suckers and get out with their cash before the whole thing comes crashing down."

It's been 3 $^{1}/_{2}$ years since Molly White penned her infamous blockchain critique and for Blockchain, It's *still* not still the early days. Meanwhile, blockchain:

- Still remains, an append-only linked list using cryptographic hashes, which have been around for decades;
- Still remains highly inefficient and with blockchain, inefficiencies and waste continue as features, not bugs; and
- Still remains a failure at just about everything the technology promises to accomplish.

Remember when Beeple's $69 million JPEG was bought with ether? The ether wasn't sent over the Ethereum blockchain — Christie's demanded direct transfer of the ether from one account on an exchange to another account on the same exchange.

As famed technologist David Gerard so eloquently stated back in 2021, *"The blockchain works so much better when you don't use it."*

Blockchain -- the particular flavor of cryptography/Merkle Trees compounded with a digital token system -- was invented in 2008. That is quite a long time ago in tech years. The obvious truth is that it has been 18 years or so since Blockchain "became a thing," and still there's not a single example of ANY application that blockchain does better than existing non-blockchain technology.

Indeed, virtually every implementation of blockchain is riddled with serious problems and whatever system it aims to provide utility to, from being a digital currency, to improving authentication, supply chain, ticketing or "digital ownership" rights, ends up being 10x worse than existing systems we're already using.

Blockchain's Inconvenient Truth

The actual blockchain application vacuum runs markedly counter to the bluster and boasting of blockchain enthusiasts. For instance, consider the typical earnings calls of Apple, Amazon, Alphabet, Microsoft, Oracle and others, where discussions of blockchain are not just absent, blockchain as a concept is wholly ignored.

Along the same lines, ask any technologist (not working in the cryptoverse): 1) To name any non-crypto phone application that uses blockchain; 2) To name any company that uses blockchain; or 3) To name any websites or social media sites that use blockchain. The answer will more than be radio silence.

Meanwhile, despite the fact that blockchain technology is not simply inferior, but dramatically inefficient, because it's popular and there's money being thrown at it by non-technologists, some companies and institutions have tried to use it. But in almost every single case, these projects have never materialized:

IBM/Maersk shut their blockchain system down, Microsoft shut their blockchain projects down, even municipal blockchain projects like Australia's stock exchange, admitted it was a failure.

If started at all, even the largest blockchain projects peter out quietly. Consider that six years after its initial launch, Microsoft shut down its Azure Blockchain as a Service project. Microsoft provided no real explanation for the termination except to tell ZDnet:

"We are asking customers to transition to the ConsenSys Quorum Blockchain Solution. Microsoft has a rich history of working with partners with the shared goals of innovating and delivering solutions to our customers. As industry dynamics have changed, we made the decision to shift our focus from a product-oriented offering to a partner-oriented solution."

Yes, there may exist a few random *Big Tech* aspirational projects and some splashy web pages replete with blockchain marketing collateral. But with these companies, there appears to be nothing exciting, innovative or even remotely profitable going on with blockchain. In stark contrast to legitimate technological wonders from fax machines to the internet to the iPhone to the cloud and to artificial intelligence, blockchain has become a deified pet rock, because after 15 years, there exists not a single blockchain project or blockchain use that actually makes anyone's lives better.

In fact, while the collapses of FTX, BlockFi, Celsius, Voyager, Terra and other crypto products and services dominated headlines, the failure of projects that attempted to use blockchain in private, corporate settings, has been quite telling yet has received far less attention.

Some Blockchain History

Back in 2015 and 2016, banks and large companies embraced blockchain's potential, pledging to take blockchain technology "into private, firewalled realms where groups of companies could use the tech to track assets and distribute an immutable record of their existence." But these blockchain ambitions have fallen dramatically short of expectations.

For instance, TradeLens, a blockchain system built by software firm IBM and closely linked to shipping giant Maersk, announced it was shutting down, citing a lack of commercial traction. Along the same lines, consider the Australian Securities Exchange (ASX) recent announcement that it was scrapping a much-delayed blockchain announced in 2016 that was meant to replace the clearing and settlement system that powers that equities market. ASX went so far as to proclaim that it will no longer attempt to rebuild its software platform with blockchain-based technology. In a revealing recorded conversation, Bloomberg reported that:

"Asked if the next attempt would "go down the more conventional route, that is without the focus on DLT (or) blockchain", exchange project director Tim Whiteley told the meeting that 'while we

continue to explore all the options, certainly we will need to use a more conventional technology than in the original solution in order to achieve the business outcomes.'"

The statement signals the end of what was to be one of the world's most prominent blockchain use cases, which was touted as a high-tech means to accelerate online transactions by processing them securely in multiple locations.

Similarly, it should also come as no surprise that Brisbane-based Everledger, which used blockchain technology to track the provenance of diamonds and other precious goods, has been quietly placed into voluntary administration after expected investor funding failed to happen. The move came despite it securing $57 million in backing, including from the federal government and Chinese internet giant Tencent. Founded in 2015, Everledger was one of the world's major companies pioneering blockchain-based platforms for tracking supply chains. These failures are not just significant -- they are the norm. As noted in a recent Forbes article:

"While the end of the business venture might seem insignificant anywhere but in the world of supply chain, the end of this joint venture is important for three reasons. Tradelens is the only successful deployment of Enterprise Blockchain in a public supply chain network, Maersk is backing away from building a utility to improve ocean shipping, and IBM is admitting failure in thought leadership in Enterprise Blockchain in the public sector. When it comes to Tradelens, Enterprise Blockchain as a technology worked, but the limited deployment vision was a death nail."

Indeed, going back to as early as 2009, enterprise blockchain was touted as a promising technology to improve collaboration "between trading partners that don't naturally collaborate but need to track compliance (e.g. labor usage, food safety, and climate data) in a safe and secure manner." But if mega tech companies like IBM and Maersk could not make blockchain work after years of trying and hundreds of millions of funding, who can? *And who is still even willing to try?* Blockchain is not just a technological failure – it has become an industrial relic.

As an aside, how on Earth were IBM and Maersk going to solve shipping problems by putting all the information on the blockchain. What shipping company wants their competitors to know how much they are shipping, what they are shipping, where they are shipping to and from, etc. – how could any company voluntarily opt to open themselves up to that sort of perilous transparency?

In fact, for all of blockchain's promise, blockchain promoters still consistently struggle to explain its practical applications. Take for example, when famed Andreessen Horowitz adviser Packy McCormick went on the tech podcast *Cartoon Avatars* and bumbled his way through explaining some sort of blockchain application for property purchasing, an oft touted aspirational blockchain use case. A clip of segment went viral on Twitter amid jeers, roasts and catcalls. Consider also AWS (Amazon Web Services), who looked hard and found no real practical use cases for blockchain where a database would have not worked. But since so much VC money was focused on blockchain: they built it because their customers paid for it.

As famed Amazon technologist Tim Bray explained regarding AWS and blockchain:

"We went looking around the industry from behind our screens and discovered a few things:

- Actual working business applications of blockchain were really, really hard to find.

- Plenty of blockchain products were on offer, characterized as "polished," "robust," "production-ready," and "regulator-approved." But if you looked hard at their customer stories, it got pretty vaporous pretty fast.

- The throughput of proof-of-waste blockchains was just as bad as we thought.

- In practice, the technology is a database. Everyone who did anything had some sort of a database structure mapped over the actual blockchain, with the usual B-trees and so on. It wasn't obvious how anything would be different if there were something other than a blockchain behind the B-trees.

- The Australian Stock Exchange was betting the farm on blockchain, which seemed to prove this was no joke.

- A huge, almost incomprehensible, volume of venture capital was flowing into the sector, and that money was localized in the Finance sector, specifically in Manhattan.

- AWS was already making a lot of money off blockchain.

All these venture-financed companies had to build out infrastructure, and most of them were all-in on cloud, either AWS or GCP (don't think Azure got much of that biz). So, there was a serious flow of cash from VC firms into AWS."

And believe it or not -- bogus blockchainification is still going on.

Blockchain and the California Department of Motor Vehicles

Recently, California's Department of Motor Vehicles (DMV) digitized 42 million car titles somehow using blockchain technology in a bid to detect fraud and smoothen the title transfer process. The project, reportedly in collaboration with tech company Oxhead Alpha on Avalanche blockchain, promises to allow California's more than 39 million residents to claim their vehicle titles through a mobile app, the first such move in the United States.

First off, the California DMV blockchain sounds like yet another private blockchain project (what level of insanity would make all DMV car titles public), so it is just another private database that will unfortunately run very poorly if at all and offer zero benefits over a regular database. It looks like yet another in a series of IT project that does not actually need "blockchain" but uses the term as marketing theater (at a cost of $46 million!).

Second, why not use a traditional database? An app (like the one I use with Geico and Chubb) displays my car's registration details, insurance, and even my driving licenses details. There's also a county website shows any driving or parking tickets. None of it requires "blockchain". This project is most probably using the typical SQL database at the backend to store actual data and there's an app front end. It sounds like someone built a *private* blockchain that functions as a *copy/replication* of the real DMV database that will ultimately rule the day.

Third, blockchain transactions are permanent. How is that helpful if a title is stolen, or transferred fraudulently, or illegally? What if a transaction contains sensitive or private information, or inappropriate language? What if the title holder moves – how can they change their address? The California DMV must have control in those situations – hence, bringing us back to the question, what does blockchain do in this circumstance?

Fourth, there are legal disputes that end with a title holder being forced to change their title – lawsuits, divorces, collections, and the list goes on. Unless the California DMV plans to shut itself down and let people transact cars peer to peer then it's all meaningless and unnecessary. Along the same lines, the intermediary of a judge, arbitrator or other decision maker is imperative to all of those situations.

Given the futility of blockchain asset tokenization, the perils of so-called smart contracts and the demands of California automobile owners, my take is that, in time, the DMV's blockchain project will crash and burn. Just like IBM's TradeLens, Microsoft's Azure Blockchain-as-a service and all the other blockchain dream projects of the past 18 years, DMV will quietly shut the project down and adopt instead a more powerful, more versatile, more robust, more secure and more practical Oracle solution

A Case Study: Blockchain and Ridesharing

Every time some shill touts some incredible futuristic application of blockchain, it takes five minutes of analysis to expose it as unrealistic, aspirational folly. Consider for example, the claim that blockchain will somehow revolutionize ride-sharing. Blockchain-based ride-sharing represents the typical blockchain puffery. Per a recent CoinTelegraph article which described the blockchain/ride-share process: "Ride request: When making a ride request, a passenger must include the pick-up and drop-off locations, the vehicle they need and the fare they are prepared to pay. This information is stored on the blockchain."

Wow, thanks blockchain for allowing the world to forever know precisely when someone is away from home and precisely where they'll be. Finally, a bona-fide and verifiable blockchain use case — except in this case the true utility is for murder, mayhem, rape, theft, robbery and so many other crimes.

Blockchain and ride-sharing is madness. What customer problem is being solved? This blockchain solution simply does what Uber does — but does it poorly and introduces horrendous risk, which, as has been meticulously explained by countless technologists, is pretty much the case every time blockchain is introduced into a product or service.

Here we have the usual example of blockchain hype and bluster, where blockchain is unnecessary, solves no problem and creates enormously dire consequences, in this case an ideal criminal use. Per its promotors, ride-sharing apps will someday utilize:

"Smart contracts and digital currency which will streamline payment processes, lower fraud risks and do away with the requirement for a central authority to oversee transactions – and

disputes between riders and drivers may be resolved through self-executing agreements and a decentralized arbitration process."

This is Alice in Wonderland incoherence. For instance, how is a "decentralized arbitration process" superior to logging on to your credit card account and disputing the charge? So-called smart contracts do not lower fraud risks, they increase fraud risks exponentially and lack any trustworthy means to manage disputes, problems, mistakes, etc. Ride-sharing is a classic example of blockchain manipulative groupthink, where a blockchain promotor:

1. *Finds a service that already works successfully;*

2. *Injects blockchain into the service and makes all sorts of unrealistic, misleading and downright silly aspirational claims about the service;*

3. *Instantaneously castes aside all privacy concerns while rendering the service significantly worse and even dangerous;*

4. *Adds a new and monstrous amount of risk into the process;*

5. *Pretends their blockchain high-tech solution will change the world, equalize and democratize situations and is the "next big thing;" and*

6. *Reaps huge profits down the line.*

Land registers on the blockchain follow the same exact pattern. Blockchain promoters love to weave thrilling tales of how "someday, all land registries that track titles for houses will be stored on some hypothetical public distributed digital ledger." Some even advocate that blockchain-based property registries may help lift poor people out of poverty. But does this mean that someone will suddenly own your house because they have some sort of cryptographic key?

Even more importantly, real estate transactions can be incredibly complex and convoluted, so what happens when a real estate transaction experiences a problem or snag? Will the parties run to their computers, click a few keystrokes, and somehow utilize blockchain to solve the conflict?

Hence, it is not surprising that no blockchain real estate application has become successful. Take Realux for example. Realux claimed that it was "focused on making real estate open or accessible to all consumers, at affordable costs in a very intuitive manner by using a system of digital tokens that were supposed to be backed by real estate investments." Realux made the usual promises to cure financial exclusion in real estate market, democratizing real estate investing and "that they aimed to address the wealth inequality problem by eliminating barriers, associated costs, intermediaries, social background, and various other restrictions."

The project's white paper promised to tokenize the real estate market, minting DLT-based tokens that represent the value of actual buildings. Once acquiring tokens, investors and traders were not real estate moguls. Realux supported their public relations campaign with hype from viral tweets and YouTube videos, published by influencers promoting the coin. But in February 2022

the project team dumped all their tokens, Realux completely disappeared -- with its social media accounts, website and Telegram channel all gone.

Many U.S. counties already use digital land registries built on SQL databases and most real estate closings can be done entirely virtually. Real estate transactions have never worked better and enabling the digitization of land records is an ideal objective well underway. But the digitization of land records is not the same as the tokenization of land records. Enabling digitization of records makes transactions easier but injecting blockchain into the process only serves to wreak havoc, create confusion and increase risk. And for what? There is no benefit except a buzzword – and perhaps some repressive profiteering by some blockchain carnival barker.

The Internet Had Its Skeptics Too (But Look at the Internet Now!)

Blockchain groupthinkers proclaim that new technologies always have skeptics, and that the same naysayers who deride blockchain are an identical reincarnation of the naysayers who derided the Internet in the early 1990s – and that those naysayers should be ignored.

This argument -- that the technological transformative capabilities of the Internet are somehow comparable to the technological transformative capabilities of blockchain -- is not just misleading, it is absurd. Yes, there may have been a few "Internet detractors" in the 1990s, but they were few and far between. Most people were too busy enjoying the Internet's clear and growing online benefits and excitement to have the time for "Internet skepticism."

From 1998-2009, I served as Chief of the SEC's Office of Internet Enforcement and before that, was for four years Special Counsel for Internet Projects in the SEC Division of Enforcement. During that time, I did not decry the Internet at all. In fact, I considered myself a promoter of it, an Internet Evangelist as many would recall.

Indeed, even if there were Internet detractors, no one paid them any mind because their arguments were so easily shut down and the technology was so clearly and so instantaneously revolutionary. Every company was piling on with Internet projects and development and people experienced the Internet's benefits on so many levels. The Internet's enthusiasm was incredibly exciting and promising – and exponentially infectious.

For instance, on May 25, 1995, then Microsoft CEO Bill Gates boldly wrote a memorandum to all Microsoft employees entitled, "The Internet Tidal Wave" stating:

> *"The Internet is a tidal wave. It changes the rules. It is an incredible opportunity as well as an incredible challenge. I have gone through several stages of increasing my views of the Internet's importance . . . Now I assign the internet the highest level of importance . . . I want to make clear that our focus on the Internet is crucial to every part of our business."*

The point of Gates's memo was that the Internet was fast becoming a ubiquitous force that was already changing the way people and businesses communicated with each other. Gates even appeared on the David Letterman show to broadcast his message of Internet growth and

possibilities. With the Internet -- just like with other breakthrough technologies like the cloud and the iPhone -- everyone could easily envision the Internet's infinite promise.

The Futility of Blockchain Asset Tokenization

As Professor Kelvin Lowe noted about the ASX blockchain debacle:

"The only thing the blockchain accelerates is simpleton syndrome where every complex problem is grossly oversimplified so that a blockchain is its solution. ASX learnt this the hard way. How many others will have to do so for themselves?"

In other words, it may be possible for some trusted, well governed third party operate a blockchain as an "enterprise blockchain" or "permissioned blockchain" but why? All that creates is a very poor, slow, difficult to manage database. As Professor Kelvin Low recently added presciently in his blockchain exposé titled: "The (F)utility of Blockchain Asset Tokenization:"

"It bears repeating that we have passed the 14th anniversary of Satoshi Nakamoto's white paper and while the blockchain has promised much, it has delivered little unless we are looking for frauds and scams and consumer harm. It is past time to take blockchain skepticism seriously."

For example, blockchain promoters have long touted the revolutionary impact of blockchain to better harmonize cross border, cross currency transactions. But blockchain is not necessary as the backend for supporting instant remittances across currency zones. Indeed, as SWIFT has already demonstrated, all that's necessary is a database. Specifically, SWIFT has piloted instant cross border payments, and no, they did not need or use blockchain. Just a plain old database.

Payment speeds are never limited by technology. We can do payments as quickly as correspondent banks can swap numbers in a relational database, which is nanoseconds.

Despite the fierce tides of blockchain groupthink, blockchain, the core of web3 promotion is not just bunk, it has also evolved into a dangerous swindle. As famed technologist and chief scientist for software engineering at IBM Research Grady Brooch, said so eloquently in a *recent InfoWorld interview:*

"Web3 is a flaming pile of feces orbiting a giant dripping hairball. Cryptocurrencies—ones not backed by the full faith and credit of stable nation states—have only a few meaningful use cases, particularly if you are a corrupt dictator of a nation with a broken economic system, or a fraud and scammer who wants to grow their wealth at the expense of greater fools. I was one of the original signatories of a letter to Congress in 2022 for a very good reason: these technologies are inherently dangerous, they are architecturally flawed, and they introduce an attack surface that threatens economies."

A Blockchain Due Diligence Primer

To avoid blockchain groupthink, when evaluating the use of blockchain technology, the following five simple due diligence lessons apply:

- **Don't Follow the Horde**. Instead, seek expert, objective and independent sources. Unfortunately, in today's world, there exists a glaring lack of objectivity concerning blockchain and other Web3 nonsense. Too much information is being spread by those who are biased, and too many digital investment products are being peddled by those who lack independence. In fact, most of those shilling blockchain and Web3 elixir are promoters, marketers and other hired hands, who are heavily invested in the very same blockchain and Web3 products that they insist on touting as the next big thing.

- **If You Don't Get It, Don't Get It**. Don't' be deterred by the Big Crypto playbook's typical retorts of: *"You just don't get it*." "*You need to get educated*." "Y*ou need to do the research." "OK Boomer." And the list goes on.* When all other arguments fail, crypto enthusiasts, blockchain advocates, DeFi evangelists and the many Web3 true-believers will too often pivot to this kind of clever *Emperor's New Clothes* modus operandi. The hope is that we will all become too afraid to admit that there is nothing to get. Thankfully, there now exists a growing anthology of objective, unbiassed, contemplative and evenhanded thought leadership relating to Web3, including blockchain, cryptocurrency, non-fungible tokens (NFTs), decentralized finance (DeFi) and all other things fintech (whatever the term "fintech" actually means). Find neutral, impartial and nonpartisan analysis that: 1) Educates and informs about Web3's emerging prominence and hype; and 2) prepares and primes individuals and their companies to ask the right questions and better understand the litany of evolving labyrinthian hazards and threats created by cryptocurrency, decentralized finance, digital trading platforms, non- fungible tokens and the litany of other Web3 digital products and services.

- **What If It All Vanished Tomorrow**. Cut through the cognitive dissonance and chaotic noise of blockchain promotors and charlatans by asking anyone who promotes blockchain to explain in easy terms to understand exactly how blockchain benefits anyone in their daily lives. And bear in mind that complexity, opaqueness and aspirational hype is not a sign of sophistication -- it's a glaring red flag. If blockchain vanished tomorrow, would anyone other than Blockchain investors really care? Or even know? If the Cloud suddenly shut down, if the Internet suddenly shut down or if iPhone's all suddenly down, chaos would ensue. But if blockchain suddenly shut down? Nothing would change for anyone.

- **Show Me the Money**. Ask this question of any neutral, objective and independent technologist: "If blockchain disappeared tomorrow, would anyone even notice? Would anyone even care?" The answer will inevitably be a resounding and definitive "No." The truth is that beyond being a rather awkward, arguably antiquated and extremely inefficient kind of database technology and beyond providing the underlying technology for criminals to use crypto pseudonymously to commit crimes, blockchain is not just remarkably unremarkable, blockchain also makes products and services worse.

- **Avoid the Conflation Rabbit Hole**. There exists a lot of confusion about what blockchain actually is – which not only creates misconceptions but offers ideal opportunities to trumpet blockchain as a revolutionary buzzword triggering a massive, global financial sea-change. Along these lines, there has evolved a cadre of blockchain

enthusiasts who claim they are *anti-crypto, but pro-blockchain*. This logic fails completely. Simply stated, there cannot exist a public blockchain without a crypto token. The crypto provides the incentive for the public blockchain's creation. Miners are rewarded in crypto for creating the public blockchain. Public blockchains are permissionless, allowing anyone to join the network and participate in the blockchain.

Thus, without any reward, there is no enticement to build a blockchain. In other words, without crypto as part of a public blockchain, there is no one to perform the necessary proof of work. Private blockchains, on the other hand lack decentralization and are invitation-only networks run by a single organization.

"It's a Spreadsheet, John!"

I once mentioned the lack of utility of any blockchain application to a senior engineer friend of mine at a big tech firm and the problems of blockchain groupthink – and he quickly snapped back: *"John, blockchain is a spreadsheet, that's it. Nothing more. How on Earth is a spreadsheet going to change the world??!!"*

Thankfully, objective sources like my friend are ubiquitous and easily accessible to anyone. One need only look around. Along these lines, due diligence regarding blockchain seems to have gone askew. Drilling down into companies, pouring over financial statements and digging into the people, products and services of a possible investment opportunity too often takes a back seat to the answer to two simple questions:

- *Can this company's blockchain pitch generate enough buzz and hype to convince investors that it is the next big thing? and*

- *Can our legion of shills manipulate the company's blockchain buzz and hype to rapidly inflate the company's enterprise value exponentially, so we can sell it all for a quick and gargantuan profit of 10x or more?*

Sadly, these high-tech robber barons and their cohorts may as well be bankrolling heroin plants or blood diamond mines. It's all about short term profits that can boost personal cash flow.

Of course, everyone wants to get ahead, make better lives for family and friends. That's how capitalism works. And unless there is fraud, it is all more or less lawful.

But the bulk of Big Crypto profiteers, including so many self-proclaimed "fintech" lawyers, have evolved into nothing more than high-tech carnival barkers, the likes of which we have seen before, who greedily line their own pockets at the expense of everyday investors, leaving only economic devastation in their wake.

Just consider blockchain from a commonsense perspective. Historical technological game changers from fax machines to the Internet to the iPhone to the cloud and to artificial intelligence, all have one notion in common: upon their invention, it was easy to immediately envision the revolutionary and exciting prospects ahead. But with blockchain, not so much. Just

ask anyone (on the street or in a corporate office) how blockchain is going to make their lives better and the answer will undoubtedly be: *"I have no idea."*

And don't get fleeced into believing that *"Well, if Wall Street is using blockchain, blockchain must be an ideal investment to get rich quick."* This is how menacing crypto-promoters exploit blockchain antics with groupthink toxicity and crypto-sophistry. Clearly, the success of crypto, blockchain or any other web3 iteration will not stem from private, permissioned blockchains used to settle bond placements by huge, multinational investment banks.

Along the same lines, the notion that, *"Hey those guys from Shark Tank are smart, so I'll invest"* is precisely the kind of groupthink that blockchain, crypto, DeFi and other Web3 promoters coopt as part of their chicanery. Indeed, the perils of blockchain-groupthink have already resulted in dire investor carnage. Consider the millions of investors who relied on Kevin O'Leary (and lost their life savings by trusting now bankrupt FTX) or who relied on Mark Cuban (and lost their life savings by trusting now bankrupt Voyager).

Just because some big bank or flexing billionaire seems to be using a private blockchain internally for a project that sounds exciting and forward-thinking, does not mean it's time to jump on the blockchain bandwagon.

From where I sit, the vast, if not overwhelming, number of current blockchain projects are "private blockchain" projects which are not open to the public, not decentralized, not permissionless, not technologically transformative, not futuristic (but are instead antiquated) and cannot perform any better than a Google Docs spreadsheet.

The Stark reality is that the whole concept of private blockchain is an oxymoron and can be easily replaced by a more efficient database. Blockchain remains, and will likely forever be, a useless, shoddy, inefficient database scheme and is not remotely close to becoming any sort of technological panacea. Ironically, blockchain's only practical use seems to be for con artists who tout blockchain to scam investors.

FINAL THOUGHTS

Right now, Congress and the SEC are considering an epic securities regulation overhaul – and I still cannot understand why. After 16 years, so called crypto-innovations have provided little, if any, financial market or other societal benefit while creating horrific externalities and colossal global financial systemic risk. As securities compliance expert and former Compliance Week editor Matt Kelly commented recently:

> *"Every day in every way, crypto demonstrates that it has no useful purpose other than fraud, tax evasion, and corruption. Otherwise, it's just a speculation toy for billionaires and a sucker's bet for everyone else."*

Along the same lines, famed economist Paul Krugman recently wrote in an op-ed in the New York Times:

"In the years since Bitcoin was introduced, digital payment systems that skip the hocus-pocus, like Venmo and Apple Pay, have become ubiquitous. But for most of us, crypto assets have few uses other than the purchase of other crypto assets; notable exceptions are money laundering, extortion and scams."

Even more importantly, there is nothing about the cryptoverse that suggests that digital asset investors are less deserving of the protections of U.S. securities laws or the need for a new framework. Indeed, in a remarkably short period of time, judicial precedent pertaining to digital assets has grown considerably and there now exist dozens of federal decisions on the books proclaiming that whatever their iteration, digital assets are securities and trigger SEC jurisdiction and enforcement.

Above all else, the SEC and its Crypto Task Force does not have, nor should it have, the ability to unilaterally repeal the *sine qua non* of the '33 Act, '34 Act and '40 Act; yet the SEC seems to be doing just that.

While crypto-advocates may not like the outcome of the litany of crypto-related judicial decisions discussed and cited herein, that does not amount to an absence of clarity, Due Process or Fair Notice. It just means that the digital asset industry needs to get its act together and adapt to the laws that apply to it — not the other way around.

Lone Democratic SEC Commissioner Caroline Crenshaw has acerbically ridiculed the new SEC crypto-posture as "regulation by non-enforcement, while Bruce Carton of Securities Docket has branded the SEC's radical crypto-turnabout a "Reverse-Sweep." SEC Sweeps once meant that the SEC had opened a cascade of investigations and filed a barrage of litigation targeting a specific industry or a specific business practice. In glaring contrast to those successful SEC sweeps of yesteryear, an "SEC Reverse Sweep" is the rapid-fire SEC dismissal of SEC - cases and seriatim closing of SEC crypto-related investigations and withdrawals of SEC crypto-related appeals.

Whatever the new slogan or nomenclature, the SEC's comprehensive and indiscriminate dismantling of its crypto-enforcement program is not just unprecedented and irresponsible -- its regulatory heresy.

For example, the SEC Division of Corporation Finance just issued guidance on meme coins saying they are NOT securities but are akin to some sort of entertaining collectable. Aside from the fact that the technological innovation and mammoth utility of crypto assets never ceases to amaze, isn't the SEC guidance precisely the kind of bureaucratic law-making that President Trump has promised to jettison? Consider the extraordinary irony of this latest "Meme Coin SEC Proclamation" – it's *SEC Regulation by Corporation Finance of SEC Regulation by Enforcement*.

Don't get me wrong. The SEC is far from perfect. But on balance, the SEC is an extraordinarily successful regulatory agency and by enforcing its effective, proven and evolving principles-based U.S. securities law framework -- be it in the cryptoverse or elsewhere -- the SEC has not gone rogue. The SEC is simply doing its job to protect not just investors but everyone,

everywhere – because when companies violate the securities laws, it is not merely investors who suffer losses, all global capital markets are at risk.

The Stark reality is that when it all hits the fan in the cryptoverse, *ask not for whom the bell tolls, it tolls for thee.* So, fail not at your peril SEC Crypto Task Force, the SEC's abdication and renunciation of its once sacrosanct investor protection mandate could both sound the death knell for a once proud, storied and vital financial watchdog, and could also propel the SEC to become the most culpable crypto-grifter of them all.