On Establishing Cryptocurrencies as Securities

Jake Ginesin

1 Introduction

Cryptocurrencies, loosely defined as digital currencies operating over a computer network, have seen exponential growth in recent years, driven in part by technical innovation, speculation, and the (rather ideological) promise of a decentralized financial system. The rapid technological development of cryptocurrencies, alongside the advent of the modern cryptocurrency industry, has presented today's governments and regulatory agencies with several unique challenges. How should digital currencies be regulated and managed? How should the associated cryptocurrency industry be moderated? Central to the evolving regulatory landscape is the question of the *digital currency classification*: should cryptocurrencies by regulated as securities, commodities, currencies, or something entirely different?

Until very recently the space has gone essentially without regulation, leading to disastrous consequences for the average investor. It is almost comical counting the instances of fraud and market manipulation in the cryptocurrency industry; the notorious website, web3isgoinggreat.com, counts 78.304 billion dollars lost to hacks and scams [1]. Notable disasters include the FTX exchange collapse [2] and the Binance money laundering scandal [3]. Many of the recent cases of cryptocurrency scams and fraud mirror historical cases of securities fraud, such as Enron's collapse [4] and Stratton Oakmont's notorious pump-and-dumps with small-cap IPOs [5]. However, the Securities and Exchange Commission generally lacks the authoritative capability to more tightly tie down the cryptocurrency industry.

This is in-part due to SEC v. Ripple [6], SEC's legislative attempt to charge Ripple - the company behind the XRP cryptocurrency - with securities fraud, thereby implicitly seeking to set the precedent that cryptocurrencies can be regulated as securities. The court ruled in favor of Ripple, declaring XRP is "not necessarily a security." The SEC filed a further appeal, which was later dropped. Following a recent presidential executive order on the third day of Donald Trump's presidency, "Strengthening American Leadership In Digital Financial Technology," the SEC in-tow established the Crypto Task Force with the goal to better regulate the crypto industry [7]. The Crypto Task Force is actively holding public "roundtables" with panelists from academia, industry, and government[1]. As an alternative to presenting a case at the in-person roundtable, this essay may serve as a possible argument presented at the public roundtable.

In short, we advocate for the establishment of cryptocurrencies of a certain caliber as financial securities, given two criteria are met. First, the cryptocurrency but be sufficiently *centralized*; that is, one person or organization has authority to control the blockchain (i.e. the cryptocurrency's transaction history), or controls 20% or more of the digital asset. Second, the cryptocurrency must have a sufficiently high market cap to be considered a financial security. The exact value is up for debate (perhaps, around 50 million). Legislatively, there are two viable paths for the establishment of cryptocurrencies as a security. SEC v.

[1]For more information, please see the link: www.sec.gov/about/crypto-task-force/crypto-task-force-roundtables

Ripple can be overturned by a future court decision, or congress can pass legislation explicitly establishing cryptocurrencies as securities.

The following proposal will be structured as follows. First, we will introduce the respective background on cryptocurrencies, Ripple Labs, and XRP, thereby motivating the need for more stringent cryptocurrency legislation. Then, we will provide background on the SEC v. Ripple case, as well as detail the other pieces of relevant legislation. Then, we will discuss the details of our policy proposal and its feasibility in the current political climate.

2 Technical Background

In this section we establish the relevant technical background on cryptocurrencies, as well as describe the relevant background on Ripple and XRP.

2.1 Background On Cryptocurrencies

As previously mentioned, cryptocurrencies are loosely defined as digital currencies that operate over a computer network. In particular, the historically large cryptocurrencies (i.e. Bitcoin & Ethereum) are designed to be both *decentralized* and *byzantine fault-tolerant*. While there certainly exists more technical definitions, we (somewhat loosely) define a decentralized network to be a network in which no one central authority manages the network state (that is, a critical mass of peers must *agree* on any one action), and we define a byzantine fault-tolerant network to be a network that can tolerate some fraction of evil (byzantine) users. In the case of cryptocurrencies, a *shared transaction history*, or a blockchain, is continually agreed upon, in a decentralized and byzantine fault-tolerant way.

While cryptocurrencies have a lengthy technical history, from e-cash to digicash to hashcash [8], they mostly remained as purely cryptographic research projects and never received any serious public attention nor legislative scrutiny. That was, until 2009, when the famous paper "Bitcoin: A Peer-to-Peer Electronic Cash System" was published under the pseudonym Satoshi Nakamoto, combining *proof-of-work* (i.e. reversing a computationally hard one-way function) with continual byzantine agreement to create the first modern blockchain system [9]. While the communities surrounding byzantine systems and digital currencies has always been somewhat *libertarian* in nature, the Bitcoin paper quite blatantly opens with the quote:

> "A purely peer-to-peer version of electronic cash [referencing hashcash [8]] would allow online payments to be sent directly from one party to another without going through a financial institution."

Besides this quote, several other stabs are made at centralized financial institutions throughout the paper.

Since the advent of its first real-world implementation and deployment in 2009, Bitcoin has experienced remarkable growth, reaching a market cap of 1.69T as of April 2025. Several countries, namely the USA, thus hold "strategic" Bitcoin reserves [10]. Additionally, distributed and cryptographic systems have continued to evolve, allowing for entirely distributed, verifiable, trustless, *general* computation at scale [11, 12].

Despite massive growth and the continual rise in societal importance of cryptocurrencies, no effectively legislative framework regulating the space has been successfully implemented. This is in-part due to the

fundamental difficulty of regulating any distributed system that is sufficiently distributed and byzantine. Evidently, this makes protecting against crimes at the individual level, such as theft, extremely challenging.

In particular, we acknowledge the technical infeasibility of tracing cryptocurrency transactions *in general*, and thus the infeasibility of more fine-grained legislation reasoning about any one individual cryptocurrency transaction. Standard currencies feature unique serial numbers on physical bills, and financial institutions meticulously log transactions, allowing for governments to enforce, for example, effective anti-ransom legislation. We observe such tracing features are provably infeasible with several cryptocurrencies. Monero, for example, employs a battery of protocols (bulletproofs) to obfuscate transaction values and transaction participants, while still letting individuals privately verify transactions against the public ledger [13, 14]. Furthermore, infrastructure exists to anonymously and verifiably exchange Monero with other cryptocurrencies (i.e. Bitcoin, USDT) without relying on one central institution, broadly labeled as "(pooled) atomic swaps" [15]. To hammer this point home, the US treasury department has issued several contracts to private companies to attempt to trace Monero transactions [16], presumably to no avail.

Thus, to frame the *angle* of our legislation proposal, we acknowledge the fundamental technical difficulties presented by cryptocurrencies and thus seek to instead regulate how established institutions and organizations manage, control, and manipulate cryptocurrencies. To do so, we seek to empower government organizations with the authority to successfully regulate organizations that misuse cryptocurrencies.

2.2 Background on Ripple Labs and XRP

Ripple Labs is an American company founded in 2012 that seeks to employ cryptocurrencies for various financial services, including cross-border payments with fast settlement times, on-demand liquidity, and secure asset custody services. To do so, Ripple Labs employs the XRP Ledger (occasionally called the *Ripple Protocol*), a cryptocurrency platform that is *claimed* to be independent from Ripple Labs. The goal of this section is two-fold: first, we seek to provide the technical background on XRP and the institutional background on Ripple Labs; second, we seek to motivate our legislative proposal by presenting the *fundamental* flaws presenting in XRP and Ripple Labs. To do so, we will first describe in-detail the XRP protocol and its fundamental flaws, then we will describe the fundamental flaws in Ripple Labs.

2.2.1 The XRP Ledger and Its Flaws

As of December 2024, XRP has the third largest market cap at just over 150 billion dollars, and as aforementioned XRP is actively employed by *Ripple Labs*. The Ripple consensus protocol is *fundamentally different* than other consensus algorithms employed by other cryptocurrencies. Ripple consensus does not use Proof-of-Work or Proof-of-Stake for agreeing on new transaction proposals; rather, Ripple consensus uses a modified Byzantine consensus algorithm that does *not* rely on reversing a computationally hard one-way function. Instead, Ripple consensus is conducted peer-to-peer through a set of validators. To achieve consensus in a Byzantine setting, the Ripple consensus protocol has two main features:

- **Unit Node Lists (UNLs)**. Each Ripple consensus validator pre-declares a list of trusted validators; for a validator to accept a proposal, it only requires consensus between its trusted validators.
- **UNL overlap**. Different UNLs are *assumed* to have overlap. The existing literature on Ripple consensus has disagreed on the amount of UNL overlap required for consensus in the Byzantine setting.

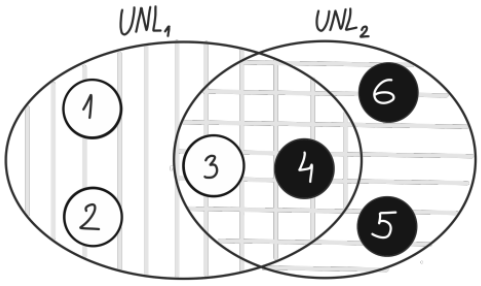

Figure 1: Visualization of a Ripple network configuration, taken from [17]. This network configuration features two UNLs: $\mathsf{UNL}_1 = \{1, 2, 3, 4\}, \mathsf{UNL}_2 = \{3, 4, 5, 6\}$. Notice, validators 3 and 4 have the most influence, as they are in the intersection of both UNLs.

For a full description of the Ripple protocol, please refer to [18].

Provably Insecure Design. The first major flaw of XRP is the *provable insecurity* of its high-level design. The standard in modern distributed systems is to mathematically *prove* a protocol demonstrates various desired performance and stability guarantees[2]. This was supposedly done for Ripple – non-peer-reviewed "proofs" of relevant security properties for Ripple consensus were posted to a pre-print server in 2018 by Brad Chase and Ethan MacBrough, two members of Ripple Labs [17]. However, in 2020, cryptographers from the University of Bern published a peer-reviewed paper demonstrating that Ripple Consensus does *not* maintain the design-level security guarantees claimed by Chase and MacBrough [20]. Namely, Ripple Consensus's guarantees fundamentally break down if (1) there is any delay in the network (i.e. the network is not *synchronous*), (2) there is UNL overlap under 90%, or (3) if there is a well-placed Byzantine node. A visualization of a hypothetical attack presented by [20] on the third scenario, causing different UNLs to agree on different proposals (i.e. "split-brained behavior", is visualized in Figure 2.

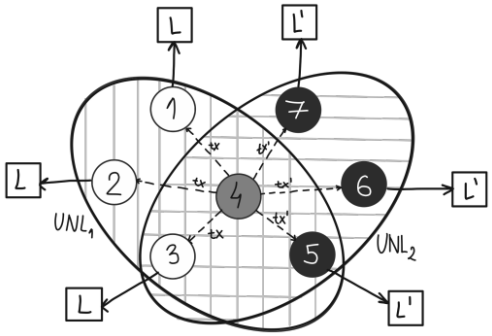

Figure 2: Visualization of an attack on the Ripple consensus protocol, taken from [18]. White nodes adopt one UNL (L), black nodes adopt another (L'), and the grey node is Byzantine. The Byzantine node exhibits split-brained behavior, selectively sending different consensus communications ($\mathrm{tx}, \mathrm{tx}'$), ensuring UNL_1 and UNL_2 agree on different proposals.

The conclusion of design-level provable insecurity of the Ripple consensus protocol was later handsomely reproduced with computer-aided proofs by Ginesin and Zhu in 2024 [21]. However, despite the demon-

[2]We do not seek to get into the specific distributed systems guarantees practitioners seek to reason about and prove within the scope of this work; for more details on distributed systems properties of interest, please see [19].

stration of XRP's *provable*, *verifiable* insecurity, there was no response from Ripple Labs, and virtually no discussion online outside of academic circles This is highly unusual, as major flaws in major open-source projects of public importance historically generate lots of discussion online – when similar vulnerabilities in the open-source secure messaging protocol Matrix were discovered [22], ample discussion was triggered[3].

Unusually Small Network Participation. we observe that in practice, Ripple consensus validators are *highly centralized*. The main validators for Ripple consensus are apart of just one UNL, "dUNL" (standing for, "default" UNL). Additionally, as of December 2024, Ripple consensus has *just 110* validators active on the network and *just 66* on the latest version, as shown in Figure 3. This is in stark comparison to Bitcoin and Ethereum, which has 21728 nodes and 7033 nodes respectively as of April 2025 (according to network scanners bitnode.io and etherscan.io respectively).

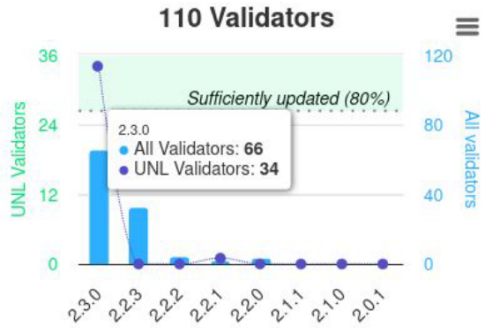

Figure 3: Screenshot from xrpscan.org, a website which tracks the current number of validators on the Ripple network.

2.2.2 Ripple Labs and Its Flaws

Ripple Labs, the aforementioned financial technology company behind XRP, exhibits a number of structural, financial, and ethical flaws that strongly motivate tighter regulatory oversight.

Unambiguous Centralization. As of December 2024, Ripple Labs owns approximately **50%** of all XRP in circulation [23]. This entirely undermines any claim of decentralization and qualifies Ripple as a de facto central authority over the asset. Despite public-facing claims that the XRP Ledger is "independent," Ripple controls the monetary supply and effectively the validator set, as the default UNL, the only active UNL for verifying transactions, is maintained and endorsed by Ripple Labs. Naturally, many of the founders have cashed out, selling their initial stakes in XRP for massive profits[4].

Opaque Revenue Sources. Ripple reports extremely small profits from transaction fees on its financial products — only $530,000 in 2023 [24]. This is incredibly small in comparison to Ripple's 11 billion-dollar valuation according to its 2019 series C. For comparison, Ripple's revenue-to-profit ratio is ~20750x, while Nvidia's (for example) is ~37 as of April 2024. The bulk of Ripple's income stems from "strategic" XRP sales. Ripple launders "sells" XRP to several Asian companies, of which all are partially owned by Ripple themselves [24]. Effectively, Ripple has created an international subsidiary structure that allows it to buy

[3]Principal of which can be found in the associated Hacker News thread: news.ycombinator.com/item?id=33930776

[4]One such case: ripple.com/insights/the-stand-is-finally-out-of-tacos/. Other instances of sell-offs include Larson who sold $450 million of XRP between 2015 and 2025, and Garlinghouse who sold $150 million of XRP between 2017 and 2019.

and sell XRP as it pleases. This raises just incredible concerns about corporate transparency and investor misrepresentation.

Political Spending and Legal Obstruction. Ripple Labs has spent over $100 million of its $250 million in seed funding litigating against the SEC [25] in the SEC v. Ripple case. Additionally, Ripple Labs founded Fairshake, a superPAC whose goal is to push "crypto-friendly" legislation, and funneled $45 million into it. Fairshake has went on to be extremely successful in electing candidates of interest, with 33 of 35 of its backed candidates going on to win their respective elections [26]. Evidently, this is not just defensive lobbying; it is an aggressive financial campaign to suppress regulatory oversight through sheer capital power.

2.2.3 Discussion

The evidence is damning: Ripple Labs and XRP are fundamentally flawed. And yet, Ripple Labs still employs thousands of people, XRP has a high market cap and remains actively traded, and public confidence in Ripple & XRP remains high. How long can this possibly last? It is important to emphasize that, through XRP's technical incompetence and Ripple Labs' institutional mismanagement, it is the average investor in XRP who suffers. We as a society have learned these lessons before through countless historical cases of securities fraud and market manipulation. We believe it is only proper that legislative infrastructure is put into place to not only reel in Ripple, but to set a precedent for a clean, fair digital economy.

3 Legislative Background

The legislative conversation around regulating Ripple and cryptocurrencies at large hinges on two major events: the lawsuit *SEC v. Ripple*, and the broader policy context following the Dodd-Frank Act.

SEC v. Ripple. The Securities and Exchange Commission (SEC) filed a lawsuit against Ripple Labs in 2020, alleging that Ripple's Sale of XRP constituted an unregistered securities offering. To quote the SEC's press release [27]:

> "Issuers seeking the benefits of a public offering, including access to retail investors, broad distribution and a secondary trading market, must comply with the federal securities laws that require registration of offerings unless an exemption from registration applies. We allege that Ripple, Larsen, and Garlinghouse failed to register their ongoing offer and sale of billions of XRP to retail investors, which deprived potential purchasers of adequate disclosures about XRP and Ripple's business and other important long-standing protections that are fundamental to our robust public market system."
> — Stephanie Avakian, the director of the SEC's Enforcement Division

The core of the lawsuit centered on Ripple's "Institutional Sales," which involved $728 million in XRP sold "directly to certain counterparties (primarily institutional buyers, hedge funds, and ODL customers) pursuant to written contract." The SEC further argued that Ripple's long-standing market practices implied XRP was an investment contract, thereby satisfying the Howey Test.

> The **Howey Test** determines whether an instrument qualifies as an "investment contract" for the purposes of the Securities Act of 1933: "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party" [28]

Ripple pushed back by insisting that XRP was a "digital token," not a security, and thus not subject to the same disclosure or registration rules. This yielded a mixed result:

> "XRP, as a digital token, is not in and of itself a "contract, transaction[,] or scheme"" that embodies the Howey requirements of an investment contract. Rather, the Court examines the totality of circumstances surrounding Defendants' different transactions and schemes involving the sale and distribution of XRP."
> — SEC v. Ripple

And thus, ruling that XRP is "not necessarily a security," the case concluded:

> "For the foregoing reasons, the SEC's motion for summary judgment [that XRP is classified as security] is GRANTED as to the Institutional Sales, and otherwise DENIED. Defendants' motion for summary judgment is GRANTED as to the Programmatic Sales, the Other Distributions, and Larsen's and Garlinghouse's sales, and DENIED as to the Institutional Sales"
> — SEC v. Ripple

The SEC attempted to appeal this partial loss, but the appeal was dropped in 2025. Ripple and the crypto industry celebrated the outcome, with the Ripple Labs CEO remarking, "There were no victims, there was no investor loss. They were just not acting in good faith." Ripple agreed to pay a $50 million fine, effectively closing the case [29]. As it stands, SEC v. Ripple sets the precedent that cryptocurrencies, even if centralized, are not to be classified as securities.

Proposed Policy. The most notable piece of *proposed* policy is the "Financial Innovation and Technology for the 21st Century Act" introduced to congress in late 2024 [30]. This act, in summary, was to step over SEC v. Ripple and to establish *centralized, functional* cryptocurrencies as securities to be regulated by the SEC (to some definition of "centralized", and to establish *decentralized, functional* cryptocurrencies as commodities to be regulated by the CFTC. This bill takes precedent from the Dodd-Frank Act of 2011, which established derivatives as financial securities [31], and has so far passed in the House of Representatives in 2024. However, no further movement on this piece of legislation has occurred since the advent of the second Trump administration.

Other Relevant Policy. There are several other pieces of legislation that dictate, in general, how securities, commodities, and financial institutions behave. The Securities Act of 1933 and the Securities Exchange Act of 1934 defines the legislative notion of a security and establishes the legal framework surrounding them. Similarly, the Commodity Exchange Act (CEA) of 1936 and its subsequent amendments, gives the Commodity Futures Trading Commission (CFTC) authority over commodity derivatives markets and certain spot market activities. The CEA's definition of "commodity" is broad, and encompasses all "services, rights, and interests." Additionally, the Bank Secrecy Act of 1970 requires financial institutions to assist government agencies in detecting and preventing money laundering crimes.

4 Policy Proposal

The primary aim of this proposal is straightforward: cryptocurrencies of significant caliber must be regulated explicitly as financial securities. This classification is paramount to curbing the rampant fraud, manipulation, and institutional mismanagement exemplified by Ripple Labs, coupled with the technical mismanagement of XRP. To achieve this objective, we advocate a legislative and judicial dual-track approach: overturning the precedent set by *SEC v. Ripple* or explicitly establishing through congressional

legislation that certain classes of cryptocurrencies fall under the definition of securities.

Our proposal seeks to establish two concrete criteria for classifying a cryptocurrency as a financial security:

1. The cryptocurrency must possess a sufficiently high market cap. While the exact threshold is debatable, a market capitalization of approximately fifty million dollars serves as a reasonable starting point. This criterion ensures only assets with substantial economic significance fall under securities regulation.
2. The cryptocurrency must demonstrate clear centralization. Specifically, a single institution or individual must either (1) control at least 25% of the cryptocurrency's circulating supply, or (2) exercise significant control over the cryptocurrency's transaction validation mechanism (i.e., mining or validator sets).

These thresholds directly target entities like Ripple Labs, which, as noted, controls nearly 50% of XRP and maintains substantial influence over its validator nodes. Classifying XRP and similarly structured cryptocurrencies as financial securities would subject Ripple to the Securities Act of 1933, and the Securities Exchange Act of 1934, allowing the SEC to enforce rigorous disclosure requirements, anti-manipulation safeguards, and investor protection mandates. In the motivating case of Ripple Labs, classifying XRP as a security would allow further SEC scrutinization, potentially addressing Ripple's current practices by:

- **Enhancing Transparency**: Mandating detailed financial disclosures on XRP holdings, internal trading activities, and revenue sources, thereby preventing covert revenue schemes such as Ripple's international XRP laundering.
- **Prohibiting Market Manipulation**: Applying stringent market integrity rules analogous to those governing traditional securities markets, thus preventing Ripple from leveraging its dominant position to manipulate XRP's market price.
- **Ensuring Investor Protection**: Enforcing fiduciary responsibilities, preventing Ripple from misrepresenting the independence and security of XRP, and requiring accurate risk disclosures to investors.

Similarly, stipulating that cryptocurrencies must surpass a certain market cap threshold serves to protect upcoming-and-coming experimental cryptocurrencies from further regulation and scrutiny.

An alternative legislative avenue involves revisiting and enacting policies similar to the proposed "Financial Innovation and Technology for the 21st Century Act," which differentiates cryptocurrencies as either commodities or securities based on their centralization. Our proposal aligns closely with the decentralization argument presented in the aforementioned act, advocating that decentralized cryptocurrencies continue to be regulated as commodities by the CFTC, whereas highly centralized cryptocurrencies fall explicitly under the SEC's purview as financial securities. Similarly, our legislative proposal would follow in-precedent with the Dodd-Frank act that congress can explicitly establish certain asset classes as securities.

Potential Pushback. Currently, there exists significant obstacles that stand in the way of enacting this proposal. Evidently, Ripple Labs and the broader cryptocurrency industry have demonstrated formidable lobbying power via its formation of the superPAC "Fairshake" and its record of successful political influence. Moreover, the political environment introduced by the recent Trump administration is markedly

anti-regulatory and very openly pro-crypto. Donald and Melena Trump endorsed "meme" coins[5] just before Trump took office; the price of both coins crashed a few days after launch "rug-pulled," enriching the initial owners via trading fees and causing significant losses for early investors. Evidently, the current President endorsing a pump-and-dump crypto scheme – literal securities fraud, if cryptocurrencies were to be classified as securities – does not necessarily spell good news for this proposal[6]. Additionally, the establishment of the Crypto Task Force under this administration, although nominally aimed at enhancing American digital financial leadership, may complicate efforts toward stringent cryptocurrency regulation.

Thus, in order to enact this proposal and establish cryptocurrencies (under the aforementioned criteria) as securities, securing bipartisan congressional support, overcoming aggressive lobbying efforts, and shifting the public and political narrative toward recognizing the necessity of financial accountability in cryptocurrency markets will be imperative.

5 Conclusion

Motivated in-part by Ripple's centralized control of XRP, the technical unsoundness of Ripple Consensus, and Ripple Labs' opaque financial practices, our proposal offers a concrete, criteria-based framework for classifying certain cryptocurrencies as securities. Legislative or judicial adoption of this framework is essential to curb systemic abuse, enforce accountability, and protect investors in increasingly influential digital markets.

References

[1] M. White, "Web3 is going just great," Apr. 2025. [Online]. Available: https://web3isgoinggreat.com/

[2] D. Yaffe-Bellany, M. Goldstein, and J. E. Moreno, "Sam Bankman-Fried Is Found Guilty of 7 Counts of Fraud and Conspiracy," *The New York Times*, Nov. 2023. [Online]. Available: https://www.nytimes.com/2023/11/02/technology/sam-bankman-fried-fraud-trial-ftx.html

[3] "Binance and CEO Plead Guilty to Federal Charges in 4 billion dollar Resolution," Nov. 2023. [Online]. Available: https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution

[4] New York Times. (2007) Enron shareholders look to sec for support in court. [Online]. Available: https://www.nytimes.com/2007/05/10/business/worldbusiness/10iht-enron.1.5648578.html

[5] Federal Register Online, "United States v. Alex. Brown & Sons, Inc., et al.; Stipulation and Order and Competitive Impact Statement," 1996. [Online]. Available: https://www.govinfo.gov/content/pkg/FR-1996-08-02/html/96-19597.htm

[6] U.S. Securities and Exchange Commission, "SEC v Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larsen ." [Online]. Available: https://www.sec.gov/enforcement-litigation/whistleblower-program/notice-covered-actions/award-claim-2024-123

[5] I shit you not

[6] Similarly, in response to this action, the Modern Emoluments and Malfeasance Enforcement Act (MEME, ironically) was introduced. This act would prohibit the issuance or endorsement of any financial asset by the president, senior White House officials, or members of Congress, or their spouses or children [32]. Though this is highly unlikely to pass, given the current state of the US government.

[7] M. T. Uyeda, "Crypto task force designation," U.S. Securities and Exchange Commission, February 2025. [Online]. Available: https://www.sec.gov/files/crypto-task-force-designation-letter.pdf

[8] A. Back, "Hashcash - a denial of service counter-measure."

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system."

[10] The White House, "ESTABLISHMENT OF THE STRATEGIC BITCOIN RESERVE AND UNITED STATES DIGITAL ASSET STOCKPILE ," Mar. 2025. [Online]. Available: https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile/

[11] R. Linus, "BitVM: Compute Anything on Bitcoin."

[12] V. Buterin, "A Next Generation Smart Contract & Decentralized Application Platform."

[13] k. Kurt, "Zero to Monero - First Edition." [Online]. Available: https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf

[14] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and More," in *2018 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA: IEEE, May 2018, p. 315–334. [Online]. Available: https://ieeexplore.ieee.org/document/8418611/

[15] M. Herlihy, "Atomic Cross-Chain Swaps," no. arXiv:1801.09515, May 2018, arXiv:1801.09515 [cs]. [Online]. Available: http://arxiv.org/abs/1801.09515

[16] The Department Of The Treasury, "Pilot IRS Cryptocurrency Tracing Award Notice ." [Online]. Available: https://sam.gov/opp/5ab94eae1a8d422e88945b64181c6018/view

[17] B. Chase and E. MacBrough, "Analysis of the xrp ledger consensus protocol," no. arXiv:1802.07242, Feb. 2018, arXiv:1802.07242 [cs]. [Online]. Available: http://arxiv.org/abs/1802.07242

[18] I. Amores-Sesar, C. Cachin, and J. Mićić, "Security analysis of ripple consensus," no. arXiv:2011.14816, Nov. 2020, arXiv:2011.14816 [cs]. [Online]. Available: http://arxiv.org/abs/2011.14816

[19] J. Ginesin, M. von Hippel, E. Defloor, C. Nita-Rotaru, and M. Tüxen, "A formal analysis of sctp: Attack synthesis and patch verification," no. arXiv:2403.05663, Mar. 2024, arXiv:2403.05663 [cs]. [Online]. Available: http://arxiv.org/abs/2403.05663

[20] I. Amores-Sesar, C. Cachin, and J. Mićić, "Security analysis of ripple consensus," *LIPIcs, Volume 184, OPODIS 2020*, vol. 184, pp. 10:1–10:16, 2021.

[21] J. Ginesin and R. Zhu, "Replication: Security Analysis of Ripple Consensus." [Online]. Available: https://jakegines.in/assets/ripple.pdf

[22] M. R. Albrecht, S. Celi, B. Dowling, and D. Jones, "Practically-exploitable cryptographic vulnerabilities in matrix," in *2023 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, May 2023, p. 164–181. [Online]. Available: https://ieeexplore.ieee.org/document/10351027/

[23] Ripple, "Q4 2024 XRP Markets Report." [Online]. Available: https://ripple.com/insights/q4-2024-xrp-markets-report/

[24] J. Hyatt, “What A Sputtering SPAC Reveals About Ripple’s Billion-Dollar XRP Business.” [Online]. Available: https://www.forbes.com/sites/johnhyatt/2023/04/19/what-a-sputtering-spac-reveals-about-ripples-billion-dollar-xrp-business/

[25] M. Sigalos, “Harris PAC’s $1 million contribution from Ripple’s Chris Larsen shows crypto industry warming to VP,” Oct. 2024. [Online]. Available: https://www.cnbc.com/2024/10/15/kamala-harris-got-1-million-from-ripples-chris-larsen-crypto-warms.html

[26] E. Wilkins, “Crypto industry super PAC is 33-2 in primaries, with $100 million for House, Senate races,” Jun. 2024. [Online]. Available: https://www.cnbc.com/2024/06/26/crypto-pac-house-senate-elections.html

[27] Securities and Exchange Commission, “SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering.” [Online]. Available: https://www.sec.gov/newsroom/press-releases/2020-338

[28] “U.S. Reports: S.E.C. v. Howey Co., 328 U.S. 293 (1946).” [Online]. Available: https://www.loc.gov/item/usrep328293/

[29] CourtListener, “ Securities and Exchange Commission v. Ripple Labs Inc. (24-2648) Court of Appeals for the Second Circuit.” [Online]. Available: https://www.courtlistener.com/docket/69230851/securities-and-exchange-commission-v-ripple-labs-inc/

[30] G. R.-P.-. Rep. Thompson, “Text - H.R.4763 - 118th Congress (2023-2024): Financial Innovation and Technology for the 21st Century Act,” Sep. 2024. [Online]. Available: https://www.congress.gov/bill/118th-congress/house-bill/4763/text

[31] “Oversight of Dodd-Frank Act Implementation.” [Online]. Available: https://financialservices.house.gov/dodd-frank/

[32] M. A. NOTUS, “Silicon Valley lawmaker wants to make it illegal for Trump to hawk crypto,” Feb. 2025. [Online]. Available: https://sanjosespotlight.com/silicon-valley-lawmaker-wants-to-make-it-illegal-for-trump-to-hawk-crypto/