Unicorns in the Wild West: Empirical Analysis of Cybercrime Facilitated by Cryptocurrencies

Arghya Mukherjee
Tandy School of Computer Science
College of Engineering and Computer Science
The University of Tulsa
Tulsa, OK, USA
arghya-mukherjee@utulsa.edu

Tyler Moore
School of Cyber Studies
College of Engineering and Computer Science
The University of Tulsa
Tulsa, OK, USA
tyler-moore@utulsa.edu

***Abstract*—The explosion of cryptocurrencies has created countless opportunities for abuse by cybercriminals. In theory, thousands of newly minted coins and tokens could offer miscreants the chance to hide illicit activities from view. In practice, most crypto-facilitated cybercrime transacts in Bitcoin and Ethereum, the two most popular cryptocurrencies. This paper seeks empirical answers to questions about which types of cybercriminal activities are undertaken at different cryptocurrencies. We focus on 406 widely traded cryptocurrencies, with a special focus on the 54 "unicorns" that have achieved market capitalizations exceeding $1 billion. Using summary statistics and regression analysis, we confirm that more popular coins are used in crimes more often. Ethereum is more likely to be used for cryptocurrency-enabled cybercrime, whereas Bitcoin is used more for legacy cybercrimes. We also present evidence that utilization in cybercrimes vary based on coin characteristics and popularity.**

***Index Terms*—Scams, Crimes, Cryptocurrency, Unicorns**

I. Introduction and Background

The cryptocurrency market has seen remarkable growth since its inception, reaching a valuation of over $3 trillion as of 2024, according to coinmarketcap.com. Cryptocurrencies represent a groundbreaking innovation in digital finance, promising features such as pseudonymity, low transaction costs, and the elimination of intermediaries like banks or payment processors. However, these same characteristics have also facilitated a significant rise in cybercrime. While the pseudonymous nature of cryptocurrency transactions enhances user privacy, it also provides a fertile ground for illicit activities.

Bitcoin, the first and most widely adopted cryptocurrency, gained early notoriety for its role in facilitating ransomware payments. This enabled bad actors to extort victims with a higher degree of anonymity. Following Bitcoin's rise, privacy-focused cryptocurrencies such as Monero and Z-Cash emerged, offering even greater transaction confidentiality. While this development has its advantages, it has also made cryptocurrencies an attractive tool for money laundering and other illicit activities, even becoming the preferred medium in some scenarios.

Cryptocurrencies have not only facilitated cybercrimes but also spawned entire new categories of crime specific to its unique design. The cross border functionality and pseudonymous nature of cryptocurrencies fueled cybercrimes, also the design and development of hundreds of cryptocurrency project which are not fully vetted by experts have resulted in crypto specific cybercrimes which never existed. However, not all coins are targeted equally, factors such as popularity, privacy features, transaction speed plays a role in susceptibility of cryptocurrencies. Prior studies provide a foundational insight into different kinds of crimes perpetrated by criminal groups.

Vasek and Moore [1] analyzed scams targeting Bitcoin, including High Yield Investment Programs (HYIPs), mining investment scams, fraudulent wallet services, and scam exchanges. Hamrick et al. [2] measured the prevalence of pump-and-dump schemes in the cryptocurrency market, uncovering nearly 5,000 pump events over a six-month period.

The proliferation of ransomware has been closely linked to the rise of cryptocurrencies, which enable anonymous and efficient ransom payments. Kshetri and Voas [3] tracked the dramatic growth of ransomware incidents, noting an increase from a single known ransomware strain in 2012 to 193 by 2016. This growth was attributed to the ease of receiving payments via cryptocurrencies, which reduced the risks and complexities of traditional financial transactions. Enterprises, especially those managing critical data, were found to be more likely to pay ransoms when the demanded amounts were deemed affordable. Liao et al. provided a detailed case study of CryptoLocker [4], one of the earliest ransomware strains to adopt Bitcoin as its payment method. Their research identified 968 Bitcoin addresses associated with CryptoLocker, estimating its revenue at 1,128.40 BTC (approximately $310,472), with potential peaks exceeding $1.1 million. Additionally, the authors revealed connections to Bitcoin mixers such as *Bitcoin Fog*, exchanges like *BTC-e*, and other cybercrimes, including the Sheep Marketplace scam. Together, these studies underscore how the adoption of cryptocurrencies has facilitated the rapid growth and sophistication of ransomware attacks, enabling both widespread adoption and targeted extortion of enterprises.

Cable et al. [5] conducted an in-depth analysis of ransomware operations using blockchain data and novel heuristics. They identified $700 million in previously unreported

979-8-3315-8969-1/25/$31.00 © 2025 IEEE

ransomware payments, with the median ransom rising from $250,000 in 2019 to $2.5 million in 2022. The study also revealed that most ransom payments were laundered through mixers and high-risk exchanges. Zimba and Chishimba measured the economic impact of crypto ransomware attacks, focusing on their evolution, attack vectors, and financial consequences. Their findings highlighted a shift in ransomware targets from individuals to enterprises, leading to larger financial losses [6] .

Sextortion scams have evolved significantly in recent years, leveraging technological and financial innovations to target victims. Paquet-Clouston et al. [7] examined bulk sexual extortion email campaigns, where spammers demanded Bitcoin payments, generating an estimated $1.3 million in revenue over 11 months. Edwards and Hollely [8] expanded on this by analyzing over 23,000 reports of online sextortion collected over a decade. Their study highlighted the offenders' use of platforms like Facebook and Skype, with a recent shift towards Instagram. Payments in these cases were initially demanded through Western Union, but the methods have diversified in recent years, complicating enforcement efforts. Both studies emphasize the adaptive strategies employed by sextortion offenders, the increasing role of digital platforms and payment systems, and the challenges these trends pose for law enforcement and victim support systems.

Crimes in the decentralized finance (DeFi) sector have caused significant financial losses, totaling over $30 billion between 2017 and 2022, with one-third attributed to DeFi and the rest to centralized finance (CeFi) [9]. Carpentier-Desjardins et al. analyzed 1,048 DeFi-related crime events, categorizing attacks by their technical and human vulnerabilities. They found that 52.2% of incidents targeted DeFi actors, with protocol vulnerabilities accounting for the majority of damages (83%). DeFi actors also acted as perpetrators in 40.7% of incidents, primarily through rug pulls and market manipulation, although these caused smaller financial losses. The study highlighted the role of technical vulnerabilities, such as smart contract exploits, and human risks, emphasizing the need for improved cyber security measures and user awareness to mitigate these crimes.This are prime examples of new sort of crimes that gave rise to crypto specific crime which added fuel to e-crimes.

In this chapter, we delve into the analysis of cybercrime trends from 2018 to 2024, with a particular focus on the role of cryptocurrencies. The primary objective of this research is to examine how cryptocurrencies are utilized in cybercrime and to uncover the factors influencing the preference for one coin over another. Section II outlines the methodology for data collection, data cleanup and research questions based on the exploratory data analysis. Section IV then delves into statistical analysis with a series of regressions as a measure to substantiate our hypothesis.

II. Methodology

We compiled data on cryptocurrency-related crimes reported by individuals and enterprises from two primary sources: chainabuse.com (formerly bitcoinabuse.com) and the Crypto Defenders Alliance (CDA). The majority of the dataset, comprising **198,000** reports of attempted scams and crimes, was obtained from Chainabuse.com. These reports were well-structured, including timestamps, the cryptocurrency involved, crime categories, and detailed messages used to target victims. Most contributions to this dataset originated from Chainabuse.com.

The second data source, Crypto Defenders Alliance, is a Telegram channel with contributors from academia, cybersecurity experts, and data analysts affiliated with cryptocurrency exchanges and aggregators. From this channel, we scraped and analyzed approximately **3,000** messages containing crime reports. Unlike the Chainabuse.com dataset, the CDA reports featured a diverse range of cryptocurrencies, including less popular coins, which enriched our dataset with additional insights.

To ensure consistency, we standardized the data by categorizing reports into the same crime categories used by Chainabuse.com. Additionally, we grouped the crimes into two broad types: **Legacy Cybercrime** and **Cryptocurrency-Enabled Crimes**. This comprehensive approach allowed us to create a structured dataset to analyze the intersection of cybercrime and cryptocurrency as well as measure the relationships between different cryptocurrencies and types of cybercrime for based on popularity and other characteristics.

The Chainabuse dataset was classified was narrowly classified in to different types of crimes such as Airdrop, Fake Projects, Blackmail, Phishing, Pig Butchering etc II. On the other hand, the data from the telegram channel was unclassified into different types of crimes and scams. Hence, we identified the the uniqueness of the telegram group messages and found reports of Stolen Funds with wallet addresses. Sometimes, the chain name was mentioned and in a handful of cases only the wallet address was provided.

We decided to classify the Telegram channels messages into similar categories as defined by Chainabuse. Initially, we wanted to create a classification model. Due to the lack of consistent nature of the texts from the Telegram channel, we had to change strategy. Prior research has shown that LLMs can serve as high-performing text classifiers through prompt-based reasoning [10]) and that such models exhibit strong adaptability and reliability across diverse domains [11]. These results motivate the use of LLM-based classification methods in this study.

We employed a medium-sized model available through Ollama, selected for its balance between inference speed and classification capability, to assign each message to one of the 17 categories defined in the Chainabuse dataset. A structured prompt was designed to constrain the model to this predefined taxonomy and to assign the label *Unknown* when no category was sufficiently aligned. Through repeated rounds of prompt refinement on a randomly sampled subset of messages, we developed a stable and reliable prompt that produced consistent classifications on the validation samples.

The finalized prompt was then applied to the full dataset.

The resulting classifications demonstrated a high degree of accuracy, as confirmed through manual verification. A small subset of unusually long messages did not fully adhere to the expected behavior; in these cases, the model occasionally produced novel explanatory labels instead of selecting exclusively from the approved set. Nevertheless, the model's contextual reasoning in these instances could be mapped back to the existing Chainabuse categories, ensuring consistency across the dataset [12]. During this process of classification, we used a two-pronged approach to identify the coins mentioned in the dataset. The first preference was given to look for mentions of coin by its names and if address was mentioned, we used regular expressions of coin/token addresses to map them with actual coin.

After the dataset was classified into one of the seventeen Chainabuse categories (or assigned the label *Unknown*), we removed all messages labeled as *Unknown* to obtain a cleaner and more reliable corpus for subsequent analysis. We then excluded all rows for which no coin match could be identified, resulting in a dataset sufficiently curated for rigorous empirical work.

To introduce an additional analytical layer, we further classified each message into one of two higher-level crime typologies. We refer to these as **Legacy Cyber Crime** and **Crypto-Enabled Cyber Crime**.

Legacy Cyber Crime encompasses traditional online crimes in which cryptocurrency serves primarily as the medium of transaction. These activities existed prior to the advent of blockchain technology, but the pseudonymous, borderless nature of cryptocurrencies has made them increasingly attractive for operational execution. Examples include blackmail, ransomware, and sextortion/extortion.

Crypto-Enabled Cybercrime, by contrast, includes illicit activities that originate from the technical and economic structure of cryptocurrency ecosystems themselves. These crimes are native to blockchain environments and would not exist without the underlying technology. Examples include airdrop-related scams, smart-contract exploits, and other forms of protocol-level abuse.

This two-tiered classification framework allows us to distinguish between crimes that merely adopt cryptocurrency as a transactional tool and those that emerge endogenously from the cryptocurrency ecosystem.

A. Research Questions

We plan to investigate the following questions with the data gathered.

RQ1 *Is the popularity of coins correlated with the occurrence of crimes?*

RQ2 *Is the popularity of coins correlated with specific types of crimes?*

RQ3 *Is Ethereum more likely to be used in cryptocurrency specific crime?*

RQ4 *Are coins more likely to be used in crimes once they achieve unicorn status?*

RQ5 *Do bull and bear periods of Bitcoin influence the frequency and types of crimes?*

III. Data Analysis

Figure 1 illustrates the number of reported cybercrimes over time from 2018 to 2024. The blue line shows aggregated monthly reports collected from chainabuse.com and the orange line represents number of reported crime by crypto defender alliance which dates back to 2018. Overall the plot reflects domination of reports of crimes involving cryptocurrencies with an occasional dip in 2022 which can be attributed to disruption in reporting during the time frame.

In [13] Mukherjee and Moore defined crypto unicorns as coins/tokens which ever reached $1 Billion in market capitalization. We used the same methodology to flag coins as Unicorns as True or False. After labeling the coins mentioned in the dataset as Unicorns or Non-Unicorns we settled with 124 unique cryptocurrencies (Coins and Tokens) among which 54 of them are unicorns and 352 are non unicorns.

The empirical distribution of scam reports shows that Bitcoin and Ethereum overwhelmingly dominate illicit activity within the sample. Bitcoin alone represents approximately 76% of all reports, and together Bitcoin and Ethereum account for nearly 95% of the observed cases. Although Unicorn coins constitute a comparatively smaller portion of the market by count, they appear in roughly 98% of reported incidents, underscoring their disproportionate involvement relative to their representation in the ecosystem. This concentration of reported crime in high-visibility assets is consistent with theoretical expectations: widely adopted cryptocurrencies function as highly liquid, easily transferable instruments that attract both legitimate users and malicious actors seeking reach and anonymity. The observed pattern therefore provides strong empirical support for RQ1, indicating a robust positive association between a coin's market prominence and its likelihood of being implicated in reported criminal activity.

The comparison of crime categories between Unicorn and Non-Unicorn assets demonstrates an extremely uneven distribution of reported illicit activity. Across every category in the dataset, Unicorn coins exhibit substantially higher case counts, often by several orders of magnitude. For example, Blackmail, Phishing, Other, and Ransomware each exceed ten thousand reports among Unicorn coins, while the corresponding counts for Non-Unicorn assets remain in the low tens. This pattern appears consistently across both legacy cybercrime categories and crypto enabled scam types. The dominance of Unicorn assets in high volume categories reflects their much larger user bases and higher transaction liquidity, which create more opportunities for malicious actors to engage with victims and to operationalize fraudulent schemes at scale.

In categories that involve more complex technical or social engineering mechanisms, such as Hack, Airdrop, Rug Pull, Contract Exploit, and Fake Project, Unicorn coins again exhibit very high involvement relative to Non-Unicorn assets. The gap is especially pronounced in categories tied to crypto enabled activity where the infrastructure of large scale

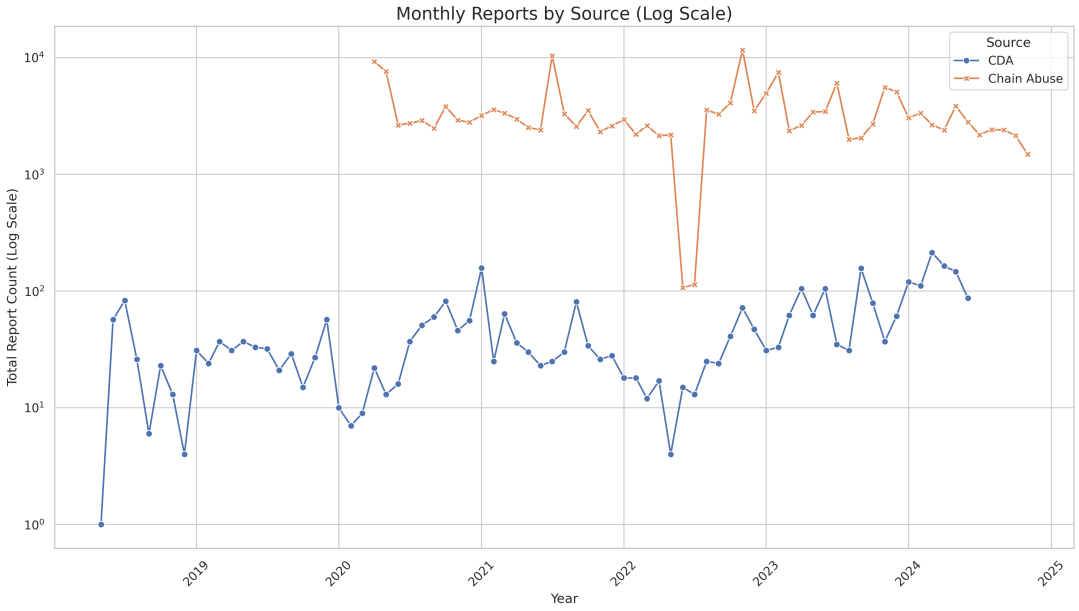

Fig. 1. Time series of reported crime (logarithmic scale)

smart contract ecosystems and high visibility token projects increases both the attack surface and the number of potential victims. The Non-Unicorn counts remain extremely small in comparison, which suggests that smaller or less visible assets rarely serve as primary vectors for large scale fraud.

Taken together, the bar plot provides strong evidence that Unicorn assets are disproportionately implicated in nearly every form of reported crypto-related crime. This is consistent with theoretical expectations that popular and highly capitalized coins attract increased criminal activity because they provide the liquidity, recognition, and broad exposure necessary for profitable illicit operations. The observed distribution strengthens the empirical support for RQ1, since Unicorn status is strongly correlated with both the frequency and the breadth of crime types reported in the dataset.

Table I and II shows the distribution of the crimes across different crime types and its relationship with different coins. The tables reflect counts, percentage and significance of the distribution of each crime types between two sets of groups Bitcoin-Ethereum and Unicorns (excluding Bitcoin and Ethereum)-Non Unicorns. Results in these tables lend support to RQ2.

Finally we seek to answer RQ5, whether the rate of criminal activity varies with the price of the two leading cryptocurrencies, BTC and ETH. We collected price data for Bitcoin and Ethereum, the two leading cryptocurrencies. Similar to stock markets, the cryptocurrency market experiences periods of highs and lows, commonly referred to as bull and bear markets. These periods are typically identified by comparing short-term and long-term rolling averages, such as 30-day and 90-day moving averages.

Using this methodology, we defined bull and bear periods for Bitcoin. To account for brief fluctuations, any period shorter than 60 days was merged with the preceding and following periods to create a continuous trend. For instance, a bear period lasting less than 60 days was combined with adjacent bull periods to form a single extended bull phase.

This approach allowed us to analyze whether market fluctuations, represented by these bull and bear periods, influence the frequency or nature of crimes associated with cryptocurrencies.

Figure 4 shows the bull and bear period of Bitcoin, where the light shaded green represents bull period and the light shaded area represents bear period. The blue line in the plot shows actual price of Bitcoin, The orange and green line represents 30 and 90 day rolling mean of bitcoin which we used to represent the bull and bear periods of bitcoin. The purple line shows number of crimes committed during the time line as reported by the telegram channel Crypto Defenders Alliance where as the sky blue line denotes the the number of reported crimes by chainabuse.com.

Upon further analysis, significant differences emerge in the types of crimes associated with the two dominant players in the cryptocurrency ecosystem. To test RQ4 Figure 3 highlights these distinctions. Phishing is more prevalent with Ethereum, as are other forms of hacking and exploits that often target vulnerabilities in the code bases of Ethereum-based tokens. In contrast, crimes such as blackmail and extortion are far more common with Bitcoin, highlighting its use in schemes where anonymity and wide adoption are key factors. These findings reflect the differing roles and technical characteristics of these cryptocurrencies in the broader cybercrime landscape.

Finally we seek to answer H5, whether the rate of criminal activity varies with the price of the two leading cryptocur-

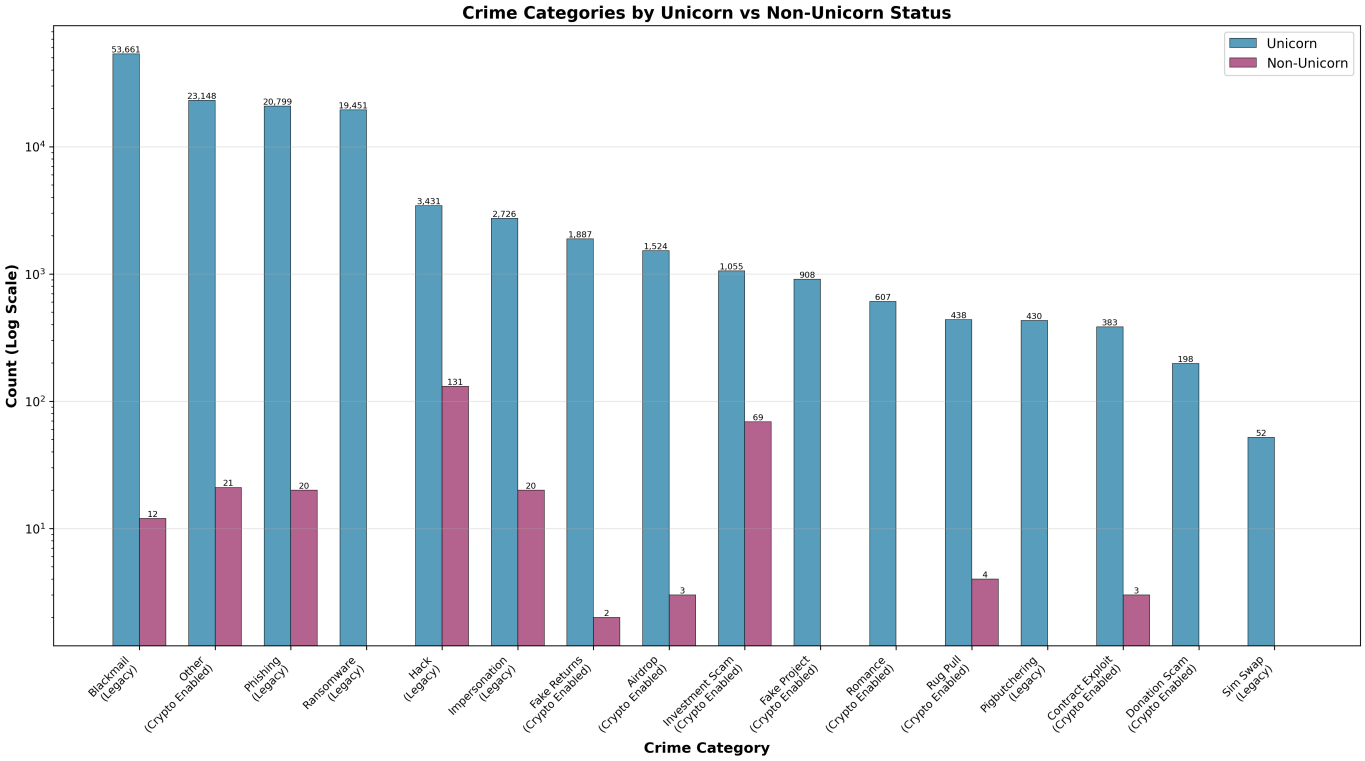

Fig. 2. Bar Plot representing crime using unicorns vs non unicorn

TABLE I
CRIME TYPE BY BTC, ETH, UNICORN (EXCL. BTC AND ETH), AND NON-UNICORN: **CRYPTO DEFENDERS ALLIANCE TELEGRAM CHANNEL**

Crime Type	BTC			ETH			Other Unicorns			Non-Unicorn		
	#	%	Sig	#	%	Sig	#	%	Sig	#	%	Sig
Impersonation	16	30.77%	-	11	21.15%		7	13.46%		18	34.62%	+
Other	63	41.18%	-	61	39.87%	+	5	3.27%	-	24	15.69%	
Blackmail	31	50.00%		5	8.06%	-	2	3.23%		24	38.71%	+
Hack	631	32.33%	-	760	38.93%	+	206	10.55%	+	355	18.19%	+
Investment Scam	902	80.46%	+	84	7.49%	-	53	4.73%	-	82	7.31%	-
Phishing	0	0.00%		0	0.00%		0	0.00%		1	100.00%	+
Pigbutchering	0	0.00%		3	100.00%	+	0	0.00%		0	0.00%	
Romance	1	100.00%		0	0.00%		0	0.00%		0	0.00%	
Total	1,644	49.15%		924	27.62%		273	8.16%		504	15.07%	

rencies, BTC and ETH. We collected price data for Bitcoin and Ethereum, the two leading cryptocurrencies. Similar to stock markets, the cryptocurrency market experiences periods of highs and lows, commonly referred to as bull and bear markets. These periods are typically identified by comparing short-term and long-term rolling averages, such as 30-day and 90-day moving averages.

Using this methodology, we defined bull and bear periods for Bitcoin. To account for brief fluctuations, any period shorter than 60 days was merged with the preceding and following periods to create a continuous trend. For instance, a bear period lasting less than 60 days was combined with adjacent bull periods to form a single extended bull phase.

This approach allowed us to analyze whether market fluctuations, represented by these bull and bear periods, influence the frequency or nature of crimes associated with cryptocurrencies.

Figure 4 shows the bull and bear period of Bitcoin, where the light shaded green represents bull period and the light shaded area represents bear period. The blue line in the plot shows actual price of Bitcoin, The orange and green line represents 30 and 90 day rolling mean of bitcoin which we used to represent the bull and bear periods of bitcoin. The purple line shows number of crimes committed during the time line as reported by the telegram channel Crypto Defenders Alliance where as the sky blue line denotes the the number of

TABLE II
CRIME TYPE BY BTC, ETH, UNICORN (EXCLUDING BTC AND ETH), AND NON-UNICORN: **CHAINABUSE**

Crime Type	BTC			ETH			Other Unicorns			Non-Unicorn		
	#	%	Sig	#	%	Sig	#	%	Sig	#	%	Sig
Blackmail	52,858	98.60%	+	95	0.18%	-	653	1.22%	-	5	0.01%	-
Other	22,352	97.12%	+	487	2.12%	-	132	0.57%	-	45	0.20%	-
Phishing	815	3.91%	-	19,355	92.97%	+	318	1.53%	-	330	1.59%	+
Ransomware	19,399	99.73%	+	29	0.15%	-	21	0.11%	-	2	0.01%	-
Impersonation	1,075	39.90%	-	1,429	53.04%	+	161	5.98%	+	29	1.08%	+
Fake Returns	814	43.09%	-	825	43.67%	+	206	10.91%	+	44	2.33%	+
Hack	326	20.25%	-	978	60.75%	+	191	11.86%	+	115	7.14%	+
Airdrop	24	1.57%	-	392	25.67%	+	1,077	70.53%	+	34	2.23%	+
Fake Project	208	22.91%	-	525	57.82%	+	135	14.87%	+	40	4.41%	+
Romance	359	59.24%	-	175	28.88%	+	70	11.55%	+	2	0.33%	
Rug Pull	108	24.43%	-	216	48.87%	+	64	14.48%	+	54	12.22%	+
Pigbutchering	125	29.27%	-	238	55.74%	+	62	14.52%	+	2	0.47%	
Contract Exploit	22	5.70%	-	233	60.36%	+	41	10.62%	+	90	23.32%	+
Donation Scam	138	69.70%	-	40	20.20%		17	8.59%	+	3	1.52%	
Sim Swap	13	25.00%	-	32	61.54%	+	4	7.69%	+	3	5.77%	+
Investment Scam	2	66.67%		1	33.33%		0	0.00%		0	0.00%	
Total	98,638	77.28%		25,050	19.63%		3,152	2.47%		798	0.63%	

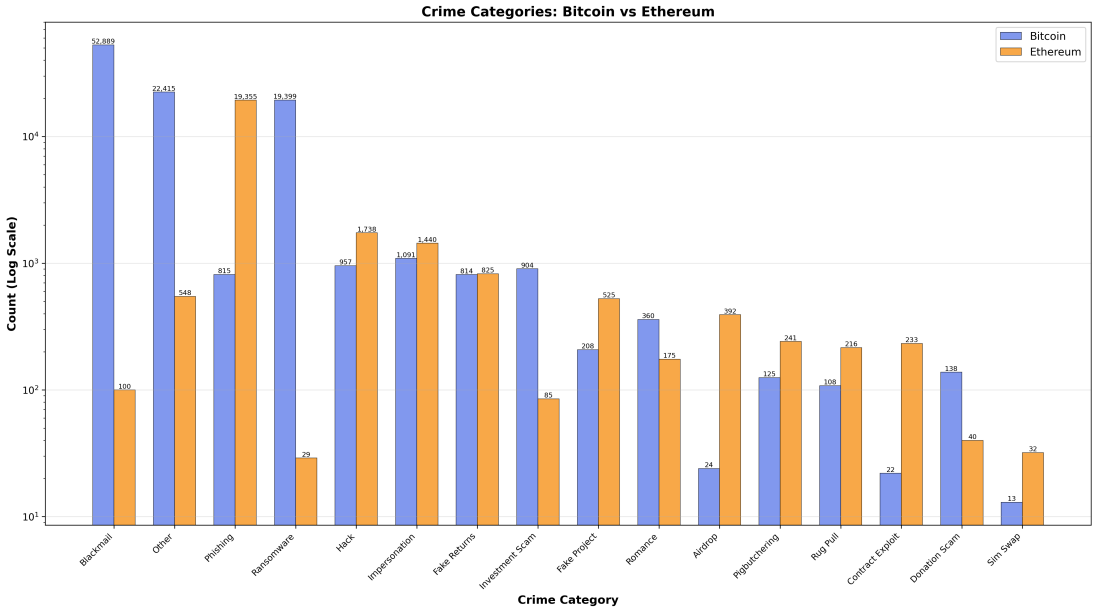

Fig. 3. Bar plot showing different types of crimes using just Bitcoin and Ethereum

reported crimes by chainabuse.com.

IV. REGRESSION ANALYSIS

We ran a series of regressions, linear as well as logistic, depending on the research questions. This section primarily focuses on explaining the regression analysis for all the research questions as mentioned in II. Regression tables for the some hypotheses are mentioned in this section, some regression tables can be found in the Appendix section of this paper.

A. Evaluating RQ2 and RQ3

We estimated a set of logistic regression models to evaluate RQ2, which proposes that certain coins exhibit distinct patterns of involvement in cryptocurrency enabled crime relative to legacy cybercrime. The dependent variable classifies each incident as either a cryptocurrency enabled offense (coded as 1 in the `Crime Label`) or a legacy cybercrime (coded as 0). The four principal specifications emphasize different coin level indicators in order to isolate whether particular assets are systematically associated with the mechanisms of crypto

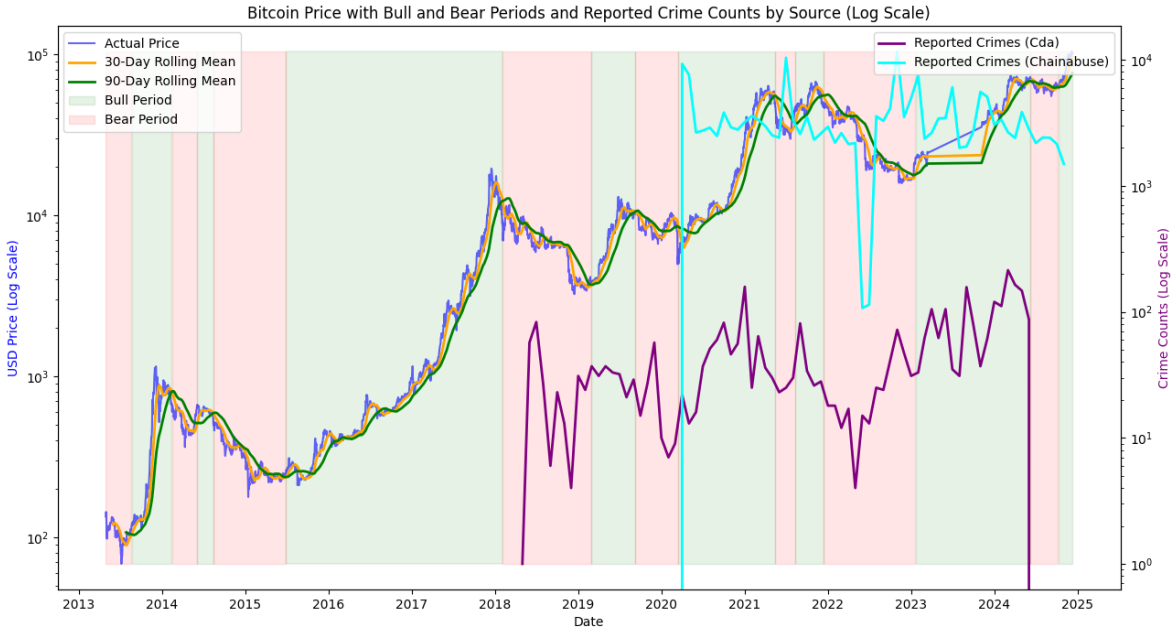

Fig. 4. Bitcoin Bull and bear periods and scam counts.

TABLE III
LOGISTIC REGRESSION: CRYPTO ENABLED (=1) VS LEGACY (=0)

Variable	**Model 1**	**Model 2**	**Model 3**	**Model 4**
Intercept	-0.58***	-1.51***	-1.04***	-0.07*
	(0.12)	(0.01)	(0.01)	(0.03)
Unicorn [True]	-0.60***			
	(0.12)			
Bitcoin (vs. others)		0.41***		
		(0.02)		
Ethereum (vs. others)			-0.89***	
			(0.02)	
BTC-ETH Group				-1.17***
				(0.03)
N	130,983	130,983	130,983	130,983
McFadden R^2	0.000	0.005	0.016	0.010
AIC	1425.41	1419.29	1402.57	1411.91
BIC	1425.98	1419.85	1402.13	1411.48
Log-Likelihood	-712.71	-709.64	-701.78	-705.95

native criminal activity.

Model 1 introduces only an indicator for whether the report involves a unicorn coin. The estimated coefficient is negative and highly significant, and the implied odds ratio of approximately 0.55 indicates that unicorn related incidents are less likely to be classified as cryptocurrency enabled crimes. In this reduced form model reports mentioning unicorn assets fall more often within categories that resemble traditional online crime rather than the distinctive modalities of blockchain based exploitation.

Model 2 isolates Bitcoin. The coefficient on *Bitcoin (vs. others)* is positive and strongly significant, yielding an odds ratio close to 1.51. This pattern suggests that Bitcoin related reports are more frequently associated with cryptocurrency enabled crime than reports involving any other coin. This is consistent with Bitcoin's longstanding role within early illicit marketplaces and its prominence in the historical development of ransomware, extortion, and similar crypto native behaviors.

Model 3 focuses exclusively on Ethereum. The coefficient on *Ethereum (vs. others)* is sharply negative, with an estimated odds ratio of about 0.41. In contrast to Bitcoin, incidents involving Ethereum are substantially less likely to be coded as cryptocurrency enabled. The implication is that Ethereum related reports in this dataset exhibit characteristics more aligned with legacy forms of cyber offending rather than the mechanisms commonly associated with cryptocurrency specific exploitation. Among the four models, Model 3 also attains the lowest AIC and BIC values, indicating comparatively better fit when distinguishing Ethereum from other coins.

Model 4 introduces a combined indicator for Bitcoin and Ethereum. Here the coefficient remains negative and significant, and the implied odds ratio of roughly 0.31 demonstrates that reports involving either of the two dominant assets are less likely to be classified as cryptocurrency enabled crimes relative to reports involving other coins. This specification highlights that once the two largest ecosystems are grouped together their collective pattern resembles the Ethereum specific result in Model 3 rather than the Bitcoin specific pattern in Model 2.

Across all four models the McFadden R^2 statistics remain small, ranging from zero to approximately 0.016. These

values demonstrate that although the identity of the coin is statistically associated with the probability of an incident being labeled as cryptocurrency enabled, coin characteristics alone explain only a modest fraction of the overall variation. The results therefore reveal meaningful but limited structural relationships, reflecting the heterogeneous and multifactorial nature of cyber and crypto-enabled crime.This also suggests that the models capture directional associations rather than providing a comprehensive explanation of crime type classification as the R^2 statistics is very low.

TABLE IV
LOGISTIC REGRESSION RESULTS: PREDICTING CRYPTO-SPECIFIC CRIMES

Variables	**Model 5**	**Model 6**	**Model 7**
Intercept	-0.5845***	-0.5845***	-0.3537**
	(0.1236)	(0.1236)	(0.1378)
Unicorn	-0.6016***	-0.6776***	0.4097
	(0.1237)	(0.1238)	(0.2778)
Other Unicorn		1.1602***	1.1786***
		(0.0251)	(0.0423)
Alleged Sec Securities Tag			-0.1432
			(0.3195)
Bnb Chain Tag			0.0321
			(0.1813)
Defi Tag			-1.0126**
			(0.4603)
Injective Ecosystem Tag			0.3384**
			(0.1431)
Layer 1 Tag			-1.2678***
			(0.1440)
Medium Of Exchange Tag			-2.8371***
			(0.1565)
Mineable Tag			-1.1746***
			(0.2579)
Payments Tag			0.7668***
			(0.2515)
Platform Tag			0.0797
			(0.2508)
Smart Contracts Tag			-1.1251***
			(0.1698)
AIC	142,579.41	140,565.89	136,998.01
Observations	130,983	130,983	130,983
Pseudo R^2	0.000	0.014	0.039

Note: Standard errors in parentheses. $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$.

Another way of examining RQ2 specifically is to look at the characteristics of coins that could make it more or less attractive to particular crime types. Table IV shows a series of logistic regression that include Unicorn status plus categorical variables capturing attributes of the coins themselves. We adopt tags in the same manner used in Chapter 3. Model 5 confirms that Unicorns coins are less likely to be involved in crypto-specific crimes, suggesting market leaders are more often used in legacy cybercrime. Model 6 separates Bitcoin and Ethereum from other Unicorns to isolate their individual effects. The results indicate that the negative association observed between Unicorn status and crypto-specific crimes is largely attributable to these two coins. When these two are excluded, the remaining unicorn coins exhibit a strong positive relationship with scam activity, suggesting that many high-cap altcoins are more frequently implicated in crypto-specific crimes. In the end, Model 7 incorporates tags of coins as derived from associated "functionalities". Coins that are serving as platforms or layer-1 chains or part of the injective eco-system are more likely prone to crypto-specific crime/scam. In contrast, coins that are mineable and flagged by SEC as securities are more associated with legacy cybercrime.

Moreover, Table VI presents a more detailed examination using the full set of unicorn coins and tokens. This specification is designed to test whether ecosystem level attributes of unicorn assets are systematically associated with both the incidence and intensity of crime. The table contains four regression models, each targeting a distinct crime related outcome and thereby enabling a multi dimensional evaluation of the hypothesis.

In Models 8 and 9, the dependent variable is a binary indicator, *Has Scam Report*, which equals 1 if a given unicorn coin has at least one documented scam report and 0 otherwise. Of the 176 Unicorns, 21 had at least one scam report, while 155 did not have any. These models therefore capture the extensive margin of criminal involvement and allow us to assess whether particular ecosystem tags, or exposure to legacy cybercrime, predict whether a coin appears in scam data at all. Model 8 includes only `# Legacy Crime` as an independent variable in order to establish a baseline relationship, while Model 9 introduces a richer set of ecosystem attributes to determine whether the functionalities of a unicorn coin are more informative predictors of scam presence.

Model 10 shifts from a binary outcome to a continuous dependent variable: the total number of reported crimes associated with each unicorn asset. This specification examines the intensity of illicit activity rather than the mere presence of a scam report, enabling assessment of how ecosystem characteristics scale with broader criminal exposure.

Model 11 uses a similar count based structure but restricts the dependent variable to the number of cryptocurrency enabled crimes, defined as offenses that depend directly on blockchain mechanics such as smart contract exploitation, DeFi manipulation, or on chain theft. This final model isolates the crypto-native dimension of illicit activity and tests whether the same ecosystem attributes that predict overall crime also explain variation in explicitly blockchain dependent criminal behavior.

Across Models 9 through 11, the independent variables consist of the ten most prominent ecosystem classifications for unicorn coins, including tags related to regulatory categorization, technological architecture, functional role, and protocol level capability. These indicators operationalize the hypothesis that structural attributes of unicorn ecosystems shape their criminological profile. The inclusion of `# legacy crime` in the binary models further allows us to evaluate whether prior involvement in Legacy cybercrime contributes independently to scam visibility.

This regression design thus provides a structured approach to validating the hypothesis RQ2 and RQ3. The criminological landscape of unicorn assets is shaped by their underlying technological and functional ecosystems, then ecosystem tags

should consistently predict both the likelihood of scam involvement and the volume of criminal activity associated with each coin. The usage of tags used by the popular coins like BTC and ETH not only proves Hypothesis but also shows a relationship between technology and usability of the coins' feature as a key factor when it comes to selecting a coin for illicit activity.

It is worth noting that Models 9–11 have much higher R^2 variables than Models 1–8. This inidcates that the coin categories provide a lot of explanatory power when it comes to whether those coins are utilized by scammers. Categories like Platform, DeFi, BNB Chain and Alleged SEC Security experience more scams.

B. Evaluating RQ4

RQ4 investigates the temporal relationship between a coin's market capitalization and its association with crypto-specific crime. Specifically, it examines whether becoming a Unicorn increases the likelihood that the coin will be used in scams and illicit schemes that are unique to the cryptocurrency ecosystem (e.g., rug pulls, Ponzi contracts, exit scams), as opposed to traditional cybercrimes (e.g., phishing, ransomware, blackmail).

The underlying hypothesis is twofold. On one hand, unicorn coins enjoy greater visibility, liquidity, and user adoption, potentially making them more attractive targets for sophisticated actors conducting large scale fraud. On the other hand, their increased scrutiny by regulators, exchanges, and users may deter their use in novel, high-risk scams. By testing whether crypto-specific crimes increase or decrease after a coin attains unicorn status, this analysis aims to disentangle these competing dynamics.

To conduct this test, we constructed a binary variable **After Becoming Unicorn** indicating whether the crime report occurred after the coin reached unicorn status. A logistic regression was then performed with `Crime Label` (1 for crypto-specific crime, 0 for traditional cybercrime) as the dependent variable and After Becoming Unicorn as the main independent variable.

The results indicate a statistically significant and negative relationship between unicorn status and crypto-enabled crime. This suggests that crimes occurring *after* a coin achieves unicorn status are less likely to be crypto-specific. The odds of a crime being crypto-specific drop by nearly 79% after a coin becomes a unicorn, controlling for other factors. This implies that mature coins become vehicles for more established forms of cybercrime (e.g., ransomware payments in Bitcoin).

C. Evaluating RQ5

We finally investigate whether scams are more likely to increase based on the current status of the crypocurrency market. To investigate this research question, we developed a panel logistic regression model using monthly observations across the sample period. We first constructed a dataset that identified bull and bear periods separately for Bitcoin and Ethereum based on their market performance. For each month, we calculated the total number of reported crimes by aggregating incidents from multiple data platforms. These included both Legacy cybercrimes and cryptocurrency-specific offenses.

In the initial model specification, we tested whether the current bull or bear status of Bitcoin and Ethereum had any statistically significant association with the number of reported crimes. Model 1 includes only the Bitcoin bull-period indicator. The estimated coefficient is positive and statistically significant (1,260.52), suggesting that months classified as Bitcoin bull periods are associated with higher total reported crime relative to non-bull months. Substantively, this indicates that sharp Bitcoin price increases coincide with increased criminal activity.The R-squared value of 0.08 indicates modest explanatory power, which is expected given the simplicity of this specification. In Model 2 we added Ethereum bull periods alongside Bitcoin bull periods. Once Ethereum conditions are included, the coefficient on Bitcoin bull periods becomes negative and statistically insignificant, while the Ethereum bull-period coefficient becomes large, positive, and highly significant (approximately 2,954).This shift suggests that the apparent Bitcoin effect observed in Model 1 was masking a stronger underlying relationship driven by Ethereum's bull cycles. The improvement in model fit (R-squared increasing to 0.20) demonstrates that Ethereum bull dynamics explain a meaningful portion of the variation in total reported crime.

In Model 3, we added 1 month lagged variables for both Bitcoin and Ethereum.The lagged Bitcoin bull-period coefficient is negative and statistically insignificant. In contrast, the lagged Ethereum bull-period coefficient remains large (3,042), positive, and highly significant. This pattern implied that criminal activity appears to rise in the month following substantial Ethereum appreciation. This lag may reflect operational delays in scam execution, reporting timelines, or the time victims need to engage with fraudulent schemes that proliferate during bull cycles. The model fit improves slightly (R-squared = 0.23), consistent with lag structures capturing meaningful temporal dynamics.

The last model adds both the lagged 1 month lag and 2 month lag indicators for Bitcoin and Ethereum Bull periods. The Bitcoin coefficients across all lags are small or negative and statistically insignificant, implying no robust relationship between Bitcoin bull cycles and total crime once Ethereum dynamics are accounted for. By contrast, Ethereum coefficients remain consistently positive, and the two-month lag is statistically significant at the ten percent level (3,046.71). This reinforces the persistent and extended influence of Ethereum market expansions on crime activity. The R-squared rises to 0.27, which is the highest of all four models, but the adjusted R-squared drops. This means the extra lagged variables help the model fit the data slightly better overall, but once we account for how many new variables were added, they do not contribute enough useful information. In other words, adding more lags improves the model only a little.

TABLE V
LOGISTIC REGRESSION: EFFECT OF POST-UNICORN STATUS ON CRIME LABEL

Variable	**Coef.**	**Std. Err.**	**z**	**P > —z—**	**95% CI**
Intercept	-0.684***	0.119	-5.766	0.000	[-0.916, -0.451]
After Becoming Unicorn	-0.502***	0.119	-4.229	0.000	[-0.735, -0.269]
Model Information					
Dependent variable	Crime Label				
Model type	Logistic regression (logit)				
Estimation method	Maximum likelihood				
Observations	130,983				
Residual degrees of freedom	130,981				
Pseudo R^2	0.00012				
Log-likelihood	-71,290				
Null log-likelihood	-71,298				
Likelihood ratio p-value	4.16e-05				
Convergence	Yes				

Note: *** p < 0.01, ** p < 0.05, * p < 0.1. The indicator *After Becoming Unicorn* equals 1 if the reported crime occurred after the cryptocurrency achieved unicorn status, defined as a market capitalization exceeding $1 billion.

V. CONCLUDING REMARKS

Cybercriminals are spoiled for choice in deciding which cryptocurrencies to use in carrying out cybercriminal activities. In examining over 131,000 scam reports spanning more than six years, we confirm that popular coins are used the most, led by Bitcoin and Ethereum. We do find evidence that other coins are also utilized. Moreover, we distinguish between legacy cybercrimes such as ransomware payments and cryptocurrency-enabled cybercrime such as rug pulls and investment scams. In this case, we observe considerable variation. Ethereum is used more often for crypto-enabled crimes, and other coins are also utilized based upon their technological attributes.

For law enforcement actors seeking to disrupt crypto-fueled cybercrimes, we can share the encouraging message that they should focus their efforts on the top coins. They need not be discouraged by the continued growth in newly minted coins, as they are not utilized extensively in the scams we observed.

ACKNOWLEDGMENTS

We gratefully acknowledge support from the US National Science Foundation Award No. 1714291.

REFERENCES

[1] M. Vasek and T. Moore, "There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams," in *Financial Cryptography and Data Security*, R. Böhme and T. Okamoto, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, vol. 8975, pp. 44–61.

[2] J. Hamrick, F. Rouhi, A. Mukherjee, A. Feder, N. Gandal, T. Moore, and M. Vasek, "The Economics of Cryptocurrency Pump and Dump Schemes," *SSRN Electronic Journal*, 2018. [Online]. Available: https://www.ssrn.com/abstract=3303365

[3] N. Kshetri and J. Voas, "Do Crypto-Currencies Fuel Ransomware?" *IT Professional*, vol. 19, no. 5, pp. 11–15, 2017, conference Name: IT Professional. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8057721

[4] K. Liao, Z. Zhao, A. Doupe, and G.-J. Ahn, "Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin," in *2016 APWG Symposium on Electronic Crime Research (eCrime)*. Toronto, ON, Canada: IEEE, Jun. 2016, pp. 1–13. [Online]. Available: http://ieeexplore.ieee.org/document/7487938/

[5] J. Cable, I. W. Gray, and D. McCoy, "Showing the Receipts: Understanding the Modern Ransomware Ecosystem," Aug. 2024, arXiv:2408.15420 [cs]. [Online]. Available: http://arxiv.org/abs/2408.15420

[6] A. Zimba and M. Chishimba, "On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems," *European Journal for Security Research*, vol. 4, no. 1, pp. 3–31, Apr. 2019. [Online]. Available: https://doi.org/10.1007/s41125-019-00039-8

[7] M. Paquet-Clouston, M. Romiti, B. Haslhofer, and T. Charvat, "Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, ser. AFT '19. New York, NY, USA: Association for Computing Machinery, Oct. 2019, pp. 76–88. [Online]. Available: https://doi.org/10.1145/3318041.3355466

[8] M. Edwards and N. M. Hollely, "Online sextortion: Characteristics of offences from a decade of community reporting," *Journal of Economic Criminology*, vol. 2, p. 100038, Dec. 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2949791423000386

[9] C. Carpentier and J.-M. Suret, "The survival and success of Canadian penny stock IPOs," *Small Business Economics*, vol. 36, no. 1, pp. 101–121, Jan. 2011. [Online]. Available: https://doi.org/10.1007/s11187-009-9190-x

[10] X. Sun, X. Li, J. Li, F. Wu, S. Guo, T. Zhang, and G. Wang, "Text Classification via Large Language Models," Oct. 2023, arXiv:2305.08377 [cs]. [Online]. Available: http://arxiv.org/abs/2305.08377

[11] Z. Wang, Y. Pang, Y. Lin, and X. Zhu, "Adaptable and Reliable Text Classification using Large Language Models," Dec. 2024, arXiv:2405.10523 [cs]. [Online]. Available: http://arxiv.org/abs/2405.10523

[12] M. AI, "mistral:7b-instruct-v0.2-q4_k_m," model available via Ollama.

Accessed 2025-12-07. [Online]. Available: https://ollama.com/library/mistral:7b-instruct-v0.2-q4_K_M

[13] A. Mukherjee and T. Moore, "Beyond the Hype: Empirical Evaluation of Cryptocurrency Unicorn Success," in *Proceedings of the Annual Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences, 2025, iSSN: 2572-6862. [Online]. Available: https://hdl.handle.net/10125/109521

APPENDIX

TABLE VI
REGRESSION ANALYSIS OF UNICORN COIN TAGS ACROSS MULTIPLE CRIME OUTCOMES

Variable	**Model 8**	**Model 9**	**Model 10**	**Model 11**
Dependent Variable	has scam report (T)	has scam report (T)	# Crime	# Crypto Enabled Crime
Constant	0.1685***	0.0181.	6.59	6.59
	(0.0284)	(0.0104)	(19.93)	(19.93)
Alleged SEC Security	–	0.3041***	482.92***	482.92***
		(0.0689)	(132.01)	(132.01)
BNB Chain	–	0.1388.	568.67***	568.67***
		(0.0783)	(150.05)	(150.05)
DeFi	–	0.0744	1469.96***	1469.96***
		(0.1019)	(195.32)	(195.32)
Injective Ecosystem	–	0.4054***	-1136.40***	-1136.40***
		(0.0819)	(156.84)	(156.84)
Layer 1	–	0.1242*	-319.41**	-319.41**
		(0.0614)	(117.54)	(117.54)
# Legacy Crime	1.35e-05**	9.90e-06***	1.33***	0.3284***
	(4.79e-06)	(1.94e-06)	(0.0037)	(0.0037)
Medium of Exchange	–	0.6723***	88.00	88.00
		(0.0635)	(121.63)	(121.63)
Mineable	–	0.1900*	-193.76	-193.76
		(0.0743)	(142.27)	(142.27)
Payments	–	0.0857	-108.85	-108.85
		(0.0748)	(143.24)	(143.24)
Platform	–	0.2797***	641.48***	641.48***
		(0.0695)	(133.17)	(133.17)
Smart Contracts	–	0.4001***	-668.78***	-668.78***
		(0.0546)	(104.56)	(104.56)
N	176	176	176	176
R^2	0.0436	0.8974	0.9991	0.9849
Adjusted R^2	0.0381	0.8905	0.9990	0.9839
F-statistic	7.9342	130.3817	16471.9244	973.4174
F p-value	0.0054	<0.0001	<0.0001	<0.0001
AIC	155.90	-216.97	2443.42	2443.42
BIC	162.24	-178.92	2481.47	2481.47

Note: Standard errors are reported in parentheses below coefficients. *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, . $p < 0.1$.

TABLE VII
REGRESSION RESULTS ACROSS DIFFERENT MODELS OF TOTAL COMBINED CRIME

	Total Reported Crime			
	Model 1	**Model 2**	**Model 3**	**Model 4**
Intercept	1115.51***	1115.51***	1060.33***	1051.04***
	(323.34)	(302.88)	(298.25)	(307.94)
Bitcoin Bull Period	1260.52**	-1085.65		-662.41
	(492.87)	(825.51)		(1160.76)
Bitcoin Bull Period (1 month lag)			-1027.19	-111.14
			(812.90)	(1510.14)
Bitcoin Bull Period (2 month lag)				-651.91
				(1209.01)
Ethereum Bull Period		2954.44***		886.69
		(861.75)		(1667.63)
Ethereum Bull Period (1 month lag)			3042.26***	-362.43
			(848.60)	(2135.66)
Ethereum Bull Period (2 month lag)				3046.71*
				(1552.39)
R-squared	0.08	0.20	0.23	0.27
Adjusted R-squared	0.07	0.18	0.21	0.21

Note: Standard errors are reported in parentheses below coefficients. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.