THE DOUBLE-EDGED PROMISE OF CRYPTOCURRENCY: HOW INNOVATION CREATES NEW VULNERABILITIES AND HOW GOVERNMENT OVERSIGHT CAN REDUCE CRYPTO CRIME

Jason H. Meuse

THE DOUBLE-EDGED PROMISE OF CRYPTOCURRENCY: HOW INNOVATION CREATES NEW VULNERABILITIES AND HOW GOVERNMENT OVERSIGHT CAN REDUCE CRYPTO CRIME

Jason H. Meuse*

ABSTRACT

The fallout from the FTX fraud scheme brought the dangers of crypto front-and-center. Not only did FTX perpetrate a massive fraud, but its fall exposed the cryptocurrency exchange to hacking resulting in the theft of over $477 million in crypto assets. This theft is not isolated to FTX; by October 2022, hackers had already stolen over $3 billion. In addition, new organizational structure and technology in the crypto industry has introduced new vulnerabilities. Cryptocurrency exchanges, decentralized exchanges, and cross-chain bridges are prime targets for hackers to both steal and launder crypto assets. Part of the reason these technologies leave assets vulnerable is that they undermine a central premise of crypto: a currency system accountable to users within a closed ecosystem. While the industry has responded by increasing its security standards and procedures, its anti-government attitude has inhibited cooperation with government that could make the crypto marketplace even more secure. Many firms are incorporated outside of U.S. jurisdiction, lightening the compliance burden at the cost of security. However, establishing industry security standards and cooperating with the government can lead to higher security and greater consumer confidence.

INTRODUCTION

The recent catastrophe involving cryptocurrency exchange FTX puts a spotlight on an emerging cryptocurrency industry that has great potential for growth, but also is prone to criminal activity. Watching the billion-dollar collapse of FTX underscores the prevalence of fraud in the cryptocurrency field, but hackers have capitalized on the opaque and unregulated industry to steal assets and launder the digital currency through services meant to fulfill the promises of crypto, namely decentralization and interoperability.[1] As of October 2022, over $3 billion worth of cryptocurrency assets have been stolen through hacking.[2] Hackers have laundered over $477 million in crypto that they stole from FTX as law enforcement closed in on Sam Bankman Fried's fraudulent FTX-Alameda scheme.[3]

This paper explores how the decentralized crypto ecosystems and the anti-regulatory sentiments founding them have facilitated billions of dollars in stolen cryptocurrency assets and how the industry and government agencies have attempted to address the emergence of digital

* University of Maine School of Law, Class of 2023.

[1] Khristopher J. Brooks, *Hackers have stolen record $3 Billion in cryptocurrency this year*, CBS NEWS (Oct. 13, 2022), https://www.cbsnews.com/news/cryptocurrency-theft-hacker-chainalysis-blockchain-crime/ [hereinafter *Hackers Have Stolen $3 Billion*]; *see Bitcoin Explained*, UPFOLIO https://www.upfolio.com/ultimate-bitcoin-guide.

[2] *Hackers Have Stolen $3 Billion*, *supra* note 1.

[3] Arjun Kharpal, et al., *FTX-owned Service Being Used to Launder Hundreds of Millions 'Hacked' From FTX, Researchers Say,* CNBC (Nov. 21, 2022), https://www.cnbc.com/2022/11/21/ftx-theft-hackers-start-to-launder-477-million-of-stolen-crypto.html.

currency. Part II will explain how the philosophies undergirding the adoption of digital currency also exacerbate the problem of cryptocurrency theft and money laundering. Part III will give a brief overview of blockchain technology and three primary vectors cybercriminals use to steal digital assets: cryptocurrency exchanges, decentralized finance services, and cross-chain bridges. Part IV demonstrates the steps the crypto industry has taken to improve its security and address crypto theft. Part V will show that, although government agencies are participating in regulating cryptocurrency, they have yet to address vulnerabilities in the digital platforms that cybercriminals exploit to amass and clean their crypto lucre. Finally, Part VI offers recommendations for legal and regulatory response to digital asset theft.

I. THE PROMISE OF CRYPTOCURRENCY IS A DOUBLE-EDGED SWORD

Cryptocurrency evangelists fantasize a world where consumers are free from oversight of governments and large banks. To accomplish this, digital currencies like Bitcoin have arisen. Supporters of digital currency tout decentralization, verifiability, limited supply, divisibility, and security as virtues that digital currencies carry to solve problems inherent to government-issued (fiat) currency.[4] Since digital currencies like Bitcoin are not regulated by any government or bank, they can be more freely used in transactions; supporters emphasize that the decentralized nature of crypto prevents larger entities like banks from limiting how the actual owners of digital currency use it in transactions. In addition, digital currency's existence on the blockchain obviates the need for entities like banks to verify transactions. Transactions on the blockchain rely on the computers that exist on the platform for verification, essentially redistributing the responsibility typically shouldered by banks upon the entire community of users. In turn, consumers also avoid fees banks charge for their services.[5]

However, the decentralized nature of cryptocurrency facilitates cybercrime. Exchanges and autonomous organizations have less oversight and few full-time cybersecurity professionals.[6] Exchanges are often established in countries with weaker regulatory schemes, providing the benefit of decentralization for both legitimate consumers and cybercriminals. Hackers take advantage of weak centralized oversight structures to steal billions of dollars of assets from cryptocurrency exchanges.[7]

Both limited supply and divisibility address problems of inflation; since there is a finite amount of any particular digital currency[8], no entity can affect its value by minting more. Additionally, since cryptocurrencies are infinitely divisible (as opposed to dollars only being divisible into hundredths), the value of the currency can increase without pricing consumers out if they have only a small amount of it.[9] Finally, cryptocurrencies such as Bitcoin are considered

---

[4] *See Bitcoin Explained supra*, note 1.

[5] FEDERAL TRADE COMM'N, *What to Know about Cryptocurrency and Scams*, https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.

[6] Oluwapelumi Adejumo, *Vulnerability of Crypto Exchanges and the Need to Do Better*, COINCODEX (Nov. 23, 2022), https://coincodex.com/article/21321/vulnerability-of-crypto-exchanges-and-the-need-to-do-better/.

[7] Kevin Collier, *Crypto Exchanges Keep Getting Hacked, and There's Little Anyone Can Do*, NBC NEWS (Dec. 17, 2021), https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870.

[8] Mike Swigunski, *How Cryptocurrency Will Transform the Future Business Forever*, Forbes (Apr. 17, 2021), https://www.forbes.com/sites/mikeswigunski/2021/04/17/how-cryptocurrency-will-transform-the-future-business-forever/?sh=3229b4494368

[9] *See Bitcoin Explained supra*, note 1.

secure, as they employ encryption to protect the assets, only accessible with unique credentials.[10] However, the security of the currency itself is moot when hackers are able to target the exchanges that control the flow of crypto assets and take the credentials that grant access to staggering amounts of funds kept in "hot wallets."[11]

Another benefit touted by crypto supporters is the virtual anonymity digital currencies provide. However, organizations like the FTC warn that cryptocurrency transactions are not truly anonymous because they utilize the blockchain, which is a centralized public ledger containing crypto wallet addresses and transaction information that can be used to identify a consumer later.[12] Nevertheless, criminals still are able to use the relative anonymity of the blockchain to conduct hacks and other cybercrime, such as laundering money procured through ransomware attacks.[13]

However, these qualities also carry drawbacks, perhaps most clearly explained by contrasting cryptocurrency and a fiat currency, namely the U.S. Dollar. First, cryptocurrency is not backed by a government.[14] This means that there are no entities like the Federal Deposit Insurance Corporation (FDIC) to protect digital assets. The Federal Trade Commission (FTC) warns that consumers can lose digital assets through any number of issues against which governments or banks can normally safeguard, like failure of the exchange platform, hacking, theft of credentials, mistaken transfers of funds, or losing access to a digital wallet (by losing the password, for example).[15] Indeed, there are no reliable digital equivalents to the capacity of credit card companies or banks to cancel a transaction or help retrieve lost money.

In addition, cryptocurrencies are much more volatile than fiat currencies. Their values are constantly fluctuating, especially considering they are not backed by a trustworthy institution, such as the U.S. dollar backed by trust in the U.S. government. Digital currencies rely on typical market stimuli of supply and demand, heavily influenced by trust in the currency itself, rather than a backing institution.[16]

In sum, cryptocurrencies promise a financial system that eschews government oversight and institutional control of funds for consumer autonomy. The problem is that cybercriminals take advantage of decentralized, interoperable, and secure cryptocurrencies to engage in high-impact theft and money laundering without recourse.

II. BASICS OF THE TECHNOLOGY AND HOW CRIMINALS EXPLOIT IT.

Cybercriminals exploit vulnerabilities in the cryptocurrency ecosystem to steal such a sheer volume of crypto assets. To understand how they accomplish this, it is necessary to know how the technology works. First, cryptocurrencies typically derive their supply from "mining," which is the use of advanced computer equipment to solve complex math problems.[17] These

---

[10] *Id.*
[11] Collier *supra*, note 7.
[12] *See Bitcoin Explained supra* note 1.
[13] Elliptic, *Elliptic Launches Next Generation of Blockchain Analytics with Introduction of Holistic Screening for Cross-Chain Compliance*, Elliptic (Aug. 10, 2022), https://www.elliptic.co/media-center/elliptic-next-generation-blockchain-analytics-with-holistic-screening-cross-chain.
[14] *What to Know about Cryptocurrency and Scams*.
[15] *Id.*
[16] *Id.*
[17] *Id.*

currencies are then sold on exchanges that operate on a blockchain. An exchange is similar to the stock exchange in that it monitors the value of one or more cryptocurrencies and deals in their buying and selling.

The blockchain serves as the foundation for cryptocurrency exchanges. A blockchain at its heart is a centralized ledger for transactions.[18] All of the computers in a network run the same software.[19] When someone on that network makes a transaction, every computer in the network verifies the transaction.[20] Then, transaction data is grouped into a "block," which is then recorded across the whole system in a chain. Hence, a blockchain.[21]

A large enough blockchain is reasonably secure. The centralized ledger solves the "Double Spend Problem." The "Double Spend Problem" is inherent to currency that exists only online. Since transactions need to be approved across a central ledger (the blockchain), it makes it much more difficult for hackers to falsify transactions and spend the same money in two simultaneous transactions.[22] Blockchain accomplishes freedom from a centralized entity, like a bank, because every computer on a network must verify a transaction before the transaction can be recorded on the blockchain. Otherwise, the computers on the network would reject the transaction and prevent it from going through. For bad actors to get past this verification mechanism, they must either alter the histories of every computer on the network or join the network with enough computers to cheat fraudulent transactions into verification.[23] The latter technique is called a "51% attack."[24] Both techniques would be prohibitively expensive on larger networks, affirming the security of the blockchain system.

Cybercriminals are more successful when targeting entities and technology that deviates from the closed crypto ecosystem, namely cryptocurrency exchanges, decentralized finance services, and cross-chain bridges. I deal with each of these in turn.

A. Cryptocurrency Exchanges

As stated above, cryptocurrency exchanges function similarly to stock exchanges, but hackers more easily infiltrate these systems through exploiting vulnerabilities that strict oversight helps cover in the securities market. First, similarly to a bank, cryptocurrency exchanges only keep a fraction of their funds on hand, in what are called "hot wallets."[25] These "hot wallets" enable transactions with users through internet connection.[26] The rest of an exchange's assets are held in "cold wallets" that are purportedly not connected to the internet.[27] Users allow

[18] Stellar.org, *Blockchain Basics*, (Dec. 17, 2022), https://stellar.org/learn/blockchain-basics.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *See Bitcoin Explained.*
[23] Stellar.org, *Blockchain Basics*.
[24] *Id.*
[25] Kevin Collier, *Crypto exchanges keep getting hacked, and there's little anyone can do*.
[26] Jennifer Korn, *Crypto heists are only getting bigger. Here's what you should know*, CNN (Dec. 12, 2021), https://www.cnn.com/2021/12/12/tech/crypto-exchange-hacks-explainer/index.html.
[27] Aaron Lane, *Crypto theft is on the rise. Here's how the crimes are committed, and how you can protect yourself*, The Conversation (Feb. 3, 2022), https://theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027.

cryptocurrency exchanges to have custody over their assets to facilitate transactions, but these have proved to be prime targets for hacks.

The facility of transaction granted by exchanges' "hot wallets" comes at a cost. The internet connection also makes these wallets more accessible to hackers. Hackers can steal exchange employee credentials, and, by extension, the private keys of consumer "hot wallets" and all the funds therein.[28] These hackers employ tried and true methods to gain access to consumers' digital funds such as phishing and exploiting errors in code.[29]

But how could such technologically advanced firms be such easy targets for hackers? Unsurprisingly, the answer lies in the company culture surrounding cryptocurrency exchanges. Tech entrepreneurs establish their cryptocurrency exchange startups in countries that lack regulation, (for example, the now-defunct FTX was based in the Bahamas[30]) which allows them to run the organization how they wish.[31] However, the lack of regulation also makes it difficult for other countries' law enforcement agencies to pursue international hackers.[32] In addition, the startups have small staffs and employ "few if any full-time cybersecurity professionals." [33] Crypto startups are often founded with "anti-bank and anti-oversight" sentiments, cementing a culture against working with law enforcement, even though doing so would often be in their best interest.[34] Tech developers in these firms also focus more on making their code work without auditing it to ensure its security, leading to vulnerabilities that hackers easily exploit.[35] These qualities lead to poor risk management and risk monitoring within firms that would have otherwise prevented a breach. The risk of losing funds has led to some users transferring their funds from exchanges to their own software or hardware wallets.[36] While this solution is a more secure alternative than allowing vulnerable exchanges to maintain custody over digital assets, it is not a satisfying one for digital currency advocates because maintaining custody of these funds also prevents the benefits of expedient transactions.

The good news is that successful hacks against cryptocurrency exchanges are becoming less common. Exchanges have learned harsh lessons from high-profile hacks that have been catastrophic.[37] Crypto startups often do not have emergency funds; a hack often results in the failure of the company, with no recourse available for consumers whose assets were entrusted to an exchange.[38] Exchanges have since strengthened their security, but their measures are not foolproof. The recent fall of FTX and Alameda exposed the exchange to hackers who stole over $477 million in cryptocurrency assets, proving that an increased awareness of cybersecurity

---

[28] Kevin Collier, *Crypto exchanges keep getting hacked, and there's little anyone can do*.

[29] *See* Kevin Collier, *Crypto exchanges keep getting hacked, and there's little anyone can do*; Arjun Kharpal, MacKenzie Sigalos, and Rohan Goswami, *FTX-owned service being used to launder hundreds of millions 'hacked' from FTX, researchers say.*

[30] Arjun Kharpal, MacKenzie Sigalos, and Rohan Goswami, *FTX-owned service being used to launder hundreds of millions 'hacked' from FTX, researchers say.*

[31] Kevin Collier, *Crypto exchanges keep getting hacked, and there's little anyone can do*.

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] Aaron Lane, *Crypto theft is on the rise. Here's how the crimes are committed, and how you can protect yourself.*

[37] Khristopher J. Brooks, *Hackers have stolen record $3 Billion in cryptocurrency this year*.

[38] Kevin Collier, *Crypto exchanges keep getting hacked, and there's little anyone can do*.

concerns does not necessarily translate into a uniform culture of security.[39] However, hackers are targeting decentralized finance services and cross-chain bridges, which both are less regulated and have not caught up in their security.[40]

B. Decentralized Finance Services

Decentralized Finance (DeFi) services, or Decentralized exchanges, take the crypto fantasy one step further by eliminating the need for an exchange overseeing transactions. DeFi services rely on peer-to-peer exchange mechanisms that obviate intermediaries like centralized exchanges.[41] They accomplish this by using smart contracts, which are computer programs that automatically execute buying and selling.[42] DeFi users keep custody over their assets as they are being traded.[43] Like centralized cryptocurrency exchanges, decentralized exchanges run on top of blockchains to execute their trades.

Without human beings conducting minute operations in DeFi services, there is less vulnerability stemming from human error, but DeFi platforms still share plenty of problems. Much of the code used on DeFi platforms is open-source.[44] Part of the rationale for using open-source code is a philosophy of transparency in DeFi organizations, but that transparency cuts both ways, making it easier for hackers to exploit.[45] Unsurprisingly, most of the successful hacks on DeFi platforms exploit vulnerabilities in the code or app design itself.[46]

In addition, DeFi platforms use technology called "blockchain oracles" to ensure accurate pricing.[47] Blockchain oracles access data outside of the blockchain ecosystem, which means they serve as a weak point for the otherwise isolated blockchain.[48] The necessity of an oracle reveals a paradox about the blockchain. A blockchain is considered secure because it is isolated from the rest of an information ecosystem.[49] However, outside information is required to accurately estimate the value of digital currency.[50]

Even for much-needed security, blockchain oracles need to make tradeoffs. More secure oracles are slower, which means that they are more vulnerable to arbitrage, the simultaneous purchase and sale of the same or similar assets in different markets.[51] However, fast oracles are

---

[39] Khristopher J. Brooks, *Hackers have stolen record $3 Billion in cryptocurrency this year*.
[40] *See* Eray Arda Akartuna and Thibaud Madelin, *The State of cross-chain crime*; Khristopher J. Brooks, *Hackers have stolen record $3 Billion in cryptocurrency this year*.
[41] Eray Arda Akartuna and Thibaud Madelin, *The State of cross-chain crime*, 12.
[42] Chainalysis Team, *Hackers are Stealing More Cryptocurrency from DeFi Platforms Than Ever Before*, Chainalysis (Apr. 12, 2022), https://blog.chainalysis.com/reports/2022-defi-hacks.
[43] Eray Arda Akartuna and Thibaud Madelin, *The State of cross-chain crime*, 12.
[44] Chainalysis Team, *Hackers are Stealing More Cryptocurrency from DeFi Platforms Than Ever Before*.
[45] *Id.*
[46] Jennifer Korn, *Crypto heists are only getting bigger. Here's what you should know*.
[47] Chainalysis Team, *Hackers are Stealing More Cryptocurrency from DeFi Platforms Than Ever Before*.
[48] *Id.*
[49] Binance, *What's a Blockchain Bridge?*, Binance (Nov. 11, 2022), https://academy.binance.com/en/articles/what-s-a-blockchain-bridge.
[50] Chainalysis Team, *Hackers are Stealing More Cryptocurrency from DeFi Platforms Than Ever Before*.
[51] *Id.*

vulnerable to price manipulation.[52] This differs greatly from a traditional blockchain which is a closed ecosystem.[53]

C. Cross-Chain Bridges

Cross-chain bridges are a solution to the lack of interoperability of cryptocurrencies from different blockchain ecosystems. The bridges are points at which two blockchains interact. Consumers can use cross-chain bridges to transfer a cryptocurrency from one blockchain, such as Bitcoin (BTC), to another blockchain, like Ethereum (ETH).[54] Bridges allow owners of a cryptocurrency asset to use that asset in transactions across more contexts, defying the limits of one isolated blockchain.

These bridges facilitate interoperability through two primary channels, "lock-and-mint" and "wrapping."[55] "Lock-and-mint" bridges take possession of one cryptocurrency, "lock" it, and issue the exchange equivalent of the target token to the user.[56] Bridges do not actually mint more of any currency; they instead issue the target token from locked assets that they accumulate from conversions in the other direction.[57] For example, a bridge may lock BTC in exchange for ETH . This allows a user to access the Ethereum blockchain for transactions. This is akin to exchanging a U.S. dollar for a Euro.

"Wrapping" bridges instead convert an asset to a "wrapped" form of it on another blockchain.[58] "Wrapped" currencies have the same value as their unwrapped counterparts[59] (wrapped Bitcoin, wBTC, vis-à-vis BTC). Users can then spend their wrapped currency on services outside of the unwrapped currency's native blockchain.[60]

These bridges are vulnerable because they "often feature a central storage point of funds that back the 'bridged' assets on the receiving blockchain.[61] Cross-chain bridges have emerged as attractive targets for cybercriminals because they have not yet had the security revelation that cryptocurrency exchanges have.[62] Elliptic, a blockchain analysis provider, argues that cross-chain bridges have become more attractive targets based on a theory of "crime displacement" where criminals target entities where they will face the least resistance.[63] Indeed, by October 2022, assets stolen from cross-chain bridges made up 64% of all losses this year.[64] Like centralized exchanges and DeFi services, cross-chain bridges suffer cyberattacks that exploit bugs in their code. For example, a bridge called Nomad lost over $200 million worth of assets

---

[52] *Id.*
[53] Binance, *What's a Blockchain Bridge?*, Binance (Nov. 11, 2022).
[54] Khristopher J. Brooks, *Hackers have stolen record $3 Billion in cryptocurrency this year*.
[55] Eray Arda Akartuna and Thibaud Madelin, *The State of Cross-Chain Crime*, 23.
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] Chainalysis Team, *Vulnerabilities in Cross-Chain Bridge Protocols Emerge as a Top Security Risk*, Chainalysis (Aug. 2, 2022), https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/.
[62] MacKenzie Sigalos, *Crypto criminals laundered $540 million using a service called RenBridge, new research shows*, CNBC (Aug. 10, 2022), https://www.cnbc.com/2022/08/10/crypto-criminals-laundered-540-million-using-renbridge-elliptic-says.html.
[63] Eray Arda Akartuna and Thibaud Madelin, *The State of cross-chain crime*, 30.
[64] Khristopher J. Brooks, *Hackers have stolen record $3 Billion in cryptocurrency this year*.

from cybercriminals exploiting a bug.[65] In addition, the bridges "multiply their possible vectors of attack by operating across two or more blockchains."[66] This makes sense considering each interaction that an isolated blockchain ecosystem has with another presents another opening into the ecosystem for hackers to exploit.

Bridges are also attractive to cybercriminals because they offer a relatively safe means to launder cryptocurrency assets gained in other ways, such as from hacks of other crypto firms or ransomware payments. Since bridges allow currency to leave a blockchain, it is more difficult to trace criminal transactions because interoperability guarantees more anonymity.[67] Furthermore, bridges rely on thousands of pseudonymous validators called "darknodes" for verification, making stolen assets harder to trace.[68] Criminals can transfer one currency to another ecosystem, mask how they got it, and access services that the native blockchain otherwise had no access to.[69] In a cosmically fitting attack, hackers stole an estimated $477 million in crypto assets from FTX and used a bridge called RenBridge, owned by FTX counterpart Alameda, to launder the stolen Bitcoin assets into "RenBTC" a wrapped Bitcoin that operates on the Ethereum blockchain.[70] The RenBridge service is only one of many bridges that cybercriminals, including nation-state actors from North Korea, have used to process ransomware payments, fraudulent lucre, and stolen assets.[71] Elliptic estimates that cybercriminals will launder more than $10.5 billion in crypto assets by 2025.[72]

Cybercriminals take advantage of lagging regulation on cross-chain bridges. Elliptic's chief scientist notes that "cross-chain bridges are a loophole in the regulatory regime that has been painstakingly established by governments around the world, to combat crypto laundering."[73] Not only have bridge providers not internally recognized the need for enhanced cybersecurity infrastructure, but governments have also been slow to recognize bridges as the next target for criminals. At this point, bridge providers and the crypto industry at large are in the position to react most readily to bad actors, with government regulators following behind.

II. HOW THE CRYPTO INDUSTRY HAS RESPONDED TO CRYPTO CRIME

Given the millions of dollars in digital assets that have been the subject of scams, breaches, and theft, it is unsurprising that cryptocurrency firms have increased their security.

---

[65] MacKenzie Sigalos, *Crypto criminals laundered $540 million using a service called RenBridge, new research shows*.

[66] *Id.*

[67] Eray Arda Akartuna and Thibaud Madelin, *The State of cross-chain crime*, 23.

[68] MacKenzie Sigalos, *Crypto criminals laundered $540 million using a service called RenBridge, new research shows*.

[69] Eray Arda Akartuna and Thibaud Madelin, *The State of cross-chain crime*, 23.

[70] Arjun Kharpal, MacKenzie Sigalos, and Rohan Goswami, *FTX-owned service being used to launder hundreds of millions 'hacked' from FTX, researchers say*.

[71] *See* MacKenzie Sigalos, *Crypto criminals laundered $540 million using a service called RenBridge, new research shows*; Chainalysis team, Chainalysis Team, *Vulnerabilities in Cross-Chain Bridge Protocols Emerge as a Top Security Risk*.

[72] *Crypto criminals exploit blockchain vulnerability to launder $10.5 bn by 2025*, Elliptic (Nov. 30, 2022), https://www.elliptic.co/media-center/crypto-criminals-exploit-blockchain-vulnerability-to-launder-10.5bn-of-dirty-money-by-2025.

[73] MacKenzie Sigalos, *Crypto criminals laundered $540 million using a service called RenBridge, new research shows*; *Crypto criminals exploit blockchain vulnerability to launder $10.5 bn by 2025*.

Since the proliferation of several high-profile hacks, centralized cryptocurrency exchanges have strengthened their security programs, which, in turn, decreased the frequency of attacks.[74] In addition, large firms have called on governments to regulate the cryptocurrency industry. Binance, a cryptocurrency exchange established in the Cayman Islands, that does not currently serve the U.S., has called on global regulators to set regulations.[75] The CEO of Binance, Changpeng Zhao, emphasized that crypto is here to stay, stating "I think most governments now understand that adoption will happen regardless. It's better to regulate the industry instead of trying to fight against it."[76] The firm has also accepted that platforms have a duty to protect consumers and change internal processes that can prevent cybercrime, rather than facilitate it.[77] In addition, Binance has set up a Global Advisory Board to help navigate new regulatory waters.[78] This board includes former U.S. Senator Max Baucus and American political strategist David Plouffe, and purports to help advance Binance's efforts in the crypto space and stay abreast on government regulation.[79]

Crypto analytics firms, such as Chainalysis, also advocate for more resources allocated to security measures and training.[80] Others recognize that exchanges need to bring their risk management and monitoring up to the standards many companies outside the cryptocurrency field already have.[81] These strategies include implementing standard risk management programs with active and passive controls, underscored by a three-pronged focus on risk management, custody, and user protection.[82] Active controls include managing blacklists and monitoring the frequency of asset withdrawals, while passive controls include monitoring suspicious login attempts and transactions and utilizing outside vendors to protect private crypto keys.[83]

Crypto analytics firms have also stepped up to market demand for greater oversight and rapid improvement of monitoring capabilities. The crypto compliance firm Elliptic has recognized that legacy blockchain analytics have been constrained to tracking a single currency or a single blockchain.[84] This means that cryptocurrency firms are unable to check if assets have originated from sanctioned entities or have been associated with illicit activities.[85] The firm

---

[74] Khristopher J. Brooks, *Hackers have stolen record $3 Billion in cryptocurrency this year*; *see* Eray Arda Akartuna and Thibaud Madelin, *The State of cross-chain crime*.

[75] Guardian Staff and Agencies, *World's largest Cryptocurrency Exchange hacked with possible losses of $500 million*, The Guardian (Oct. 7, 2022), https://www.theguardian.com/technology/2022/oct/07/binance-crypto-hack-suspended-operations.

[76] Michele Kambas, *Binance CEO says don't fight crypto, regulate it*, Reuters (Nov. 25, 2022), https://www.reuters.com/legal/government/binance-ceo-zhao-says-dont-fight-crypto-regulate-it-2022-11-25/.

[77] Guardian Staff and Agencies, *World's largest Cryptocurrency Exchange hacked with possible losses of $500 million*.

[78] Ezra Reguerra, *Binance Establishes Global Advisory Board to work on regulatory and political issues*, CoinTelegraph (Sept. 22, 2022), https://cointelegraph.com/news/binance-establishes-global-advisory-board-to-work-on-regulatory-and-political-issues.

[79] *Id.*

[80] Chainalysis Team, *Vulnerabilities in Cross-Chain Bridge Protocols Emerge as a Top Security Risk*.

[81] Oluwapelumi Adejumo, *Vulnerability of Crypto Exchanges and the Need to Do Better*.

[82] *Id.*

[83] *Id.*

[84] Eray Arda Akartuna and Thibaud Madelin, *The State of cross-chain crime*, 43.

[85] *Id.* at 44-45

offers a solution, which they call Holistic Screening, to solve these problems.[86] The screening software allows Virtual Asset Service Providers, or VASPs, to screen multiple assets, trace movement across assets, and screen across blockchains.[87] In essence, firms like Elliptic have developed the technology necessary to make vulnerable systems like DeFi platforms and cross-chain bridges more secure through tracking measures that deter the theft, hacking, and laundering efforts of cybercriminals.[88]

The crypto industry is improving its practices and developing tools that make it easier to track and address cybercrime, and government cooperation can help fight cybercrime more easily. The impact of these efforts would be of lesser consequence if the government were not moving into the field. Thankfully, the U.S. government has already made moves to address cryptocurrency that establish a foundation for further regulation.

IV. GOVERNMENT AGENCY RESPONSE IN THE CRYPTOCURRENCY DOMAIN

Although cryptocurrency is a novel technology that does not neatly fit into existing government regulatory schemes, the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC) have found some success in regulating and addressing consumer concerns. The existing material that these government agencies have issued serves as a decent foundation that may prove useful in developing future regulation.

A. Securities and Exchange Commission

It was initially uncertain whether cryptocurrency came under the purview of the SEC because it was unclear whether crypto satisfied the definition of a "security," as defined in the Securities Exchange Act of 1934. Under the Act, securities include "investment contracts" which are "investment[s] of money in a common enterprise with reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others."[89] The SEC's investigation of the DAO began because a cybercriminal attacked the DAO (a now-defunct decentralized autonomous organization) and diverted Ethereum from the organization to his own blockchain address.[90] The question at the time was whether the DAO violated federal securities laws. For the SEC to have any jurisdiction to regulate, the agency needed to determine whether the Ethereum cryptocurrency offered by the DAO was considered a security. It was no question that Ethereum constituted "an investment of money in a common enterprise."[91] However, since the DAO had no centralized management, instead administrating funds using smart contracts, it was

[86] Elliptic, *Elliptic Launches Next Generation of Blockchain Analytics with Introduction of Holistic Screening for Cross-Chain Compliance*, Elliptic (Aug. 10, 2022), https://www.elliptic.co/media-center/elliptic-next-generation-blockchain-analytics-with-holistic-screening-cross-chain
[87] *Id.* at 43.
[88] *Id.* at 46-48.
[89] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Securities and Exchange Commission (Jul. 25, 2017), 11 (*citing SEC v. Edwards*, 540 U.S. 389, 393 (2004); *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946); *United Housing Found., Inc. v. Forman,* 421 U.S. 837, 852-53 (1975)).
[90] *Id.* at 9.
[91] *Id.* at 11.

unclear whether the investors had "a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others."[92]

The Commission found that the DAO and its parent corporation Slock.it (a German corporation) disseminated marketing materials and engaged in conduct that gave investors the required "reasonable expectation of profits[…] derived from the efforts of others."[93] The report notes that by the time the DAO and Slock.it offered the Ethereum, "The DAO's protocols had already been pre-determined by Slock.it" and had already instituted Curators [individuals selected by Slock.it] "whose function it was to (1) vet Contractors; (2) determine whether and when to submit proposals for votes; (3) determine the order and frequency of proposals that were submitted for a vote; and (4) determine whether to halve the default quorum necessary for a successful vote on certain proposals."[94] In addition, Slock.it also actively oversaw the DAO, delaying proposals after the "Attack" until it could address vulnerabilities in the code and appoint a security expert.[95]

This report shows that the SEC was able to regulate the DAO under federal securities laws even though the cryptocurrency was traded using computer programs running without human input. Participation from Slock.it and the choices it made in how the smart contracts would run and what responsibilities Curators would have, along with active intervention with the cyberattack, were sufficient to establish that the DAO was offering "investment contracts." The implications for this report are such that the SEC has jurisdiction to regulate cryptocurrency.

Recently, the SEC has cracked down on cryptocurrency offerings. The agency charged Kim Kardashian for hawking the cryptocurrency EthereumMax without disclosing that she was paid to promote the digital asset.[96] Gurbir S. Grewal, the Director of the SEC's Division of Enforcement noted, "the federal securities laws are clear that any celebrity or other individual who promotes a crypto asset security must disclose the nature, source, and amount of compensation they received in exchange for the promotion."[97] Kardashian settled the case with a payment of $1.26 million in "penalties, disgorgement, and interest."[98] While not directly related to hacking cryptocurrency exchanges, the charges against Kim Kardashian demonstrate that the FTC actively exercises the authority to enforce federal securities laws in the cryptocurrency context.

The SEC also has charged FTX co-founder and CEO Sam Bankman-Fried with "orchestrating a scheme to defraud equity investors," and is continuing investigations of other securities law violations.[99] The Commission's action against Bankman-Fried is significant because it represents a decisive exercise of authority over cryptocurrency exchanges. FTX, like many other exchanges, are established outside the U.S. to avoid U.S. Securities laws.[100] However, the SEC shows that it is willing to exercise extraterritorial authority to enforce federal

---

[92] *Id.*
[93] *Id.* at 13.
[94] *Id.*
[95] *Id.*
[96] *SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security*, Securities and Exchange Commission (Oct. 3, 2022), https://www.sec.gov/news/press-release/2022-183.
[97] *Id.*
[98] *Id.*
[99] *SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX*, Securities and Exchange Commission (Dec. 13, 2022), https://www.sec.gov/news/press-release/2022-219.
[100] Kevin Collier, *Crypto exchanges keep getting hacked, and there's little anyone can do*.

law; in response to the charges against Bankman-Fried, SEC Chair Gary Gensler stated, "the alleged fraud committed [. . .] is a clarion call to crypto platforms that they need to come into compliance with our laws. Compliance protects both those who invest on and those who invest in crypto platforms with time-tested safeguards, such as properly protecting customer funds . . ."[101]

Earlier this year, the SEC also announced that it added 20 new positions to its Crypto Assets and Cyber Unit in the Division of Enforcement.[102] This brings the number of positions in the unit to 50 and signals an investment in the enforcement of cryptocurrency under U.S. securities law.[103] Chair Gensler stated that this staff increase will make the SEC "better equipped to police wrongdoing in the crypto markets while continuing to identify disclosure and controls issues with respect to cybersecurity."[104] The Commission emphasizes that it will focus on violations related to "[c]rypto asset offerings; [c]rypto asset exchanges; [c]rypto asset lending and staking products; [d]ecentralized finance ("DeFi") platforms; [n]on-fungible tokens ("NFTs"); and [s]tablecoins."[105]

The SEC is committing to taking on crypto crime, not only the fraud schemes of the likes of Sam Bankman-Fried, but also massive crypto heists that exploit vulnerabilities in exchanges, DeFi platforms, and cross-chain bridges. The actions against Kardashian and Bankman-Fried demonstrate the Commission's confidence in its authority to regulate the cryptocurrency trade. The agency has clearly designated cryptocurrency theft as a threat that U.S. investors face as they continue to invest in the crypto market.

B. Federal Trade Commission

The Federal Trade Commission (FTC) has taken a more advisory role in the crypto field, but it is no less equipped to address crypto crime. The FTC published an article entitled "What to Know About Cryptocurrency and Scams" to help consumers make decisions about crypto investments.[106] The article explains how cryptocurrency is different from the government-issued dollar, how consumers can procure crypto, and how to spot crypto scams. [107] The Commission [108] It also outlines some scam red flags: exclusively asking for payment in cryptocurrency; guarantees of big profits or quick returns; crypto offers on dating apps; cold contact from investment managers or celebrities for crypto opportunities; impersonation of celebrities, well-known companies, startups, or government [109] In line with this advisory role, the FTC also publishes instructions for consumers to report scams or other fraud to the FTC and other government organizations.[110]

Outside of the cryptocurrency arena, however, courts have supported the FTC's regulation of companies' cybersecurity measures. In the 2015 case *Federal Trade Commission v.*

---

[101] *SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX.*
[102] *SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit*, Securities and Exchange Commission (May 3, 20222), https://www.sec.gov/news/press-release/2022-78.
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] FEDERAL TRADE COMM'N, *What to Know about Cryptocurrency and Scam*s (May 2022) https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*

Wyndham Worldwide Corporation, the Third Circuit confirmed that the FTC was able to enforce against Wyndham Worldwide's unfair business practices, namely, its poor cybersecurity practices.[111] With this in mind, it is a natural extension of the FTC's authority to enforce against the poor cybersecurity practices of cryptocurrency exchanges, DeFi services, and cross-chain bridges.

V. RECOMMENDATIONS

The proliferation of high-impact cyberattacks on cryptocurrency exchanges, DeFi services, and cross-chain bridges has demonstrated that the government must get involved in the crypto industries to safeguard consumer funds and prevent cybercriminals and nation-state actors from stealing millions in crypto assets. While this may seem contrary to the goals of cryptocurrency, the severe losses associated with crypto theft are the next theater in a cyber war that the U.S. government is already waging. To combat devastating cyberattacks on vulnerable crypto firms, I believe the government should, first, affirm executive agency authority over firms established outside the U.S. to avoid strict regulation. Second, U.S. agencies should promulgate standards for crypto firms that are in accordance with the cybersecurity standards they already enforce against domestic organizations. Finally, U.S. agencies should foster an atmosphere of cooperation with crypto firms, utilizing available technology to hold hackers accountable for their incredibly lucrative crypto crime attacks.

A. Confirm U.S. Agency Jurisdiction Over Foreign Crypto Firms

As seen from the recent prosecution of Sam Bankman Fried, U.S. executive agencies have already asserted their jurisdiction over cryptocurrency firms. Thus, Congress should introduce legislation that grants the SEC and the FTC authority over cryptocurrency businesses. By explicitly granting agencies this authority, Congress would save agencies from having to perform legislative gymnastics to assert their jurisdiction over cryptocurrency firms. An extension of agency authority would be more resilient to changes in technology that may prove more difficult for agencies to fit within the framework of century-old legislation.

The SEC has been successful in extraditing SBF for fraud charges associated with FTX. As such, there is no reason why the Commission would not be able to extend this reach to other agencies that violate federal securities laws. Similarly, the FTC has cemented itself as the *de facto* cybersecurity regulator in the United States. It is obvious that crypto firms expose American-owned crypto assets by using unfair cybersecurity practices against which the Commission has already enforced in domestic contexts.

B. Promulgate Cybersecurity Standards for Crypto Firm.

The sheer volume and impact of hacks on crypto firms necessitate government intervention to safeguard the assets of American consumers. Cryptocurrency exchanges are progressing toward being more secure, but they are not moving quickly enough to avoid catastrophic breaches that leave American investors without their assets. Decentralized finance services and cross-chain bridges have emerged as attractive vectors for cybercriminals in part because cybercriminals face less resistance when they attack them. The FTC should call on all

[111] *See* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015).

crypto firms to shore up their infrastructure to avoid hacks that leave consumers with nothing and destroy the businesses themselves.

The government must put firms on notice that it plans to enforce against their deficient and negligent cybersecurity practices. If the FTC can affirm its authority over crypto firms, it is possible that the firms will focus more on compliant, secure platforms instead of producing fast, though sloppy code that leaves millions of dollars in assets available for cybercriminals. The standards need to be flexible enough that they can apply to innovations in blockchain technology, such as the bridges that have not only enabled new possibilities for consumers but also expose investor assets to hackers.

C. Cooperate with Crypto Firms to Fight Crypto Crime

Finally, I believe that cooperation between cryptocurrency firms and the government is not fatal to the aims of cryptocurrency. On the contrary, cooperation with federal agencies allows firms to hold criminals accountable for their misdeeds. Firms like Elliptic already have and will continue to develop solutions for emerging interactions between blockchains like cross-chain bridges. The industry is already responding to the vulnerabilities created by opening up once-isolated blockchain ecosystems. Vendors develop technologies that allow exchanges to track currencies through conversions and across blockchain networks. Law enforcement cooperations can bolster efforts by cryptocurrency firms to defeat hacks and recover stolen assets.

While it does seem antithetical to involve the government in the crypto industry, whose goal is to give more power to individual consumers, this does not have to be the case. Government agencies already credit organizations that cooperate with them to address security breaches. In addition, the interests of crypto firms and the government to prevent hacks, especially from nation-state actors, already coincide. As SEC chair Gensler emphasized, compliance is a net positive for the industry.[112] Government regulation does not necessarily have to inhibit the freedom that cryptocurrency evangelists preach.

CONCLUSION

The development of cryptocurrency is moving at a breakneck pace that has proven to emphasize profits over security. Supporters prophesize a world where consumers are free to transact without gatekeeping from big banks or the limits of national currencies. However, this future remains distant as long as cryptocurrency platforms continue to suffer massive breaches resulting in the theft of millions of dollars in assets per occurrence. The industry has progressively moved towards decentralization and interoperability with the rise of cryptocurrency exchanges, decentralized finance services, and cross-chain bridges. These benefits come at the cost of security because the industry rewards rapid innovation over slower, secure growth. The potential of a currency that can be used universally has come closer to reality than ever before with bridges, but the industry has failed to respond to new vulnerabilities as quickly as they arise, leading to the crypto dream being a risky one.

All hope is not lost, though. Crypto vendors are developing tools that will allow new interoperable technology to be more secure for consumers. In addition, the U.S. government is asserting its authority over crypto firms more so than ever to tamp down on exchanges that are vulnerable to cybercrime. I believe that further government intervention in the crypto industry

[112] *SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit.*

can, instead of limiting its growth, help the industry flourish. The government can set standards to guide firms with responsible administration of consumer assets, and even though they may be reluctant to do so, firms can enlist government assistance in holding cybercriminals responsible and recovering assets whose loss would otherwise be devastating for consumers and the industry at large.