Cyber risks and initial coin offerings

Citation for published version:
An, J, Duan, T, Hou, W & Liu, X 2020, 'Cyber risks and initial coin offerings: Evidence from the world', *Finance Research Letters*. https://doi.org/10.1016/j.frl.2020.101858

Digital Object Identifier (DOI):
10.1016/j.frl.2020.101858

Journal Pre-proof

Cyber Risks and Initial Coin Offerings: Evidence from the World

Jiafu An , Tinghua Duan , Wenxuan Hou , Xianda Liu

PII: S1544-6123(20)31672-X
DOI: https://doi.org/10.1016/j.frl.2020.101858
Reference: FRL 101858

To appear in: *Finance Research Letters*

Received date: 19 May 2020
Accepted date: 18 November 2020

Cyber Risks and Initial Coin Offerings: Evidence from the World

Jiafu An[a,b], Tinghua Duan[d,e], Wenxuan Hou[c,a] and Xianda Liu[a]

[a]The University of Edinburgh Business School, 29 Buccleuch Place, Edinburgh, EH8 9JS, UK

[b]University of Portsmouth, Faculty of Business and Law, Portsmouth, PO1 3DE, UK

[c]School of Finance, Shanghai Lixin University of Accounting and Finance, Shanghai, China

[d]IESEG School of Management, 1 Parvis de La Defense, Paris La Defense, 92044 France e LEM-CNRS 9221, 3 Rue de la Digue, Lille 59000, France

Abstract

This paper examines the impact of cyber risks on ventures' initial coin offerings (ICOs) results. We match novel data on national cybersecurity with hand collected characteristics of 1,654 ICO projects and discover that cyber risks are negatively associated ICO success. We further find that institutional quality, such as the protection of investor rights and the function of the legal system, attenuates this relationship.

Keywords

ICO, cyber risks, institution quality

JEL Codes

F0; G30; G32; G38

1. Introduction

Initial coin offerings (ICOs) have become an important financing mechanism for young ventures facing financing frictions (Fisch 2019; Howell, Niessner and Yermack 2019; Zhao et al., 2020). Agency costs and information asymmetry have long limited arms-length retail investments to those with elite professional networks or close ties to venture capitalists (Hall and Lerner 2010; An and Rau 2019; An et al. 2019). ICOs, through which early-stage ventures sell blockchain-based digital tokens to raise capital on the Internet, help start-ups alleviate these frictions by providing more liquidity and transparency. According to ICObench, the combined value raised from ICOs since 2015 reached $46 billion in May 2019, which is equivalent to 12% of the value of global private equity market in 2017.

While ICOs offer substantial benefits in alleviating financial frictions, they also pose new security challenges (Howell, Niessner and Yermack 2019; Hall and Lerner 2010; An and Rau 2019; An et al. 2019). In particular, cyber-attack risks are significantly higher in ICOs than in conventional financial instruments (e.g., private equity and bank loans), since ventures going through ICOs are mostly technology driven and ICOs themselves depend on internet-based distributed ledger technology. Prior research documents that the average cost of cyber-attacks for traditional firms is about 2.5% of their market value, with a maximum loss of 15%[1] (Campbell et al. 2003; Ettredge and Richardson 2002; Garg, Curtis and Halper 2003). For an average New York Stock Exchange listed firm in 2018, value drops of these magnitudes can translate into shareholder losses of between $250 million and $1.4 billion[2]. Expected costs of cyber-attacks for ICO ventures can only be larger, since both the probability and the potential value loss of attacks are substantially higher compared to those of traditional firms.

[1] Computer Economics Inc. reports annual financial impact of major virus attacks from 1995 to 2003. The costs of major virus attacks in their sample ranges from $500 million in 1995 to $17.1 billion in 2000 (Security Issues: Virus Costs Are Rising Again 2003).

[2] Surveys by Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) reports costs of computer crims from 1997 to 2003 (CSI/FBI Computer Crime and Security Survey 1998-2004). These costs range from $100.1 million in 1997 to $455.8 million in 2002.

Despite the importance of cyber risks to ICOs and the increasing frequency of cyber-attacks globally[3], empirical evidence on such issues is scarce. This paper, to the best of our knowledge, provides the first empirical examination of how cybersecurity risks affect ventures' ICO results. In particular, our paper asks (i) whether cyber-attack risks are associated with a smaller number of ventures going through ICOs and less total amount raised in ICOs, and (ii) if institutional quality mitigates the negative impacts of cyber-attack risks on ICO outcomes.

Our result shows that cyber-attack risks are strongly, negatively associated with both the number of and the amount raised through ICOs. This result is robust to the controlling of various ICO characteristics, national indicators, Bitcoin price and volatility and year-quarter fixed effects. We further discover that better investor protection, measured by anti-director rights (La Porta et al 2002), constraints on managers' self-dealing activities (Djankov et al. 2008), court speed and protection on private foreign investments (Acemoglu and Johnson 2005), helps attenuates the negative impact of cybersecurity risks on ICO outcomes.

This paper speaks to a nascent literature that examines the determinants of ICO outcomes. For example, Howell, Niessner and Yermack (2019) investigate various issuer's characteristics in predicting ICOs' employment, failure, liquidity and trading volume. Fisch (2019) evaluates one specific dimension of ICO traits, technology capabilities, in determining the total amount of fund raised. Our paper is closely related to, but distinct from, this literature by stressing a key friction between ICO issuers' strategies and investors' preferences in high risk environment.

---

[3] See Congressional Research Service Report for Congress 2004 and Kaspersky Security Bulletin 2014-2018.

This study also relates to the literature that aims to identify the factors that help ICO firm raise higher amounts of capital (e.g. An et al. 2018; Momtaz, 2018a, b). An et al. (2018) show that both the disclosure of founders' information and founding team's human capital are associated with larger amount of fund raised and higher speed of fundraising. Momtaz (2018a, b) examines how CEO's emotion and loyalty shape a successful ICO. We take a further step to examine what factors determine ICO's financial outcomes in high cyber risk regions and provide evidence that have important implications to policy makers in such an environment.

2. Data

In this section, we describe the key data that we use to assess the relationship between cyber-attack risk and ICO outcomes, and the role of institutional quality in mitigating the impact of cyber risks. Table A1 in the appendix provides detailed definitions and data sources and Table 1 presents summary statistics.

2.1 Measures of Cyber-attack Risks

Our main data source on cyber risks is from International Telecommunication Union (ITU). ITU is a specialized agency of the United Nations that is responsible for issues regarding information and communication technologies. Together with international private partners as well as the World Bank, Indiana University and Korea Internet and Security Agency, ITU has published the global cybersecurity index (GCI) to address cybersecurity challenges in the world. The GCI index measures the level of cybersecurity relative to other countries and emphasizes the differences in terms of their level of engagement in cybersecurity programmes and initiatives. We use the GCI index as our main measure of cybersecurity risk (Cyber Security). Since we only have access to the GCI index in 2017-18, we assign the 2017 index value to observations in 2017 and before, and the 2018 index value to observations in 2018 and after. The potential measurement error in this treatment is negligible in our sample since the lion share of our observations is in 2017-18 (88%).

As shown in Table 1, this measure ranges from 0.06 to 0.93, with higher value indicates less cyber-attack risks. The average level of cybersecurity in our sample is 0.73, and a standard deviation of 0.22 indicates substantial variation in cyber risks in our sample. Figure 1 presents a geographic visualization of this measure.

[Insert Table 1 about Here]

We augment this data with an alternative cyber risk measure constructed based on a different database, Kaspersky Lab, which provides information on the ten most frequently cyber-attacked countries[4] in the world in 2017. We construct an indicator, Cyber Attack, that equals to one if: (a) a country is one of the ten most frequently cyber-attacked countries, and (b) this observation is in 2018 and 2019, and zero if (a) an observation is in 2017 and before, and (b) a country is not on the most attacked list. This variable captures relatively short-term cyber-attacks risks, thus complementing our main measure of cyber risk. As shown in Table 1, this measure has a standard deviation of 0.29, indicating substantial variations within our sample.

2.2 Measures of ICO Outcomes

We hand collect ICO outcomes and other ICO information from ICObench[5], issuer websites and white papers. ICObench is recognized as one of the most prominent and

[4] These countries include Japan, Italy, Vietnam, Bulgaria, Taiwan, Cambodia, Croatia, Lebanon, Brazil, and Indonesia.
[5] See: https://icobench.com.

respected websites that provide issuer information for a comprehensive sample of ICOs (Howell, Niessner and Yermack 2019). To measure ICO outcomes at the country-level, we construct two variables. *Amount* equals to the natural logarithm of the total amount of fund raised from ICOs for each country each quarter during 2015-2019. *Number* is total number of ICOs for each country each quarter. These proxies together capture both the intensive and extensive margins of a country's ICO outcomes, which enable us to disentangle the aggregate cyber risk effects in later analyses.

At the venture level, our measures of ICO outcomes are *Fundraise*, calculated as the natural logarithm of the total amount of fund raised, and *Raise/day*, the daily equivalent of *Fundraise*. As presented in Table 1, the aggregate amount of money raised through ICOs in our sample equals $46 billion as of May 2019, which is equivalent to 12% of the value of global private equity market in 2017. The maximum amount raised in a single ICO is $1700 million in 2018 and $4198 million in 2017, respectively. Other measures of ICO characteristics include *Pre-sale*, *Payment*, *Bonus*, *Utility*, *Fiat* and *Verification*. Table A1 in the Online Appendix provides detailed definitions and data sources for the indicators.

2.3 Measures of Institutional Quality

We focus our attention on four specific investor protection institutions, including (i) the quality of anti-director rights (La Porta et al 2002); (ii) the degree of control on managers' self-dealing activities (Djankov et al. 2008); (iii) the extent to which lenders can collect a commercial debt at ease and (iv) the level of protection on private foreign investments (Acemoglu and Johnson 2005). These institutions are believed to be the most important ones for firm access to external finance. We obtain data on anti-director index (*ADRI*) from Spamann (2010), which provides an updated version of the index in La Porta et al. (2002). Anti-self-dealing index (*ASDI*) is accessed from Djankov et al. (2008). Following Acemoglu and Johnson (2005), we measure the extent to which lenders can collect a commercial debt at ease and the level of protection on private foreign investments using *Procedural complexity* and *Protection against expropriation*. For all these measures, higher values indicate better quality. As shown in Table 1, measures of institutional quality have substantial variations within our sample.

2.4 Other Macroeconomic Variables

We also control for various macroeconomic conditions to isolate the effects of cybersecurity risks on ICO outcomes in our analyses. Particularly, *Bitcoin Price* is the natural logarithm of quarterly average of closed price of Bitcoin; *Bitcoin Volatility* is the standard deviation of closed price of Bitcoin in each quarter; *GSI* is an equal weighted average of google search index on four keywords: “Bitcoin”, “Blockchain”, “ICO”, and “Cryptocurrency”; *ICO Ban* is a dummy variable that equals one if a country has banned ICO and zero otherwise; *GDP* is the natural logarithm of average GDP over the period of 2005-2015; *GDP per capita* growth is the average growth rate of GDP per capita over the period of 2005-2015; and *Population* is the natural logarithm of the total population. Table A1 in the Online Appendix provides detailed definitions and data sources for the indicators.

3. Results

In this section, we present empirical results on the relationship between cyber-attack risk and ICO outcomes, and the role of institutional quality in mitigating the impact of cyber risks.

3.1 Cyber-attack Risk and ICO Outcomes

We begin with cross-country, ordinary least squares (OLS) regressions to examine the relationship between measures of cyber-attack risks and ICO outcomes. Specifically, we use the following regression specification:

$$ICO_{c,t} = \alpha + \beta Cyber\ Proxy_{c,t} + \gamma Crypto\ Controls_t + \delta Marco_c + \zeta_t + \varepsilon_{c,t} \quad (1)$$

where the dependent variable, $ICO_{c,t}$ is one of the two country-level measures of ICO outcomes, *Amount* or *Number*, in country *c* year quarter *t*. The key explanatory variable is $Cyber\ Proxy_{c,t}$ for country *c*, at year *t*, which measures a country's level of cybersecurity based on the global cybersecurity index obtained from International Telecommunication Union. $Crypto\ Controls_t$ is a vector of crypto currency related confounders, including *Bitcoin Price, Bitcoin Volatility*, *GSI* and *ICO Ban*. $Marco_c$ represents macroeconomic covariates, such as *GDP*, *GDP per capita growth*, and *Population*. ζ_t is year-quarter fixed effects that absorb common time shocks and allow comparisons across year-quarters. We report heteroskedasticity consistent t-statistics with the standard errors clustered at country-level.

[Insert Table 2 about Here]

As shown in Table 2, both measures of cybersecurity is strongly correlated with the amount of capital raised in ICOs and the total number of ICOs in a country. The coefficient on cybersecurity proxy in all regressions is statistically significant at least at the 5% significance level. The economic magnitude of our estimates is large. For example, consider the point estimate in Column (1) Panel A Table 2. The coefficient implies that on average, a one standard deviation increase in a country's cybersecurity level is associated with $1.04

million (=e^(0.165*0.22)) increase in total fund raised through ICOs in a quarter year. This is equivalent to 0.22 standard deviation of total amount of capital raised in our sample[6].

[Insert Table 3 about Here]

In Table 3, we continue our analyses at the venture level. In particular, we replace country-level ICO outcomes in model (1) with our venture-level outcomes. The results obtained from this analysis is qualitatively similar to our previous findings. For example, consider the estimated coefficients in Column (3) Panel A Table 3. The estimate implies that a one standard deviation increase in a country's cybersecurity level is, on average, associated with $1.28 million (=e^(1. 136*0.22)) increase in the amount of fund raised in a typical ICO.

3.2 The Role of Institutional Quality

In this subsection, we investigate the role of institutional quality in mitigating the negative impact of cyber-attack risks on ICO outcomes. In particular, we employ the following regression specification to examine the mediating effects of institutions:

$$ICO_{c,t} = \alpha + \beta_1 Better\ Protection_c \times Cyber\ Security_{c,t} + \beta_2 Cyber\ Security_{c,t} + \beta_3 Better\ Protection_c + \gamma Crypto\ Controls_t + +\delta Marco_{c,t} + \varepsilon_{c,t} \quad (2)$$

where the dependent variable, $ICO_{c,t}$ is one of the two country-level measures of ICO outcomes, *Amount* or *Number*, in country *c* in year quarter *t*. The key explanatory variable is an interaction term between measures of *Cyber Security* and a dummy indicator that equals to one if an institution has an above-average quality and zero otherwise. As in model (1), we

[6] We also perform a split sample test. In particular, we construct our country-level ICO success measures using either only utility tokens or other types of tokens, and re-run our country-level analyses. Results are tabulated in the online appendix. We find our results are mainly driven by the ICOs that offer utility tokens. We interpret this result based the different rights attached to these two types of tokens. Since utility tokens offer investors rights to future consumption of a venture's products, ICOs that offer this type of tokens are more sensitive to network disruption (i.e., cyber-attacks), which may lead to delay in production or lower product quality.

include a vector of crypto currency related confounders, represented by $Crypto\ Controls_t$, and macroeconomic covariates proxied by $Marco_c$. We report heteroskedasticity consistent t-statistics with the standard errors clustered at country-level.

[Insert Table 4 about Here]

As shown in Table 4, we discover that better investor protection mitigates the negative effects of cybersecurity risks on ICO outcomes, which is consistent with existing literature on institution and finance (La Porta et al. 1998. 2008; Acemoglu and Johnson 2005; Glaeser et al. 2004). These findings suggest that investors take both cybersecurity risks and institutional quality into account when making investment decisions.

4. Conclusion

This paper finds that cybersecurity risk is an important impediment to raising capital through ICOs, and institutions that better protect investors can mitigate this negative impact. This paper makes several contributions to the literature. First, it speaks to a nascent literature that examines the determinants of ICO outcomes (e.g., Howell, Niessner and Yermack 2019; Fisch 2019). Secondly, this study relates to the literature that aims to identify the factors that help ICO firm raise higher amounts of capital (e.g. An et al. 2018, Ante et al. 2018, Blaseg 2018, Burns and Moro 2018). Further, this paper also speaks to an emerging literature that studies the economics of digital currencies and blockchain (Catalini and Gans 2016; Cong, He, and Zheng 2017). Lastly, it connects to the broader entrepreneurial finance literature (Kaplan, Sensoy, and Strömberg 2009; Mollick 2014; Bernstein, Korteweg, and Laws 2017).

References

Acemoglu, D., & Johnson, S. (2005). Unbundling institutions. *Journal of political Economy*, 113(5), 949-995.

An, J., Duan, T., Hou, W., & Xu, X. (2019). Initial Coin Offerings and Entrepreneurial Finance: The Role of Founders' Characteristics. *The Journal of Alternative Investments*, 21(4), 26-40.

An, J., & Rau, R. (2019). Finance, technology and disruption. *The European Journal of Finance*, 1-12.

Ante, L., Sandner, P., & Fiedler, I. (2018). Blockchain-Based ICOs: Pure Hype or the Dawn of a New Era of Startup Financing?. *Journal of Risk and Financial Management*, 11(4), 80.

Bernstein, S., Korteweg, A., & Laws, K. (2017). Attracting early-stage investors: Evidence from a randomized field experiment. *The Journal of Finance*, 72(2), 509-538.

Blaseg, D. (2018). Dynamics of voluntary disclosure in the unregulated market for initial coin offerings. Working paper.

Burns, L., & Moro, A. (2018). What Makes an ICO Successful? An Investigation of the Role of ICO Characteristics, Team Quality and Market Sentiment. Working paper.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431-448.

Catalini, C., & Gans, J. S. (2018). Initial coin offerings and the value of crypto tokens (No. w24418). *National Bureau of Economic Research*.

Cong, L. W., Li, Y., & Wang, N. (2018). Tokenomics: Dynamic adoption and valuation. Working paper.

Djankov, S., La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (2008). The law and economics of self-dealing. *Journal of financial economics*, 88(3), 430-465.

Ettredge, M., & Richardson, V. J. (2002, January). Assessing the risk in e-commerce. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (pp. 11-pp). IEEE.

Fisch, C. (2019). Initial coin offerings (ICOs) to finance new ventures. *Journal of Business Venturing,* 34(1), 1-22.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2), 74-83.

Glaeser, E. L., La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (2004). Do institutions cause growth?. *Journal of economic Growth*, 9(3), 271-303.

Hall, B. H., & Lerner, J. (2010). The financing of R&D and innovation. In Handbook of the Economics of Innovation (Vol. 1, pp. 609-639). North-Holland.

Howell, S. T., Niessner, M., & Yermack, D. (2018). Initial coin offerings: Financing growth with cryptocurrency token sales (No. w24774). *National Bureau of Economic Research*.

Kaplan, S. N., Sensoy, B. A., & Strömberg, P. (2009). Should investors bet on the jockey or the horse? Evidence from the evolution of firms from early business plans to public companies. *The Journal of Finance*, 64(1), 75-115.

La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. (2002). Investor protection and corporate valuation. *The journal of finance*, 57(3), 1147-1170.

Mollick, E. (2014). The dynamics of crowdfunding: An exploratory study. *Journal of business venturing,* 29(1), 1-16.

Momtaz, P. 2018a. "Initial Coin Offerings, Asymmetric Information, and Loyal CEOs." Working paper.

Momtaz, P. 2018b. "Token Sales and Initial Coin Offerings: Introduction." Working paper.

Zhao, X., Hou, W., An, J., Liu, X., & Zhang, Y. (2020). Initial Coin Offerings: What Rights Do Investors Have (If Any)? European Journal of Finance, forthcoming

Figure 1: ICO projects by countries And.

Figure 2: Cybersecurity by countries (just in case).

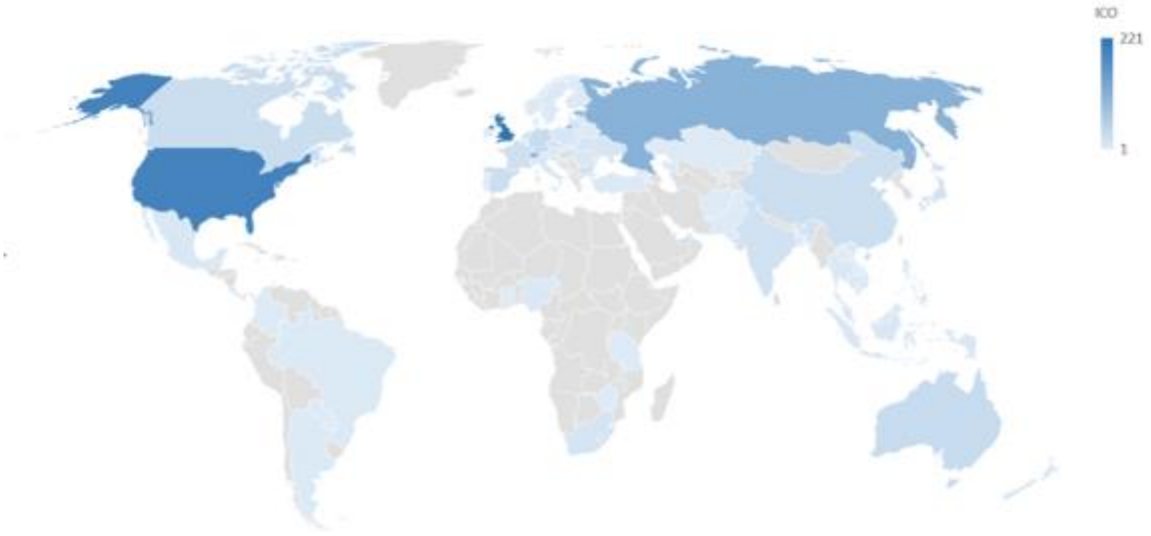

Table 1: Summary statistics

Panel A: Initial coin offerings summary

Year	2015	2016	2017	2018	May-2019
Project-level summary:					
Number of ICOs	2	18	416	1,046	166
Total amount of fundraise (in millions USD)	5.21	70.83	10,152.46	13,454.21	2,220.97
Max-amount of fundraise (in millions USD)	5	16	4,197.96	1,700	1,000
Min-amount of fundraise (in USD)	205,103	38,180	420	0.12	279
Country-level summary:					
Number of Countries launching ICOs	2	12	50	87	45
Country with max-number of ICO projects	Switzerland & USA	Switzerland & USA	USA	Singapore	Singapore
Number of ICOs	1	3	89	144	22
Country with max-fundraise in ICOs	USA	Switzerland	USA	UK	UAE
Amount of fundraise in ICOs (in millions USD)	5	20.73	6077.44	4277.70	210.52

Panel B: Descriptive statistics

	Observation	Mean	S.D.	Min	Max
Country-level variables					
Amount	397	2.77	0.15	1.73	3.10
Number	397	4.06	6.49	1.00	45.00
Cyber Security	386	0.73	0.22	0.06	0.93
Cyber Attack	397	0.09	0.29	0.00	1.00
ADRI	286	3.65	1.09	0.00	5.00
ASDI	292	0.54	0.26	0.09	1.00
Procedural complexity	317	5.27	1.37	2.92	8.61
Constraint on executive	333	5.97	1.58	1.18	7.00
Crypto-Controls					

Bitcoin Price	397	8.61	0.68	5.54	9.27
Bitcoin Volatility	397	1450.98	1308.17	22.43	4546.69
GSI	397	20.29	10.36	1.44	38.73
Marco-Controls					
ICO Ban	397	0.02	0.14	0.00	1.00
GDP	382	27.37	3.38	18.92	36.47
GDP per capita growth	382	2.15	2.04	-3.25	9.20
Population	393	16.07	2.54	10.20	21.01
Project-level variables					
Fundraise	1654	15.06	1.96	-2.12	22.16
Raise/day	1646	11.26	2.36	-6.31	18.85
Verification	1654	0.68	0.83	0.00	1.00
Pre-sale	1654	0.46	0.50	0.00	1.00
Payment	1654	2.06	1.61	1.00	13.00
Fiat	1654	0.15	0.36	0.00	1.00
Bonus	1654	0.31	0.46	0.00	1.00
Utility	1654	0.96	0.20	0.00	1.00

Table 2 Cybersecurity risk and ICO development on country level

This table presents country-level analyses of the relationship between cybersecurity risk and ICO. The dependent variable, $ICO_{c,t}$, is either *Amount*, which is the natural logarithm of total amount of ICO fundraise for each country each quarter in column (1)-(3) or *Number* which is the total number of ICO projects for each country each quarter in column (4)-(6). Our key interest variable, $Cyber\ Proxy_{c,t}$, in Panel A is *Cyber Security*, which is an index for cybersecurity for each country and a higher value suggests better protection. In Panel B, $Cyber\ Proxy_{c}$ is *Cyber Attack* which is a dummy variable that equals one country is one of the top 10 countries attacked by crypto-ransomware after 2017 and zero otherwise. $Crypto\ Controls_t$ includes *Bitcoin Price, Bitcoin Volatility*, and *GSI* in column (1), (2), (4) and (5). $Marco_c$ includes *ICO Ban*, *GDP*, *GDP per capita growth*, and *Population* in column (2), (3), (5) and (6). Year-quarter fixed effects are represented by ζ_t in column (3) and (6). Detail variable definitions are introduced in Appendix. Standard errors are clustered at the country level and *t*-statistics are in brackets. ***, **, * denote significance levels at 1%, 5% and 10% respectively.

	(1)	(2)	(3)	(4)	(5)	(6)
		Amount			Number	
Panel A:						
Cyber Security	0.165***	0.202***	0.224***	9.001***	9.102***	9.922***
	[2.996]	[3.880]	[4.069]	[3.021]	[2.907]	[2.937]
Crypto-Controls	Yes	Yes	-	Yes	Yes	-
Marco-Controls	-	Yes	Yes	-	Yes	Yes
Intercept	2.523***	2.745***	2.857***	-12.462**	-10.725*	0.494
	[23.245]	[22.369]	[34.355]	[-2.554]	[-1.968]	[0.122]
Quarterly Dummies	-	-	Yes	-	-	Yes
R-square	0.076	0.096	0.113	0.106	0.104	0.104
Observation	386	381	381	386	381	381
Panel B:						
Cyber Attack	-0.132***	-0.123***	-0.120***	-2.922***	-3.175***	-3.037**
	[-3.536]	[-3.107]	[-2.957]	[-3.394]	[-2.706]	[-2.592]
Crypto-Controls	Yes	Yes	-	Yes	Yes	-
Marco-Controls	-	Yes	Yes	-	Yes	Yes

Intercept	2.570***	2.584***	2.816***	-7.838**	-15.553**	-0.334
	[22.210]	[19.190]	[33.423]	[-2.169]	[-2.566]	[-0.075]
Quarterly Dummies	-	-	Yes	-	-	Yes
R-square	0.068	0.064	0.066	0.027	0.042	0.030
Observation	397	383	383	397	383	383

Table 3 Cybersecurity risk and ICO fundraise on project level

This table presents project-level analyses of the relationship between cybersecurity risk and ICO fundraise. The dependent variable, $ICO\ Fund_{i,c,t}$ is either *Fundraise*, which is the natural logarithm of total amount of fundraise in ICO in column (1)-(3) or *Raise/day* which is the natural logarithm of daily amount of fundraise in ICO in column (4)-(6). Our key interest variable is *Cyber Security*, which is an index for cybersecurity for each country and a higher value suggests better protection. $Crypto\ Controls_t$ includes *Bitcoin Price, Bitcoin Volatility*, and *GSI* in column (1), (2), (4) and (5). $Marco_c$ includes *ICO Ban*, *GDP*, *GDP per capita growth*, and *Population* in column (2), (3), (5) and (6). ICO_i represents ICO characteristics including *Verification*, *Pre-sale*, *Payment*, *Fiat*, *Bonus*, and *Utility*. Year-quarter fixed effects are represented by ζ_t in column (3) and (6). Detail variable definitions are introduced in Appendix. Standard errors are clustered at the country level and *t*-statistics are in brackets. ***, **, * denote significance levels at 1%, 5% and 10% respectively.

	(1)	(2)	(3)	(4)	(5)	(6)
		Fundraise			Raise/day	
Panel A:						
Cyber Security	0.615**	1.022***	1.136***	0.661	1.147**	1.404***
	[2.033]	[3.245]	[3.420]	[1.608]	[2.464]	[3.038]
Crypto-Controls	Yes	Yes	-	Yes	Yes	-
Marco-Controls	-	Yes	Yes	-	Yes	Yes
ICO-Controls	-	Yes	Yes	-	Yes	Yes
Intercept	14.885***	17.623***	16.221***	18.305***	18.179***	12.367***
	[14.298]	[14.168]	[21.699]	[10.104]	[10.033]	[11.896]
Quarterly Dummies	-	-	Yes	-	-	Yes
R-square	0.018	0.029	0.065	0.046	0.080	0.152
Observation	1583	1558	1558	1581	1556	1556
Panel B:						
Cyber Attack	-1.006***	-0.847***	-0.846***	-0.825**	-0.720**	-0.736**
	[-5.545]	[-3.107]	[-2.905]	[-2.566]	[-2.118]	[-2.019]
Crypto-Controls	Yes	Yes	-	Yes	Yes	-
Marco-Controls	-	Yes	Yes	-	Yes	Yes

ICO-Controls	-	Yes	Yes	-	Yes	Yes
Intercept	14.818***	17.030***	16.368***	18.282***	17.682***	12.671***
	[13.836]	[12.285]	[20.404]	[9.901]	[9.215]	[11.568]
Quarterly Dummies	-	-	Yes	-	-	Yes
R-square	0.023	0.027	0.060	0.046	0.076	0.145
Observation	1612	1561	1561	1610	1559	1559

Table 4: Investor protections and Cyber risks

This table presents the country-level analyses of the market reaction of cybersecurity and investor protections.

The dependent variable, $ICO_{c,t}$, is either *Amount*, which is the natural logarithm of total amount of ICO fundraise for each country each quarter in column (1) and (3) or *Number* which is the total number of ICO projects for each country each quarter in column (2) and (4). Our key interest variables in Panel A are the interaction terms of $Cyber\ Security_{c,t}$ and better investor protection indicators of *ADRI*, which is a dummy variables that equals one if the country has an above-mean score on anti-director rights index and zero otherwise in column (1) and (2) and better protections on *ASDI* in column (3) and (4), which is a dummy variables that equals one if the country has an above-mean score on anti-self-dealing index and zero otherwise. In Panel B, our key interest variables are the interaction terms of $Cyber\ Security_c$ and better protection indicators of *Procedural complexity*, which is a dummy variables that equals one if the country has a below-mean score on index of complexity in collecting a commercial debt and zero otherwise in column (1) and (2) and indicators of *Protection against expropriation* in column (3) and (4), which is a dummy variables that equals one if the country has an above-mean score on risk of expropriation and zero otherwise. $Crypto\ Controls_t$ includes *Bitcoin Price, Bitcoin Volatility*, and *GSI* and $Marco_c$ includes *ICO Ban*, *GDP*, *GDP per capita growth*, and *Population*. Detail variable definitions are introduced in Appendix. Standard errors are clustered at the country level and *t*-statistics are in brackets. ***, **, * denote significance levels at 1%, 5% and 10% respectively.

	(1)	(2)	(3)	(4)
	Amount	Number	Amount	Number
Panel A:				
	ADRI		ASDI	
Cyber Security × Better Protection	0.252**	12.796*	0.439***	30.962***
	[2.048]	[1.689]	[3.396]	[2.876]
Cyber Security & Better Protection	Yes	Yes	Yes	Yes
Crypto & Marco-Controls	Yes	Yes	Yes	Yes
Intercept	2.758***	-10.286*	2.733***	-11.127*
	[23.429]	[-1.935]	[23.425]	[-1.769]
R-square	0.115	0.127	0.164	0.215
Observation	381	381	381	381
Panel B:				

	Procedural complexity		Protection against expropriation	
Cyber Security × Better Protection	0.278**	17.714**	0.369**	24.151**
	[2.134]	[2.204]	[2.053]	[2.113]
Cyber Security & Better Protection	Yes	Yes	Yes	Yes
Crypto & Marco-Controls	Yes	Yes	Yes	Yes
Intercept	2.771***	-9.224*	2.821***	-8.506
	[22.414]	[-1.755]	[22.668]	[-1.447]
R-square	0.144	0.190	0.114	0.159
Observation	381	381	381	381

Appendix: Variable definitions

Variable Names	Description
Country-level	
Amount	The natural logarithm of the total amount of fund (USD) raised from Initial Coin Offerings (ICOs) for each country each quarter[7]. The date of an ICO project is defined as the completion data. Source: https://icobench.com/
Number	The total number of ICO projects for each country each quarter. The date of an ICO project is defined as the completion data. Source: https://icobench.com/
Cyber Security	Global Cybersecurity Index (GCI) that ranks countries' cybersecurity based on measures on five dimensions that include legal, technical, organizational environmental, capacity building and cooperation. Source: International Telecommunication Union (ITU) report 2017 & 2018.
Cyber Attack	An indicator of cyber-attacks that equals to one if a country is one of the ten countries in the world that have been seriously attacked by crypto-ransomware after 2017, and zero otherwise. These countries include Japan, Italy, Vietnam, Bulgaria, Taiwan, Cambodia, Croatia, Lebanon, Brazil, and Indonesia. Source: Kaspersky Lab.

[7] The county refers to the ICO company incorporated country.

ADRI	An index of anti-director rights that aggregates six key measures including: (1) proxy by mail allowed, (2) shares not blocked before shareholder meeting, (3) cumulative voting and proportional representation allowed, (4) oppressed minority protection, (5) pre-emptive rights to new share issues, (6) percentage of shares needed to call an extraordinary shareholder meeting. Each measure is a dummy variable that equals to one if a firm support such anti-director rights and zero otherwise. The index ranges from 0 to 6, whereby a higher value indicates stronger anti-director rights. Better protection indicator is a dummy variable that equals one if the country has an above-mean score on *ADRI* and zero otherwise. Source: Spamann (2010).
ASDI	Anti-self-dealing index is an average of *ex ante* and *ex post* private control of self-dealing scores. The *ex-ante* private control of self-dealing score is the first component of measures including approval by disinterested shareholders and ex ante disclosure by the buyer, the insider, and independent review. The *ex post* private control of self-dealing scores is the first component of measures including the disclosure in periodic filings and the ease of proving wrongdoing (holding the insider and the approving body civilly liable and having access to evidence). Better protection indicator is a dummy variable that equals one if the country has an above-mean score on *ASDI* and zero otherwise. Source: Djankov et al. (2008).
Procedural complexity	An index of complexity in collecting a commercial debt, valued at 50% of annual GDP per capita. This measure ranges from 0 to 10. Better protection indicator is a dummy variable that equals one if the country has a below-median score on index of *Procedural complexity* and zero otherwise. Source: Acemoglu and Johnson (2005)
Protection against expropriation	An index of risk of expropriation of private foreign investment, ranging from 0 to 10, with higher scores indicating less risk; we calculated the mean value for the period of 1985-1995. Better protection indicator is a dummy variable that equals one if the country has an above-median score on *Protection against expropriation* and zero otherwise. Source: Acemoglu and Johnson (2005)

(Continued)

Appendix: Variable definition – Continued

Variable Names	Description
Crypto-Controls	

Bitcoin Price	The natural logarithm of quarterly average of closed price of Bitcoin (in USD) in Coordinated Universal Time (UTC time). Source: https://coinmarketcap.com/currencies/bitcoin/
Bitcoin Volatility	The standard deviation of closed price of Bitcoin (in USD) in each quarter. Source: https://coinmarketcap.com/currencies/bitcoin/
GSI	Google search index. The equal weighted average of google search index on four keywords: “Bitcoin”, “Blockchain”, “ICO”, and “Cryptocurrency”. Source: Google
Marco-Controls	Source: World Bank
ICO Ban	A dummy variable that equals to one if a country banned ICO and zero otherwise. Data is accessed from: https://www.loc.gov/law/help/cryptocurrency/world-survey.php#ftn501
GDP	The natural logarithm of average GDP over the period 2005 through 2015 for each country adjusted for purchasing power parity (PPP).
GDP per capita growth	The average growth of GDP per capita for each country over the period 2005-2015.
Population	The natural logarithm of average of total population for each country over the period 2005 -2015.
Project-level	Source: https://icobench.com/
Fundraise	The natural logarithm of total amount of fund (USD) raised for each ICO project.
Fundraise per day	The natural logarithm of amount of fund (USD) raised for each ICO project per day, including the pre-sale period.
Verification	An categorical index that equals to two if an ICO project has been verified by both Know Your Customer (KYC) and Whitelist, one if an ICO has one of the two verifications, and zero if an ICO has none of both. KYC refers to the verification processes that requires the disclosure of an applicant’s identification (e.g., passport, driver’s license, etc.) as well as a photo in which the applicant holds his/her ID. Whitelist is an independent party that provides verifiable information on upcoming ICO that have higher potential value to investors.
Pre-sale	A dummy variable equals one if the ICO offers a pre-sale before ICO and zero otherwise.
Payment	The total number of payment methods that an ICO accepts, including various types of cryptocurrencies (e.g., Bitcoin, Ethereum, Bitcoin Cash) and a range of fiat currencies (e.g., EUR, USD, Pound).
Fiat	An indicator that equals one if an ICO accepts fiat currencies in the token sale and zero otherwise.
Bonus	An indicator that equals one if an ICO offers bonus/discount for early investors

	and zero otherwise.
Utility	An indicator that equals one if an ICO issues utility type of tokens and zero otherwise. Utility type of tokens are those that give its holders consumptive rights to access to a product or service.