Technology, Cybersecurity, and Cryptocurrency Returns

Abstract

Are cryptocurrencies mere speculative bubbles, or do their returns reflect the quality of their underlying technology? To address this question, we examine crypto technological flaws leading to cybersecurity exposures. Technological flaws in the underlying technology of cryptos, their publicly visible source code on GitHub, are bugs documented by developers to be fixed later. We find that one flaw predicts a 7 basis points decrease in the coin's daily return. A portfolio that longs no-flaw coins and shorts high-flaw ones, which we term the "cybersecurity factor," earns 30 basis points daily. Our results demonstrate that cryptocurrency returns reflect the quality of their underlying technology.

Keywords: Technology, Cryptocurrency, Cybersecurity, GitHub
JEL Classification: G10, G12, G14

Disclosure Statement

We have not received any outside research support and have no conflicts of interest to disclose.

1. Introduction

Many argue that investing in the cryptocurrency (crypto) market is like playing roulette because cryptos do not have an intrinsic value. Therefore, they argue that searching for crypto return predictability is futile and meaningless. The counter-argument is that crypto returns reflect the quality of the underlying blockchain technology, which may become valuable in the future (Y. Liu, Tsyvinski, & Wu, 2022). How does the market incorporate the technology in crypto returns? As a digital asset, cryptocurrencies can be stolen due to flaws in the blockchain technology. Indeed, as of 2023 over $6 billion worth of crypto has been stolen by hackers who exploit flaws in the underlying technology (see **Table 1**). Investors understand this cybersecurity risk and impound the quality of the technology, i.e., hack resistance, into crypto returns (Biais, Bisiere, Bouvard, Casamatta, & Menkveld, 2023; Pagnotta, 2022). This paper empirically examines whether crypto returns can be predicted by the cybersecurity risk arising from the technology. Our results address the question of whether crypto returns are random draws or a market mechanism reflecting the underlying blockchain technology.

We begin by measuring the flaws in the technology underlying cryptocurrencies. Most cryptocurrencies are open-source projects with public source code housed on GitHub, a platform that allows developers to create, store, manage, and share their code. A public timeline of the versioning history, GH Archive, has terabytes of records including the evolution of the code base and all interactions between developers, with precise timestamps at the second level. An important type of these interactions, called "Issues," are initiated by anyone who finds a problem with the project, ranging from vague documentation to bugs in the source

code. Issues describe the nature of the bug and are effectively a call for help from other developers to fix the problem.

We match 1,414 coins with market capitalization above $1 million to their corresponding GitHub repositories. Using a dictionary-based approach, we flag Issues that identify bugs in the source code. We then count the number of bug-identifying Issues for a coin each day or week to form a *Technology Flaws* measure that captures cybersecurity exposure in coins on a daily or weekly level, respectively. Unsurprisingly, Issues that identify bugs in the source code, which represent problems that can lead to hacks, are rare. 98% of coin-days and 94% of coin-weeks have zero *Technology Flaws*. On the other hand, a significant portion (roughly one-third) of coins have had technology flaws during the sample period, as 458 coins have ever had positive *Technology Flaws*.

We find that the number of *Technology Flaws* predicts future coin returns. One new technology flaw in the past day and week predicts a decrease in subsequent daily and weekly returns by 7 and 13 basis points, respectively. The predictability is slightly weaker but remains robust in a subsample of coins with large market capitalization and stronger with small coins. The effect also remains robust at the intensive margin – the estimates are similar if we only use observations with positive *Technology Flaws*. These results ensure that the effect is not driven by only small coins or a large fraction of zeros in the main independent variable.

To understand the magnitude of the return predictability in the cross-section, we form a portfolio that longs coins with zero lagged *Technology Flaws* and shorts coins in the top decile based on lagged *Technology Flaws*. On average, coins in the short leg of the portfolio have 13.4 *Technology Flaws* per day. We term this portfolio the "Cybersecurity Factor" in

cryptocurrencies. The daily and weekly Cybersecurity Factors earn 30 and 88 basis points per period, respectively. While we do not claim this portfolio to be a profitable trading strategy (as it ignores costly rebalancing), the economically large magnitude of its long-short returns suggests significant return predictability in the cross-section. The magnitude is large but it is in line with the findings in the literature. For comparison, the weekly market, size, and momentum factors developed by Y. Liu et al. (2022) earn 167, 353, and 99 basis points, respectively. In addition, the cybersecurity factor is not explained by these three factors. We double-sort coins first by size or past return and then by *Technology Flaws*, and find that the long-short portfolios earn similar returns in each size or past-return tercile. We also find that the cybersecurity factor earns an alpha of roughly 60 basis points against a 3-factor model including the crypto market, size, and momentum factors.

This paper makes several contributions. First, we address the important question – whether cryptocurrencies are mere speculative bubbles or financial assets that represent something economically meaningful. The conventional wisdom is that cryptocurrencies do not have an intrinsic value and therefore are irrational bubbles with no return predictability. We challenge this view by demonstrating that flaws in the technology underlying cryptocurrencies predict crypto returns. Our results support the view that cryptocurrency returns reflect the quality of the underlying blockchain technology.

Second, many existing theoretical studies on cryptocurrencies model a "hacking risk" in crypto returns (Athey, Parashkevov, Sarukkai, & Xia, 2016; Biais et al., 2023; Pagnotta, 2022). To the best of our knowledge, we are the first to provide direct evidence that technological flaws and cybersecurity risks are priced in crypto returns. In related work, Y. Liu, Sheng, and Wang (2024) also study how technological sophistication affects cryptocurrency

pricing. They find that coins with more sophisticated technology claimed in their Initial Coin Offering (ICO) documents have a higher listing price at ICO. Our results suggest that investors value technology beyond the initial offering and pinpoint cybersecurity risk as the economic channel between technology and crypto returns.

The methodology of our measure also opens new avenues for future research in crypto characteristics and returns. To date, most studies in this literature only capture cross-sectional variation in crypto characteristics (e.g., technological innovation) using ICO white papers (Bourveau, De George, Ellahie, & Macciocchi, 2022; Dittmar & Wu, 2019; Howell, Niessner, & Yermack, 2020; Y. Liu et al., 2024). Our methodology can capture time-varying crypto characteristics in both the code base and developer interactions at any frequency, which can then be used to study broad crypto-related outcomes.

2. Related Literature

This paper contributes to a growing literature on cryptocurrency return predictability (Bouri, Lau, Lucey, & Roubaud, 2019; Y. Liu & Tsyvinski, 2021; Y. Liu et al., 2022). Many studies justify crypto return predictability with the existence of fundamental value derived from the utility of the token (Cong, Li, & Wang, 2021; Prat, Danos, & Marcassa, 2019; Sockin & Xiong, 2020). We remain agnostic on the existence of the fundamental value of cryptos and take a different approach. As long as the price of cryptocurrencies is not exactly zero, their returns are predicted by the quality of the underlying technology because cybersecurity exposure affects investors' return from holding crypto assets (Biais et al., 2023; Pagnotta, 2022). Our approach is similar to several studies focused on ICOs (Bourveau et al., 2022;

Dittmar & Wu, 2019; Howell et al., 2020; Y. Liu et al., 2024) but with higher resolution of the quality of technology over time.

We also add to the growing literature that studies how cybersecurity risk affects capital markets. Most studies examine how cybersecurity affects firms through the productivity or reputation of the firm (Akey, Lewellen, Liskovich, & Schiller, 2023; Crosignani, Macchiavelli, & Silva, 2023; Kamiya, Kang, Kim, Milidonis, & Stulz, 2021). This effect is then reflected in stock returns depending on how the firm discloses cybersecurity exposures (Amir, Levi, & Livne, 2018) and how markets understand them (T. Liu, Makridis, & Galinkin, 2023). Our study has a different and much more direct mechanism – the coin itself (analogous to the stock of the firms) can be stolen due to cybersecurity exposure, affecting how much investors value the coin (Biais et al., 2023; Pagnotta, 2022). Our Cybersecurity Factor has an important distinction from the cybersecurity risk premium in the literature. Florackis, Louca, Michaely, and Weber (2023) and Jiang, Khanna, Yang, and Zhou (2024) document that firms with higher cybersecurity risk earn higher returns. The positive risk premium suggests that the cybersecurity risk captured by the textual analysis in their studies is instantly fully priced in the market. We find that technology flaws in cryptocurrencies' code base predict a lower future return. Our results suggest that the market does not fully price the cybersecurity exposure in crypto returns, consistent with the empirical observations in T. Liu et al. (2023).

3. Data and Variables

We describe the data and variable construction in this section. We first provide an overview of GitHub, a developer platform that houses repositories (repos) for open-source projects including most cryptocurrencies. The computer code underlying these cryptocurrencies' technology is stored in GitHub repos. We then explain our methodology to capture technology flaws in cryptocurrency GitHub repos that could lead to cybersecurity exposures. Lastly, we describe the crypto trading and return data and the sample construction process.

3.1. Open Source Projects and GitHub

Most cryptocurrencies are open-source projects with code repositories housed on GitHub (Reibel, Yousaf, & Meiklejohn, 2018), a platform that stores computer code and facilitates the ongoing development of projects. GitHub is popular among developers due to its transparent versioning system. All changes to the code and interactions between developers since the project's inception are documented systematically and are viewable to the public.

The code of a project, for a cryptocurrency or not, changes and improves to add new features or fix bugs. This process can be initiated by the developers or the users. In either case, the common practice is to open an "*Issue*" which documents features to be added or bugs to be fixed. An Issue is effectively a call for help from all coders on GitHub to work on the feature upgrade or fix the bug. Subsequently, a "*Pull Request*" is created when someone proposes a change to the code, though not all Pull Requests are accompanied by a preceding Issue. Pull Requests are reviewed by project developers who have "admin privilege" and can approve or reject the proposed change. Approving a Pull Request creates a "*Push Event*"

which implements the change into the project's code base.[1]

3.2. Measuring Technological Flaws

We construct a measure of *Technology Flaws* that captures cryptocurrencies' cybersecurity exposure due to bugs in the underlying code. We obtain *Technology Flaws* by counting the number of Issues that identify bugs. Sometimes, Issues ask for feature updates or report minor problems such as vague documentation. These Issues are not expected to lead to cybersecurity exposures. Therefore, we apply a dictionary-based filter and only count Issues that contain keywords that indicate cybersecurity exposures.[2] We create the *Technology Flaws* measure at the coin-day and coin-week levels.

Table 2 presents the summary statistics of the *Technology Flaws* measure. We see that on average 0.03 and 0.22 bugs are reported for a given coin-day and coin-week, respectively. *Technology Flaws* is right-skewed. Unsurprisingly, Issues reporting bugs are rare, as 98% of coin-days and 94% of coin-weeks have zero *Technology Flaws*. On the other hand, a significant portion (roughly one-third) of coins have had technology flaws during the sample period as 458 coins have ever had positive *Technology Flaws*.

Insert **Table 2** About Here

[1] We only describe a simplified process with limited types of GitHub events relevant to our study. We refer readers to GitHub's REST API documentation for a detailed description of the workflow and full set of event types at https://docs.github.com/en/rest/using-the-rest-api/github-event-types.

[2] The keywords are bug, wrong, mistake, problem, incorrect, issue, bad, flaw, risk, break, breach, compromise, attack, malware, phishing, ransomware, hijack, intrusion, backdoor, and tamper. We iterate over different dictionaries that contain either broad keywords such as "bug" and "problem" or specific keywords such as "malware, phishing, ransomware, hijack, and backdoor". All empirical results remain qualitatively similar.

3.2.1. Examples of GitHub Issues and Cybersecurity Exposure

We provide several concrete examples of Issues to demonstrate how technology flaws can lead to cybersecurity vulnerabilities. The following is an Issue initiated by username TippyFlitsUK on the filecoin-project project's lotus repository on November 6, 2020, at 22:59:19 GMT:

> *"I have lost a large amount of money this week primarily as a result of snapshot sync irregularities and deal completion failures. We are very much still in the early stages of Filecoin mainnet and there will obviously be bugs and obstacles to navigate. As early miners we fully accept this but it is also crucial to remember that we are now dealing with real money and livelihoods at a time of great economic instability. I for one am sincerely grateful to the developer team for their considerable efforts and excellent communication in these early days but the fact remains that bugs are an inevitability. I would respectfully like to propose that a contingency fund be established that will allow miners to apply for reimbursement in the unfortunate event of unavoidable financial loss."*[3]

This example shows how the crypto community uses Issues as a means to identify problems and call for help. It also highlights that technology flaws can lead to monetary losses.

Issues sometimes provide specific details about bugs in the code even for prominent coins. The following is an Issue initiated by username nopara73 on the Bitcoin project's Bitcoin repository on October 2, 2018, at 00:34:21 GMT:

> *"At the time of writing approximately 86.51% of the Bitcoin network is vulnera-*

[3]See the original post at https://github.com/filecoin-project/lotus/issues/4759.

ble to CVE-20181-7144. It has been two weeks since 0.16.3 was tagged with the vulnerability fix. I believe the occasional breaking of user space is one of the contributing factor to this situation where things can be improved. I believe marking an RPC method deprecated and removing it within a few new release may not be sufficient, since most developers do not code directly against Bitcoin Core, rather I they take an RPC client implementation, written by someone else in their respective programming language. These projects tend to be unmaintained, incomplete, sometimes even buggy. These developers, in such an environment may consider upgrading their Core nodes risky. I know it is hard living together with legacy code and immature API design decisions, but a "never break the user space" policy may result in a more secure and stable environment."[4]

These examples demonstrate how GitHub Issues capture flaws in cryptocurrencies' underlying technology and how *Technology Flaws* can lead to cybersecurity exposure and monetary losses.

3.2.2. Discussion of GitHub Issues and Cybersecurity Exposure

We address two questions concerning the validity of using GitHub Issues to measure technology flaws leading to cybersecurity exposures.

First, how much should we trust the quality of these "bug reports" in GitHub Issues? Are these bug reports really informative considering that people who report the bugs might not have been the ones who wrote the code? There are two pieces of evidence that these Issues systematically capture technology flaws. First, relying on users to report bugs is widely

[4]See the original post at https://github.com/bitcoin/bitcoin/issues/14363.

used by the software development industry to improve software quality and security. For example, Ethereum, the second largest cryptocurrency by market capitalization as of 2023, and Coinbase, the largest US-based crypto exchange as of 2023, have bug bounty programs that incentivize outsiders to find and report bugs.[5] Second, even though it is impossible to systematically link every Issue with the corresponding subsequent Pull Request that fixes the bug, we observe a positive correlation between the number of Issues and future Pull Requests. These observations support that GitHub Issues systematically report bugs in the code underlying cryptocurrencies.

Second, do these bugs lead to serious cybersecurity failures, or are they merely inconveniences for users? Some bugs do lead to serious cybersecurity failures and, eventually, massive monetary loss. For example, in the Wormhole Network exploit, the bug allowed the hacker to "mint" 120,000 wrapped ETH (worth $325 million) out of thin air. While the bug was identified and fixed in the code base, it did not go live before the exploit happened.[6] More importantly, it is difficult to assess the severity of most bugs. A bug that looks innocuous can have unexpected grave consequences. For example, an NFT project accidentally locked $34 million worth of ETH in the smart contract simply because the code did not properly add index numbers to the assets in the smart contract, which would seem

[5]Ethereum's bug bounty program rewards up to $250,000 and can be viewed at https://ethereum.org/en/bug-bounty/. Coinbase's bug bounty program can be viewed at https://hackerone.com/coinbase. See additional background on the inception of Coinbase's bounty program based on outsiders' bug reports at https://www.coinbase.com/blog/retrospective-recent-coinbase-bug-bounty-award.

[6]See the Solana blockchain record of the hacker "minting" 120,000 wETH at https://solscan.io/tx/2zCz2GgSoSS68eNJENWrYB48dMM1zmH8SZkgYneVDv2G4gRsVfwu5rNXtK5BKFxn7fSqX9BvrBc1rdPAeBEcD6Es. See the bug fix in Wormhole Network's code base that would have prevented the exploit at https://github.com/wormhole-foundation/wormhole/commit/7edbbd3677ee6ca681be8722a607bc576a3912c8#diff-0d27d8889edd071b86d3f3299276882d97613ad6ab3b0b6412ae4ebf3ccd6370L92-R101. See more details about this exploit at https://www.theverge.com/2022/2/3/22916111/wormhole-hack-github-error-325-million-theft-ethereum-solana.

almost trivial ex-ante.[7] Therefore, the bugs reported in GitHub Issues could lead to serious cybersecurity exposures beyond mere inconvenience.

To summarize, since GitHub Issues report bugs that could lead to cybersecurity exposures and monetary losses, we develop the measure of technology flaws using these Issues and examine whether it predicts crypto returns in subsequent analyses.

3.3. Crypto Trading Data and Sample Construction

Finally, we obtain daily and weekly crypto trading data, including trading volume, market capitalization, and price, from CoinGecko for 14,909 coins. We require that a coin enters the sample after having a $1 million market capitalization and never leaves the sample afterward unless its trading stops altogether. We then manually match coins to their corresponding GitHub repository and discard ones that we could not match. The final sample consists of 1,414 cryptocurrencies from 2014 to 2023. Summary statistics for daily and weekly returns, trading volumes, and market capitalizations are presented in **Table 2**. The average daily and weekly returns for the sample coins are 0.36% and 1.73%, respectively. The market cap of a coin can fall below $1 million and stay in the sample after falling below the initial $1 million threshold to enter.

4. Technological Flaws and Crypto Returns

In this section, we examine the relation between *Technology Flaws* and future crypto returns. We show that *Technology Flaws* negatively predict subsequent crypto returns and that the

[7] See more for details about the incident of the Aku Ethereum NFT launch at https://decrypt.co/98530/aku-ethereum-nft-launch-ends-with-34m-locked-in-flawed-smart-contract.

negative predictability is robust.

4.1. Technology Flaws and Crypto Returns

We examine whether *Technology Flaws* predict future crypto returns with the following equation:

$$\text{Return}_{i,t} = \beta_0 + \beta_1 \textit{Technology Flaws}_{i,t-1} + \boldsymbol{\beta} \boldsymbol{X}_{i,t} + \zeta_t + \phi_i + \epsilon_{i,t}, \tag{1}$$

where i indexes coin and t indexes day or week. $\boldsymbol{X}_{i,t}$ is a vector of control variables including the log of trading volume and the log of market cap. ζ_t represents day or week fixed effects that sweep out factors that apply to all coins in the market such as the overall sentiment in the crypto market. ϕ_i is coin fixed effects that sweep out coin-specific time-invariant characteristics such as how prominent a coin is. Returns are expressed in percentage points and *Technology Flaws* is expressed as a count. **Table 3** reports the results.

Insert **Table 3** About Here

Table 3 shows that *Technology Flaws* negatively predict future crypto returns. Panels A and B report daily and weekly results, respectively. In both panels, columns (1) to (4) show specifications with different fixed effects. Column (1) estimates **Equation 1** without any fixed effects. Columns (2) and (3) add time and coin fixed effects, respectively. Column (4) adds both time and coin fixed effects. We see that *Technology Flaws* negatively predicts future crypto returns consistently across all specifications with statistical significance at the

1% level and similar economic magnitudes. We focus on the most saturated specification with the most conservative estimates in column (4). If one additional Issue reporting a bug is posted on GitHub, the corresponding coin sees a decrease of 7 (13) basis points in the return over the next day (week). The effect of *Technology Flaws* on crypto returns is economically large – an additional *Technology Flaw* reduces the return in the next day (week) by 19% (8%) of the unconditional mean return in the sample.

4.2. Robustness of the Return Predictability

We address two concerns about the negative predictability of *Technology Flaws* on crypto returns. First, we show that the predictability is not just concentrated in small coins. A large empirical asset pricing literature suggests that return predictability is more likely to be concentrated in illiquid assets with small market caps (Asparouhova, Bessembinder, & Kalcheva, 2010; Chu, Hirshleifer, & Ma, 2020). We examine whether *Technology Flaws* predict returns only for small coins by estimating Equation 1 separately for small and large terciles based on lagged market capitalization. **Table 4** reports the results.

Insert **Table 4** About Here

We see that the return predictability is stronger in small coins but remains robust in large coins. Columns (1) to (4) show the estimates for small coins. On average, these estimates are three to five times larger compared to the baseline results in **Table 3**, except for column (4) in the weekly panel. Columns (5) to (8) show the estimates for large coins. The point estimates are similar to those in the baseline results and remain statistically significant. As

a result, we conclude that the negative return predictability is not entirely driven by small coins and remains robust with large coins.

Second, we show that the results are not driven by a large number of zeros in the independent variable, *Technology Flaws*. Since over 98% of coin-days and 94% of coin-weeks have zero *Technology Flaws*, the extremely right-skewed distribution may give rise to spurious results. To address this concern, we estimate Equation 1 using only observations with positive *Technology Flaws*. This estimate allows us to obtain the intensive margin of the effect.

Insert **Table 5** About Here

Table 5 shows that the results remain qualitatively similar in the positive *Technology Flaws* subsample. The results alleviate the concern that the predictability is driven by the right-skewed distribution of *Technology Flaws* with a large fraction of zeros.

5. Cybersecurity Factor

In this section, we examine the cross-sectional predictability of *Technology Flaws* on returns by forming a long-short portfolio based on *Technology Flaws*. We term this portfolio the "Cybersecurity Factor." We show that the Cybersecurity Factor is profitable and robust to double sorting against size and momentum. Finally, we show that the Cybersecurity Factor earns a meaningful alpha against existing factors in the cryptocurrency return predictability literature.

5.1. Cybersecurity Factor Returns

Following Y. Liu et al. (2022), we develop a Cybersecurity Factor at both daily and weekly levels. In each period, the portfolio longs coins with zero lagged *Technology Flaws* and shorts coins with lagged *Technology Flaws* in the top decile.[8] On average, coins in the short leg have 10.9 *Technology Flaws* per day. **Table 6** shows the average return of the Cybersecurity Factor on daily and weekly levels.

Insert **Table 6** About Here

Table 6 shows that the Cybersecurity Factor generates significant returns. On average, the long-short portfolio earns a daily and weekly return of 30 bps and 88 bps, respectively. These returns are statistically and economically significant. Holding the Cybersecurity Factor and rebalancing weekly from 2017 to 2023 earns a cumulative return of roughly 294%. This number may seem high but is in line with the literature. We plot the Cybersecurity Factor along with the crypto market, size, and momentum factors developed by Y. Liu et al. (2022) in Figure 1. The crypto market, size, and momentum factors earn a cumulative return of roughly 544%, 1,149%, and 323% over the same period. Similar to the argument in Y. Liu et al. (2022), while the Cybersecurity Factor is highly profitable on paper (with annualized Sharpe ratios of 2.31 and 1.19 at the daily and weekly levels, respectively), it does not account for transaction costs from frequent rebalancing. But importantly, the high

[8] When the 90th percentile of *Technology Flaws* is zero for a day or week, there are less than 10% of coins with positive *Technology Flaws* during that period. We handle this situation in two ways. For the results we report in the paper, we skip days and weeks when more than 90% of the coins have a zero *Technology Flaw*. Alternatively, in untabulated results, we short coins with zero lagged *Technology Flaws* and long coins with positive lagged *Technology Flaws*. These results are qualitatively similar.

profitability on paper suggests a strong cross-sectional return predictability of *Technology Flaws*.

Insert **Figure 1** About Here

5.2. Double Sorts on Size and Momentum

A potential concern is that the Cybersecurity Factor may be effectively sorting on coin size if size and *Technology Flaws* are correlated. In addition, it may also sort on past returns if there is any persistence in cryptocurrency returns. To address these concerns, we double-sort coins into size or past return terciles and then by *Technology Flaws* at the weekly level. **Table 7** presents the results. Panels A and B report returns of the portfolios double-sorted first on size and past returns, respectively.

Insert **Table 7** About Here

We see that the Cybersecurity Factor remains robust after conditioning on size and past returns. Panel A shows that the cross-sectional predictability is stronger in large coins. The long-short return is statistically insignificant for small coins but remains economically large. Panel B shows that the long-short return is higher among coins with low past returns. Similarly, even though the return is statistically insignificant for coins with high past returns, it remains economically significant.

5.3. Cybersecurity Factor and Existing Factors

Lastly, we explicitly contrast our Cybersecurity Factor against the existing crypto factors of market, size, and momentum (Y. Liu et al., 2022). We estimate time series regressions at the weekly level to obtain the alpha of the Cybersecurity Factor against existing factors.[9] The results are presented in **Table 8**.

Insert **Table 8** About Here

We see that the Cybersecurity Factor is not subsumed by the existing factors and earns a statistically and economically significant alpha. The results show that our long-short portfolio captures the cybersecurity exposure stemming from technology flaws that are not explained by known cryptocurrency factors.

6. Return Predictability and Crypto Hacks

In this section, we examine large crypto hacks as of 2023 to provide additional evidence on how cybersecurity risk and technology flaws affect crypto returns. Specifically, we focus on hacks that resulted in more than $100 million worth of crypto assets being stolen. **Table 1** reports the hacks with their dates, amount stolen, and amount recovered as of 2023. We interpret these hacks as shocks to the saliency of cybersecurity risks, which plausibly increase overall investor attention to cybersecurity risk. We examine the return predictability

[9]We thank Yukun Liu for making the crypto factors available on his website. Due to data availability, the sample period is from 2017 to 2023.

of *Technology Flaws* on crypto returns immediately after large hacks with the following equation:

$$\text{Return}_{i,t} = \beta_0 + \beta_1 \text{Technology Flaws}_{i,t-1} + \beta_2 \text{Technology Flaws}_{i,t-1} \times \text{Hack}_{t-1} + \boldsymbol{\beta} \boldsymbol{X}_{i,t} + \phi_i + \zeta_t + \epsilon_{i,t},$$

where Hack_{t-1} is an indicator variable that equals 1 if a hack reported in **Table 1** occurred the previous day. β_1 captures the baseline effect of *Technology Flaws* on crypto returns. The coefficient of the interaction term, β_2, captures the additional effect of *Technology Flaws* on crypto returns after major hacks. **Table 9** reports the results.

Insert **Table 9** About Here

Table 9 column 1 shows that *Technology Flaws* predict a bigger price drop following a hack. One *Technology Flaw* predicts a 7 basis point decrease in crypto prices in normal times and predicts a 21 basis point decrease the day after the hack. The heightened market reaction is consistent with the idea that cybersecurity risk is more salient to investors following a major hack. One potential concern with our categorization of hacks is that some hacks are conducted by "white-hat" hackers who stress-test the system and later return what they were able to hack. For robustness, we repeat the analysis using hacks with no subsequent recoveries in column 2. We see that the results are qualitatively similar. The return drop predicted by *Technology Flaws* post these no-recovery hacks is 35 basis points compared to 21 basis points. This result is consistent with the idea that a hack with zero subsequent

recoveries is potentially perceived as more severe and salient at the time of the hack.

Finally, worth mentioning is that these major hacks result from exploits of exchanges (e.g., Mt. Gox, Coincheck), networks (e.g., Poly, Wormhole), or wallets (e.g., Atomic Wallet). In other words, these hacks are market-wide events caused by security vulnerabilities that are not related to a particular cryptocurrency. Our *Technology Flaw* measure in individual cryptos is not meant to predict these market-wide infrastructure failures. However, these hacks allow us to pinpoint the economic mechanism – that cybersecurity risk is less salient in normal times and more salient after major hacks.

7. Conclusion

In this paper, we provide empirical evidence that cryptocurrency returns are not mere random draws, but instead reflect the underlying quality of the blockchain technology. By constructing a high-frequency measure of *Technology Flaws* from GitHub data, we show that these flaws in cryptocurrencies' code bases related to cybersecurity vulnerabilities predict lower future returns for cryptocurrencies. Our findings challenge the common perception that cryptocurrencies have unpredictable and completely random returns due to their lack of intrinsic values. The Cybersecurity Factor demonstrates the importance of technological quality and cybersecurity exposure as key drivers of returns of digital assets.

References

Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2023). Hacking corporate reputations. *Working Paper*.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? evidence from capital markets. *Review of Accounting Studies*, *23*, 1177–1206.

Asparouhova, E., Bessembinder, H., & Kalcheva, I. (2010). Liquidity biases in asset pricing tests. *Journal of Financial Economics*, *96*(2), 215–237.

Athey, S., Parashkevov, I., Sarukkai, V., & Xia, J. (2016). Bitcoin pricing, adoption, and usage: Theory and evidence. *Working paper*.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., & Menkveld, A. J. (2023). Equilibrium bitcoin pricing. *Journal of Finance*, *78*(2), 967–1014.

Bouri, E., Lau, C. K. M., Lucey, B., & Roubaud, D. (2019). Trading volume and the predictability of return and volatility in the cryptocurrency market. *Finance Research Letters*, *29*, 340–346.

Bourveau, T., De George, E. T., Ellahie, A., & Macciocchi, D. (2022). The role of disclosure and information intermediaries in an unregulated capital market: evidence from initial coin offerings. *Journal of Accounting Research*, *60*(1), 129–167.

Chu, Y., Hirshleifer, D., & Ma, L. (2020). The causal effect of limits to arbitrage on asset pricing anomalies. *Journal of Finance*, *75*(5), 2631–2672.

Cong, L. W., Li, Y., & Wang, N. (2021). Tokenomics: Dynamic adoption and valuation. *Review of Financial Studies*, *34*(3), 1105–1155.

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432–448.

Dittmar, R. F., & Wu, D. A. (2019). Initial coin offerings hyped and dehyped: An empirical examination. *Working paper*.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *Review of Financial Studies*, *36*(1), 351–407.

Howell, S. T., Niessner, M., & Yermack, D. (2020). Initial coin offerings: Financing growth

with cryptocurrency token sales. *Review of Financial Studies*, *33*(9), 3925–3974.

Jiang, H., Khanna, N., Yang, Q., & Zhou, J. (2024). The cyber risk premium. *Management Science*.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749.

Liu, T., Makridis, C., & Galinkin, E. (2023). Do financial markets understand cybersecurity: Evidence from a direct measure of firm network vulnerabilities. *Working Paper*.

Liu, Y., Sheng, J., & Wang, W. (2024). How Do Investors Value Technology in Cryptocurrency? Evidence from Textual Analysis. *Working paper*.

Liu, Y., & Tsyvinski, A. (2021). Risks and returns of cryptocurrency. *Review of Financial Studies*, *34*(6), 2689–2727.

Liu, Y., Tsyvinski, A., & Wu, X. (2022). Common risk factors in cryptocurrency. *Journal of Finance*, *77*(2), 1133–1177.

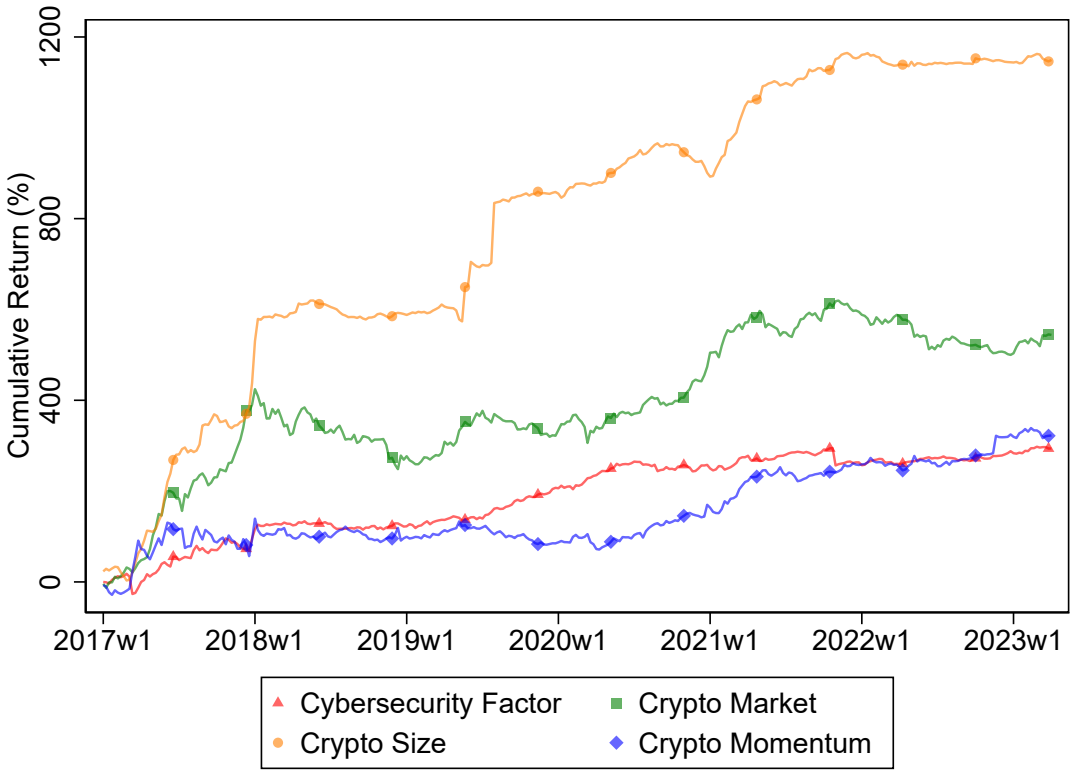
Pagnotta, E. S. (2022). Decentralizing money: Bitcoin prices and blockchain security. *Review of Financial Studies*, *35*(2), 866–907.

Prat, J., Danos, V., & Marcassa, S. (2019). Fundamental pricing of utility tokens. *Working paper*.

Reibel, P., Yousaf, H., & Meiklejohn, S. (2018). Why is a Ravencoin like a Tokendesk? An exploration of code diversity in the cryptocurrency landscape. *Working Paper*.

Sockin, M., & Xiong, W. (2020). A model of cryptocurrencies. *Working paper*.

Figure 1. Cybersecurity Factor Cumulative Return



The figure plots the cumulative return (without compounding) of the cybersecurity factor along with the crypto market, size, and momentum factors from Y. Liu et al. (2022).

Table 1
List of Crypto Hacks

This table reports all crypto hacks that resulted in $100 million or more stolen from 2014 to 2023. The data is collected from media reports, blockchain transaction records, and announcements from hacked exchanges. The hacked amount is the total dollar value of the crypto stolen by hackers. The recovered amount is the loss recovered through either hackers returning the stolen assets or the platform compensating investors, as of 2023. The cumulative hacked amount does not consider the recovered amount.

Hacks	Date	Hacked Amount ($ Millions)	Cumulative Hacked Amount ($ Millions)	Recovered Amount ($ Millions)
Mt. Gox	Feb 24, 2014	473	473	0
Parity	Nov 08, 2017	155	628	0
Coincheck	Jan 26, 2018	534	1,162	534
BitGrail	Feb 10, 2018	146	1,308	0
Gate.io	Apr 21, 2018	230	1,538	0
KuCoin	Sep 25, 2020	280	1,818	280
Poly Network	Aug 10, 2021	602	2,420	602
Cream Finance	Oct 27, 2021	130	2,550	0
Boy X Highspeed	Oct 30, 2021	139	2,689	0
BitMart Exchange	Dec 04, 2021	196	2,885	0
Vulcan Forged	Dec 12, 2021	140	3,025	0
Wormhole	Feb 02, 2022	326	3,351	326
Ronin	Mar 29, 2022	625	3,976	155
Beanstalk	Apr 18, 2022	181	4,157	0
Maiar DEX	Jun 05, 2022	113	4,270	113
Nomad	Aug 01, 2022	190	4,460	36
Wintermute	Sep 20, 2022	160	4,620	0
BSC Token Hub	Oct 06, 2022	586	5,206	459
BonqDAO	Feb 02, 2023	120	5,326	0
Euler Finance	Mar 13, 2023	196	5,522	177
Atomic Wallet	Jun 04, 2023	115	5,637	1
Multichain	Jul 06, 2023	231	5,868	0
Mixin Network	Sep 23, 2023	142	6,010	0

Table 2
Summary Statistics

This table presents summary statistics of key variables at the daily and weekly levels. *Technology Flaws* is the count of issue events that contain at least one of the keywords specified in the content filter. Returns are the daily or weekly percentage returns for crypto i at time t. Trading volume and market cap are expressed in millions of dollars for crypto i at time t. The sample contains 1,414 unique coins from 2013 to 2023.

	Mean	StdDev	p10	Median	p90	N
Daily						
Technology Flaws (#)	0.03	0.30	0.00	0.00	0.00	1,605,737
Returns (%)	0.36	10.43	-8.70	-0.15	8.94	1605737
Volume ($ millions)	21.76	111.12	0.00	0.13	14.65	1,605,717
Market Cap ($ millions)	200.54	920.03	0.10	5.98	211.48	1,605,588
Weekly						
Technology Flaws (#)	0.22	1.54	0.00	0.00	0.00	231,568
Returns (%)	1.73	26.14	-21.55	-1.33	24.65	230,146
Volume ($ millions)	150.99	761.69	0.00	0.97	110.57	231,568
Market Cap ($ millions)	198.67	915.76	0.09	5.79	208.48	231,558

Table 3
Technological Flaws and Cryptocurrency Returns

The table presents the results of the following regression:

$$\text{Return}_{i,t} = \beta_0 + \beta_1 \text{Technology Flaws}_{i,t-1} + \boldsymbol{\beta} \boldsymbol{X}_{i,t} + \phi_i + \zeta_t + \epsilon_{i,t},$$

where $\text{Return}_{i,t}$ is the return for crypto i on date t in percentage points, $\text{Technology Flaws}_{i,t}$ is the number of bug reports for crypto i on date t, and $\boldsymbol{X}_{i,t}$ is a vector of control variables including the log of trading volume and the log of market cap. ζ and ϕ are time and coin fixed effects, respectively. In the daily (weekly) specification, ζ represents date (week) fixed effects. Panel A presents daily results, while Panel B presents weekly results. Robust standard errors clustered at the coin level are reported in parentheses. *, **, and *** indicate significance at the 10%, 5%, and 1% levels, respectively.

Panel A: Daily

	(1)	(2)	(3)	(4)
Technology Flaws	-0.11***	-0.11***	-0.12***	-0.07***
	(-5.13)	(-5.15)	(-4.58)	(-2.78)
ln(Market Cap)	0.02	0.01	0.10***	0.24***
	(1.31)	(0.79)	(3.65)	(6.96)
ln(Volume)	0.01	0.01	0.15***	0.17***
	(0.57)	(0.48)	(8.35)	(8.70)
Coin FE	No	No	Yes	Yes
Date FE	No	Yes	No	Yes
Adjusted R-squared	0.000	0.124	0.003	0.128
Observations	1,492,295	1,492,295	1,492,290	1,492,290

Panel B: Weekly

	(1)	(2)	(3)	(4)
Technology Flaws	-0.16***	-0.14***	-0.24***	-0.13***
	(-3.83)	(-4.10)	(-4.49)	(-3.10)
ln(Market Cap)	0.63***	0.57***	1.32***	1.61***
	(10.10)	(9.15)	(10.40)	(9.62)
ln(Volume)	-0.24***	-0.25***	0.08	0.15**
	(-5.13)	(-5.39)	(1.23)	(2.08)
Coin FE	No	No	Yes	Yes
Week FE	No	Yes	No	Yes
Adjusted R-squared	0.002	0.180	0.008	0.186
Observations	214,558	214,558	214,548	214,548

Table 4
Technological Flaws and Cryptocurrency Returns by Coin Size

The table repeats the analyses in **Table 3** but estimates the effect in subsamples of terciles based on the lagged coin market cap. Robust standard errors clustered at the coin level are reported in parentheses. *, **, and *** indicate significance at the 10%, 5%, and 1% levels, respectively.

Panel A: Daily

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Small				Large			
Technology Flaws	-0.40***	-0.37**	-0.35	-0.21	-0.13***	-0.12***	-0.12***	-0.06**
	(-3.03)	(-2.14)	(-1.61)	(-1.06)	(-5.44)	(-4.85)	(-4.00)	(-2.03)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Coin FE	No	No	Yes	Yes	No	No	Yes	Yes
Date FE	No	Yes	No	Yes	No	Yes	No	Yes
Adjusted R-squared	0.004	0.067	0.010	0.078	0.004	0.302	0.009	0.310
Observations	494,967	494,967	494,948	494,948	498,135	498,134	498,112	498,111

Panel B: Weekly

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Small				Large			
Technology Flaws	-0.34***	-0.20*	-0.57***	-0.07	-0.18***	-0.18***	-0.27***	-0.13*
	(0.118)	(0.108)	(0.170)	(0.182)	(0.044)	(0.045)	(0.067)	(0.072)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Coin FE	No	No	Yes	Yes	No	No	Yes	Yes
Week FE	No	Yes	No	Yes	No	Yes	No	Yes
Adjusted R-squared	0.014	0.129	0.028	0.147	0.009	0.326	0.019	0.344
Observations	71,636	71,636	71,596	71,596	71,333	71,333	71,292	71,292

Table 5
Technological Flaws and Cryptocurrency Returns with Positive Technology Flaws

The table repeats the analyses in **Table 3** but use only coin-days or coin-weeks with positive $TechnologyFlaws_{t-1}$ for estimation. Robust standard errors clustered at the coin level are reported in parentheses. *, **, and *** indicate significance at the 10%, 5%, and 1% levels, respectively.

Panel A: Daily

	(1)	(2)	(3)	(4)
Technology Flaws	-0.08**	-0.04	-0.14***	-0.10***
	(0.03)	(0.02)	(0.03)	(0.03)
Controls	Yes	Yes	Yes	Yes
Coin FE	No	No	Yes	Yes
Date FE	No	Yes	No	Yes
Adjusted R-squared	0.002	0.306	0.013	0.321
Observations	29,666	29,639	29,568	29,541

Panel B: Weekly

	(1)	(2)	(3)	(4)
Technology Flaws	-0.08*	-0.05*	-0.20***	-0.16***
	(0.04)	(0.03)	(0.06)	(0.04)
Controls	Yes	Yes	Yes	Yes
Coin FE	No	No	Yes	Yes
Week FE	No	Yes	No	Yes
Adjusted R-squared	0.003	0.321	0.009	0.331
Observations	13,231	13,231	13,132	13,132

Table 6
Cybersecurity Factor Performance

This table presents the average portfolio returns for the long, short, and long-short portfolios. The long portfolio comprises of coins that had no bugs (*Technology Flaws* = 0) in period $t-1$, while the short portfolio is comprised of coins that were in the top 10th percentile of *Technology Flaws* in period $t-1$. We exclude dates where all coins had *Technology Flaws* = 0 in period $t-1$. All portfolios are equal-weighted. Portfolio returns are expressed in percentages and robust standard errors are reported in parentheses. Panel A presents daily results, while Panel B presents weekly results.

Panel A: Daily Factor

	Long	Short	Long - Short
Return	0.545***	0.246**	0.299***
	(6.79)	(2.58)	(6.08)
N	2541	2541	2541

Panel B: Weekly Factor

	Long	Short	Long - Short
Return	3.080***	2.204**	0.876**
	(4.52)	(3.02)	(3.13)
N	364	364	363

Table 7
Cybersecurity Factor Performance by Momentum and Size Tercile

This table presents the average portfolio returns for the long, short, and long-short cybersecurity portfolios, double sorted against momentum and size terciles. We initially sort into momentum or size terciles. Momentum is sorted based on the second lag of weekly returns, while size is sorted based on lagged market cap. For each size or momentum tercile, we then compute the long-short Cybersecurity portfolio. The long portfolio is comprised of coins that had no bugs (*Technology Flaws* $= 0$) in period $t-1$, while the short portfolio is comprised of coins that were in the top 10th percentile of *Technology Flaws* in period $t-1$. We exclude tercile-dates where all coins had *Technology Flaws* $= 0$ in period $t-1$. All portfolios are equal-weighted. Portfolio returns are expressed in percentages and robust standard errors are reported in parentheses. Panel A presents daily results, while Panel B presents weekly results.

Panel A: Double-Sort, Size then *Technology Flaws*

	Long	Short	Long - Short
Small Market Cap	1.828**	0.954	0.874
	(2.91)	(0.79)	(0.86)
	2.589***	0.709	1.880**
	(3.65)	(0.95)	(3.31)
Large Market Cap	3.578***	2.367**	1.211**
	(4.70)	(3.22)	(3.10)

Panel B: Double-Sort, Momentum then *Technology Flaws*

	Long	Short	Long - Short
Low Past Return	3.239***	1.902*	1.337*
	(4.60)	(2.19)	(2.42)
	2.423***	1.534*	0.889*
	(3.62)	(2.06)	(2.44)
High Past Return	3.509***	2.978***	0.531
	(4.88)	(3.42)	(1.01)

Table 8
Cybersecurity Factor and Crypto Market, Size, and Momentum Factors

The table presents the results of the following regression:

$$\text{CybersecurityFactor}_t = \alpha + \beta_1 \text{CryptoMarket}_t + \beta_2 \text{CryptoSize}_t + \beta_3 \text{CryptoMomentum}_t + \epsilon_t,$$

where $\text{CybersecurityFactor}_t$ is the return for the cybersecurity factor in week t in percentage points. CryptoMarket_t, CryptoSize_t, and CryptoMomentum_t are the Y. Liu et al. (2022) crypto market, size, and momentum factors, respectively. Newey West standard errors are estimated with one lag and reported in parentheses.

	(1)	(2)	(3)	(4)
Crypto Market	-0.03			-0.05*
	(0.03)			(0.03)
Crypto Size		0.10**		0.11***
		(0.04)		(0.04)
Crypto Momentum			0.04	0.02
			(0.08)	(0.07)
α	0.95***	0.55**	0.87***	0.59**
	(0.31)	(0.27)	(0.29)	(0.26)
Observations	325	325	325	325

Table 9
Technological Flaws and Cryptocurrency Returns after Hacks

The table presents the results of the following regression:

$$\begin{aligned}\text{Return}_{i,t} = \beta_0 + \beta_1 \text{Technology Flaws}_{i,t-1} + \beta_2 \text{Technology Flaws}_{i,t-1} \times \text{Hack}_{t-1} \\ + \boldsymbol{\beta} \boldsymbol{X}_{i,t} + \phi_i + \zeta_t + \epsilon_{i,t},\end{aligned}$$

where $\text{Return}_{i,t}$ is the return for crypto i on date t in percentage points, $\text{Technology Flaws}_{i,t}$ is the number of bug reports for crypto i on date t, and $\boldsymbol{X}_{i,t}$ is a vector of control variables including the log of trading volume and the log of market cap. ζ and ϕ are date and coin fixed effects, respectively. Hacks_{t-1} is a variable that represents either an indicator for whether a major hack occurred on day $t-1$ (Column 1) or an indicator for whether a major hack occurred on day $t-1$ and had zero dollars recovered (Column 2). Robust standard errors clustered at the coin level are reported in parentheses. *, **, and *** indicate significance at the 10%, 5%, and 1% levels, respectively.

	(1)	(2)
Technology Flaws	-0.07***	-0.07***
	(0.03)	(0.03)
Technology Flaws × Hack	-0.21	
	(0.13)	
Technology Flaws × No Recovery Hack		-0.35*
		(0.19)
ln(Market Cap)	0.24***	0.24***
	(0.03)	(0.03)
ln(Volume)	0.17***	0.17***
	(0.02)	(0.02)
Coin FE	Yes	Yes
Date FE	Yes	Yes
Adjusted R-squared	0.128	0.128
Observations	1,492,290	1,492,290