UNIVERSITY *of* NICOSIA

Week 4, Session 8

Regulatory Compliance and External Factors

BLOC 528: Token Economics

Today’s Overview

- Objective #1: To understand the role of traditional market factors for crypto assets.
- Objective #2: To explore the regulatory considerations that influence the value of a token.
- Objective #3: To understand the sources of vulnerability of cyberattacks in token projects.

Data and Measurement from Liu, Tsyvinski, and Wu (2022)

- Data on over 200 major exchanges with information on daily opening, closing, high, and low prices/volume
- Coverage of 1,827 coins between the start of 2014 to July 2020, excluding coins with less than a market capitalization of $1,000,000

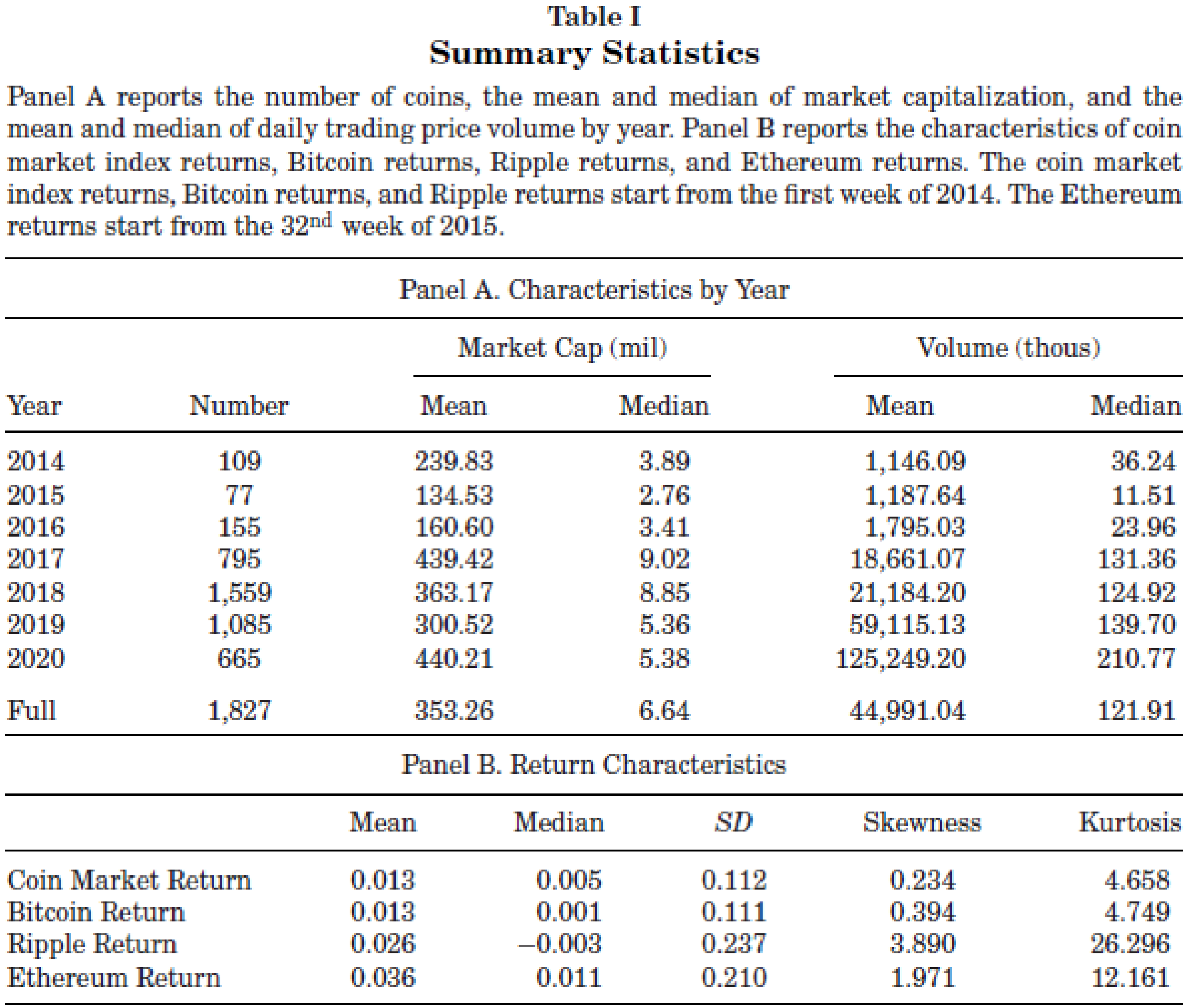


Table I

Summary Statistics

Panel A reports the number of coins, the mean and median of market capitalization, and the mean and median of daily trading price volume by year. Panel B reports the characteristics of coin market index returns, Bitcoin returns, Ripple returns, and Ethereum returns. The coin market index returns, Bitcoin returns, and Ripple returns start from the first week of 2014. The Ethereum returns start from the 32nd week of 2015.

Panel A. Characteristics by Year

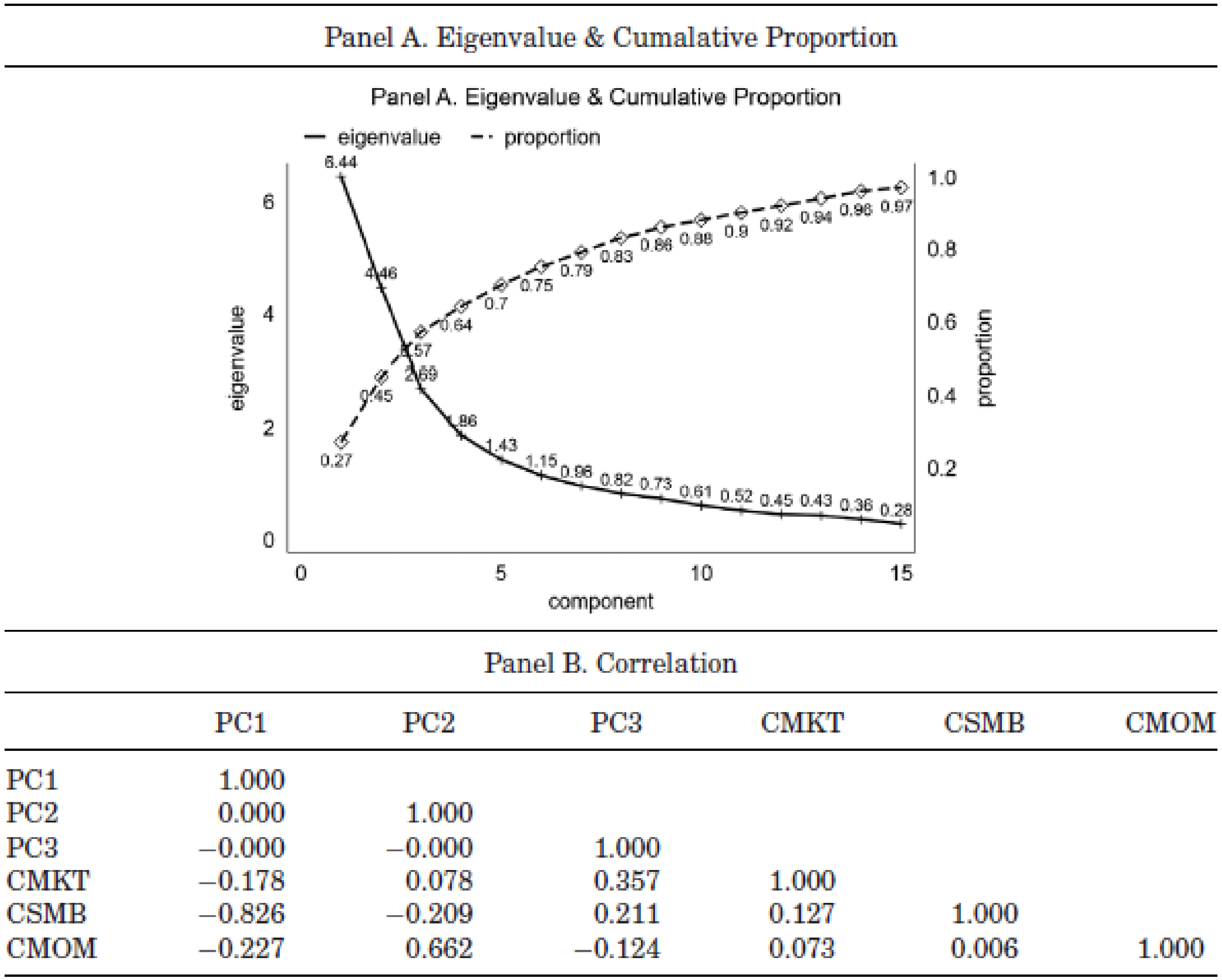
		Market Cap (mil)		Volume (thous)	
Year	Number	Mean	Median	Mean	Median
2014	109	239.83	3.89	1,146.09	36.24
2015	77	134.53	2.76	1,187.64	11.51
2016	155	160.60	3.41	1,795.03	23.96
2017	795	439.42	9.02	18,661.07	131.36
2018	1,559	363.17	8.85	21,184.20	124.92
2019	1,085	300.52	5.36	59,115.13	139.70
2020	665	440.21	5.38	125,249.20	210.77
Full	1,827	353.26	6.64	44,991.04	121.91

Panel B. Return Characteristics

	Mean	Median	*SD*	Skewness	Kurtosis
Coin Market Return	0.013	0.005	0.112	0.234	4.658
Bitcoin Return	0.013	0.001	0.111	0.394	4.749
Ripple Return	0.026	−0.003	0.237	3.890	26.296
Ethereum Return	0.036	0.011	0.210	1.971	12.161

What Explains Variation in Crypto Returns?

- Using principal component analysis on a full set of long-short strategies
- The first 2 principal components explain 45% of all the variation
- The first principal component correlates highly with the crypto size factor (corr = 0.826)
- The second factor correlates highly with the momentum factor (0.662)



Panel A. Eigenvalue & Cumalative Proportion

Panel B. Correlation

	PC1	PC2	PC3	CMKT	CSMB	CMOM
PC1	1.000					
PC2	0.000	1.000				
PC3	−0.000	−0.000	1.000			
CMKT	−0.178	0.078	0.357	1.000		
CSMB	−0.826	−0.209	0.211	0.127	1.000	
CMOM	−0.227	0.662	−0.124	0.073	0.006	1.000

Understanding the Role of Size and Momentum

The crypto size factor relates with the liquidity effect

- Small coins have lower price and higher Amihud illiquidity*, relative to the large coins
- In the cross section, the cryptocurrency size premium** is more pronounced among coins that have high arbitrage costs
- In the time series, the cryptocurrency size premium is larger at times of high cryptocurrency market volatility.

The size premium is consistent theories about the trade-off between capital gains and the convenience yield

- The size premium is large at times of high Bitcoin transactions
- Cryptocurrency momentum is more pronounced among coins that receive high investor attention, and stronger at times of high investor attention overall

*ratio of daily return to volume – proxy for institutional trading costs

**return spread between small/big coins

Regulatory Considerations and ICOs

Much like Uber was able to become a first mover in the ride sharing business through regulatory arbitrage, early cryptocurrencies were able to do that here – now the regulatory guidance is getting more stringent.

In 1946, the U.S. SEC had a case, SEC v. Howey Co in front of the Supreme Court that now has become known as the “Howey Test” for determining what is a security.

A token is a security if:

- It is an investment of money
- The investment of money is in a common enterprise
- There is an expectation of profits from the investment.

While tokens often satisfy the first two requirements, the third is not always satisfied.

- Create utility from the tokens (and some governance rights)
- Avoid promotional language

Latest Regulatory Guidance (U.S. Specific)

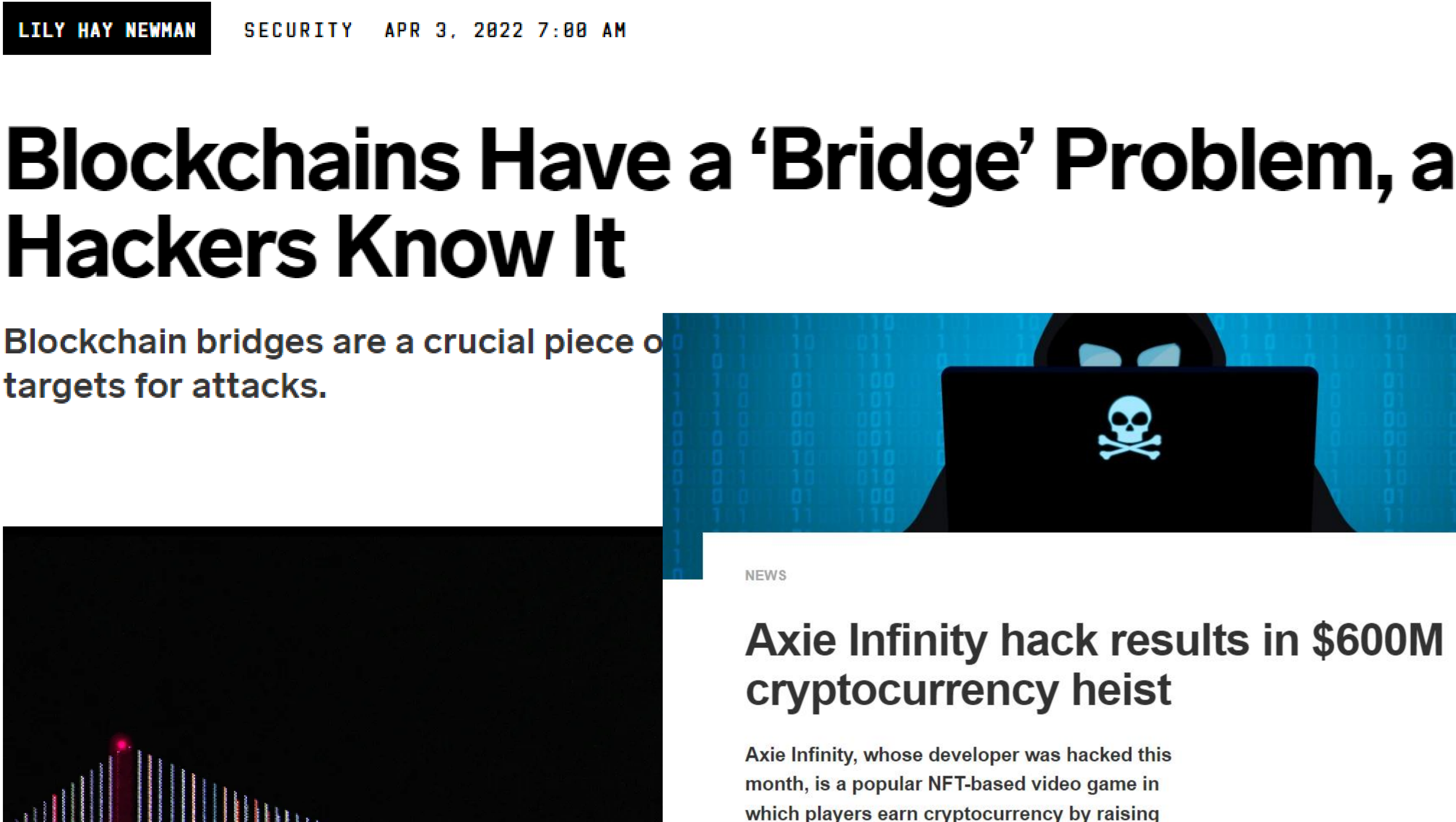
- On April 22, Wyoming's governor signed Bill 38, allowing them to recognize DAOs as LLCs
- Wyoming also passed a law that individuals and companies own digital instruments without the need for intermediaries as banks – the law allows for securities to be issued in tokenised form, thereby making Wyoming into the new "go-to" jurisdiction similar to, for example, how things are in the state of Delaware
- Federal Deposit Insurance Corporation (FDIC) issued a letter requesting that banks should notify their regional FDIC director of their crypto activities
- The SEC issued a proposal to "require communication protocol systems (or CPSs) to register with the agency and thereafter satisfy its many recordkeeping, transaction-monitoring and reporting obligations. These CPSs would be defined as systems or platforms that 'make available' the means for buyers and sellers of securities to interact.'"
- The "Stablecoin Transparency Act" would set standards for the "quality of assets held in reserves" as well as require stablecoin issuers to report on their reserves.

https://www.coindesk.com/layer2/2022/04/05/a-new-sec-definition-for-exchanges-has-big-implications-for-crypto/, https://vladanlausevic.medium.com/wyoming-as-a-blockchain-and-crypto-friendly-state-a9d02746ec9f

An Aside – What Are Stablecoins

- Because of the volatility in the crypto market, stablecoins have emerged and their price is tied towards a conventional fiat currency, like the dollar
- The entity sponsoring the stablecoin often sets up a reserve to securely store the collateral
- Some stablecoins are linked to real world assets, so whenever a holder cashes out of their token, an equal amount of the asset that backs it is taken out of reserves
- Stablecoins still have risk – does the counterparty actually have the collateral?

https://www.coindesk.com/learn/what-is-a-stablecoin/



LILY HAY NEWMAN SECURITY APR 3, 2022 7:00 AM

Blockchains Have a 'Bridge' Problem, a Hackers Know It

Blockchain bridges are a crucial piece o targets for attacks.

NEWS

Axie Infinity hack results in $600M cryptocurrency heist

Axie Infinity, whose developer was hacked this month, is a popular NFT-based video game in which players earn cryptocurrency by raising

Cyberattacks and Web3

The nature of attacks

- The vast majority of data breaches are a result of basic lapses in best practices (e.g., laptop stolen, phishing email, simple password, etc)
- While state sponsored attacks do happen, they are more rare and focused generally on bigger institutions

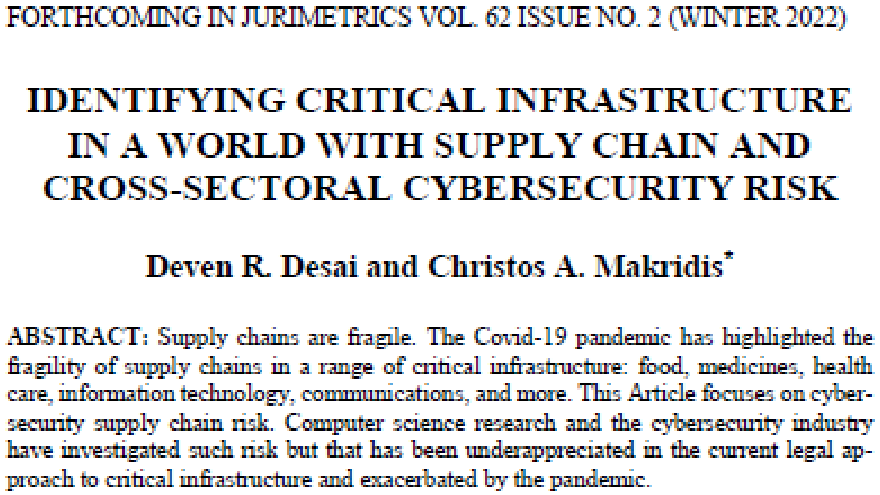
Private keys versus decentralized access

- The bulk – or perhaps all – of the breaches in crypto have been stolen custodial keys (e.g., phishing)
- DEXs are peer to peer, so much less at risk of data breaches
- There are 51% attacks, but that is why the consensus mechanism and true decentralization matters
- Routing attacks are when the hackers intercept data of the user during real-time data transfers by dropping connections in between or hijacking the IP prefixes
- Sybil attacks are when hackers try to gain disproportionate influence over the honest nodes on the network by creating enough fake identities so that they can refuse to receive or transmit blocks, blocking other users from a network

https://www.dailyhostnews.com/are-blockchain-and-web-3-0-under-cyberattack

Primer on Supply Chain Risk

- Forthcoming work of mine with Deven Desai explores one approach to measuring supply chain risk in the cybersecurity landscape
- We look at inter-sectoral linkages – what matters for your vulnerability is not only the vulnerability of your own systems, but also those of your vendors and broader network



FORTHCOMING IN JURIMETRICS VOL. 62 ISSUE NO. 2 (WINTER 2022)

IDENTIFYING CRITICAL INFRASTRUCTURE IN A WORLD WITH SUPPLY CHAIN AND CROSS-SECTORAL CYBERSECURITY RISK

Deven R. Desai and Christos A. Makridis*

ABSTRACT: Supply chains are fragile. The Covid-19 pandemic has highlighted the fragility of supply chains in a range of critical infrastructure: food, medicines, health care, information technology, communications, and more. This Article focuses on cybersecurity supply chain risk. Computer science research and the cybersecurity industry have investigated such risk but that has been underappreciated in the current legal approach to critical infrastructure and exacerbated by the pandemic.

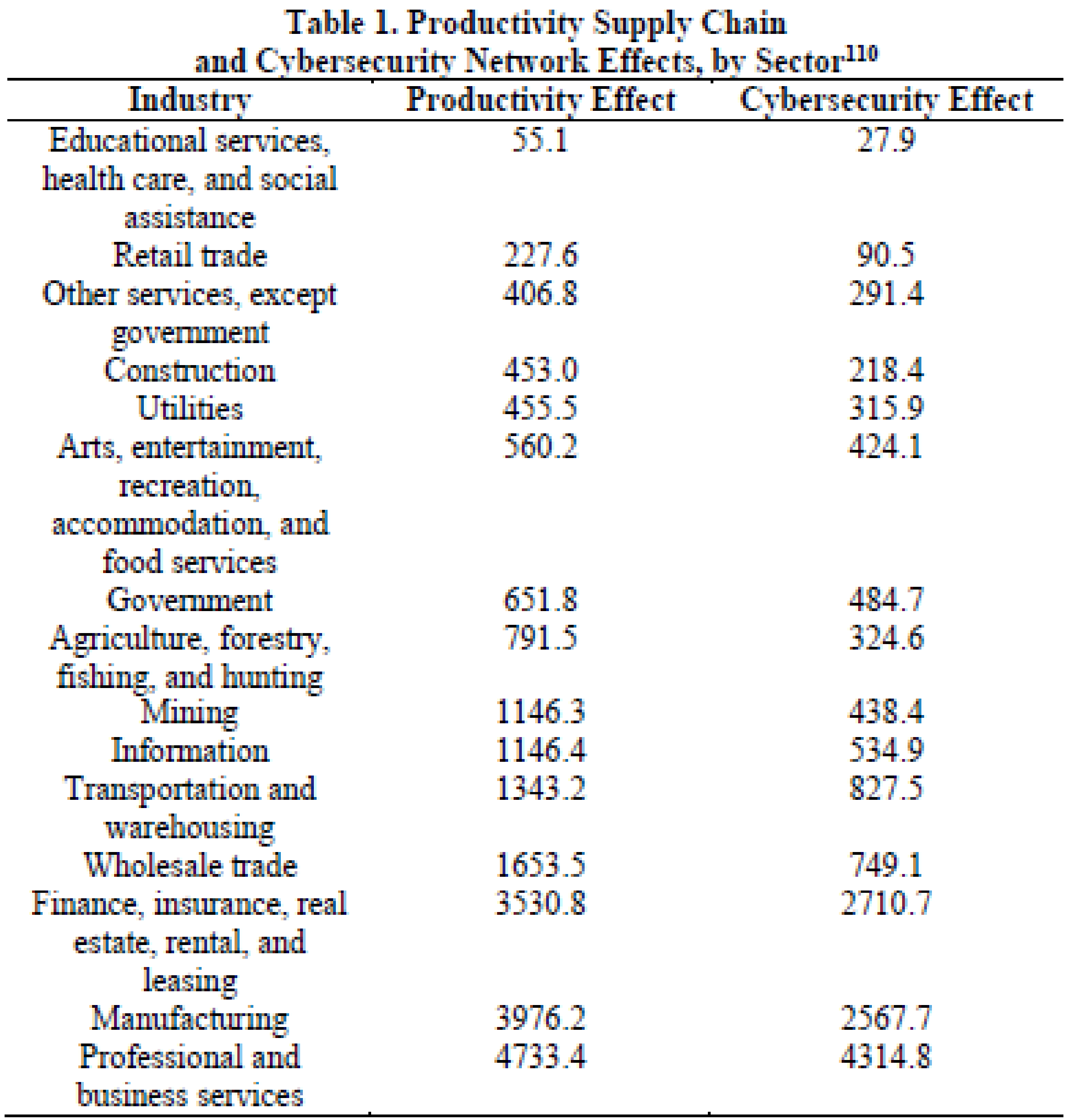
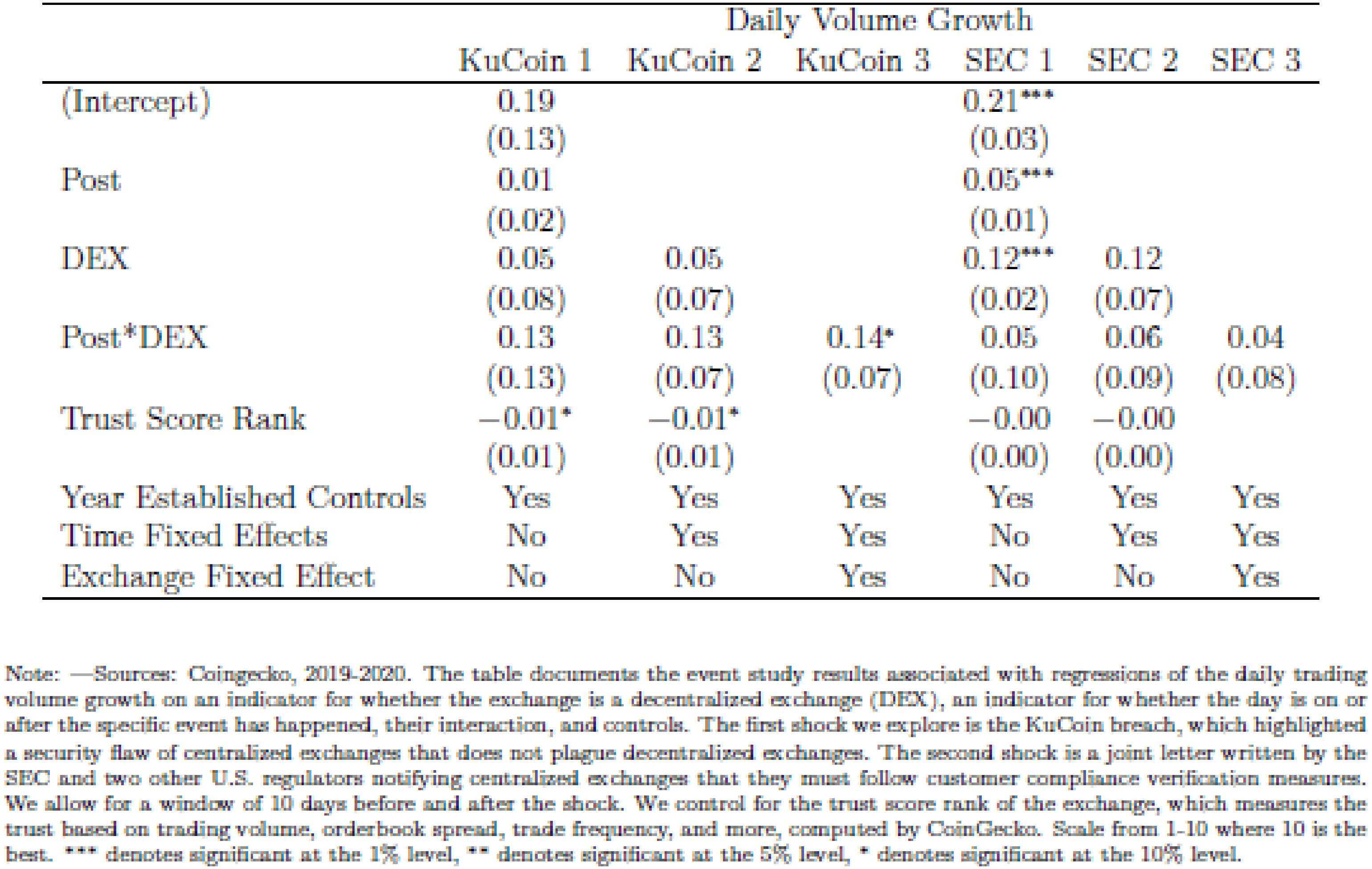


Table 1. Productivity Supply Chain and Cybersecurity Network Effects, by Sector[110]

Industry	Productivity Effect	Cybersecurity Effect
Educational services, health care, and social assistance	55.1	27.9
Retail trade	227.6	90.5
Other services, except government	406.8	291.4
Construction	453.0	218.4
Utilities	455.5	315.9
Arts, entertainment, recreation, accommodation, and food services	560.2	424.1
Government	651.8	484.7
Agriculture, forestry, fishing, and hunting	791.5	324.6
Mining	1146.3	438.4
Information	1146.4	534.9
Transportation and warehousing	1343.2	827.5
Wholesale trade	1653.5	749.1
Finance, insurance, real estate, rental, and leasing	3530.8	2710.7
Manufacturing	3976.2	2567.7
Professional and business services	4733.4	4314.8

Evidence from an Event Study

- In work with Rainer Boehme, Michael Froewis, and Kiran Sridhar, we look at DEXs and CEXs, conducting an event study where we look at volume before/after two events
- In September 2020, KuCoin was breached – we see a rise in volume growth among DEXs after the breach, consistent with people moving to safer options
- (The second event is a letter that US regulatory agencies released in October 2019.)



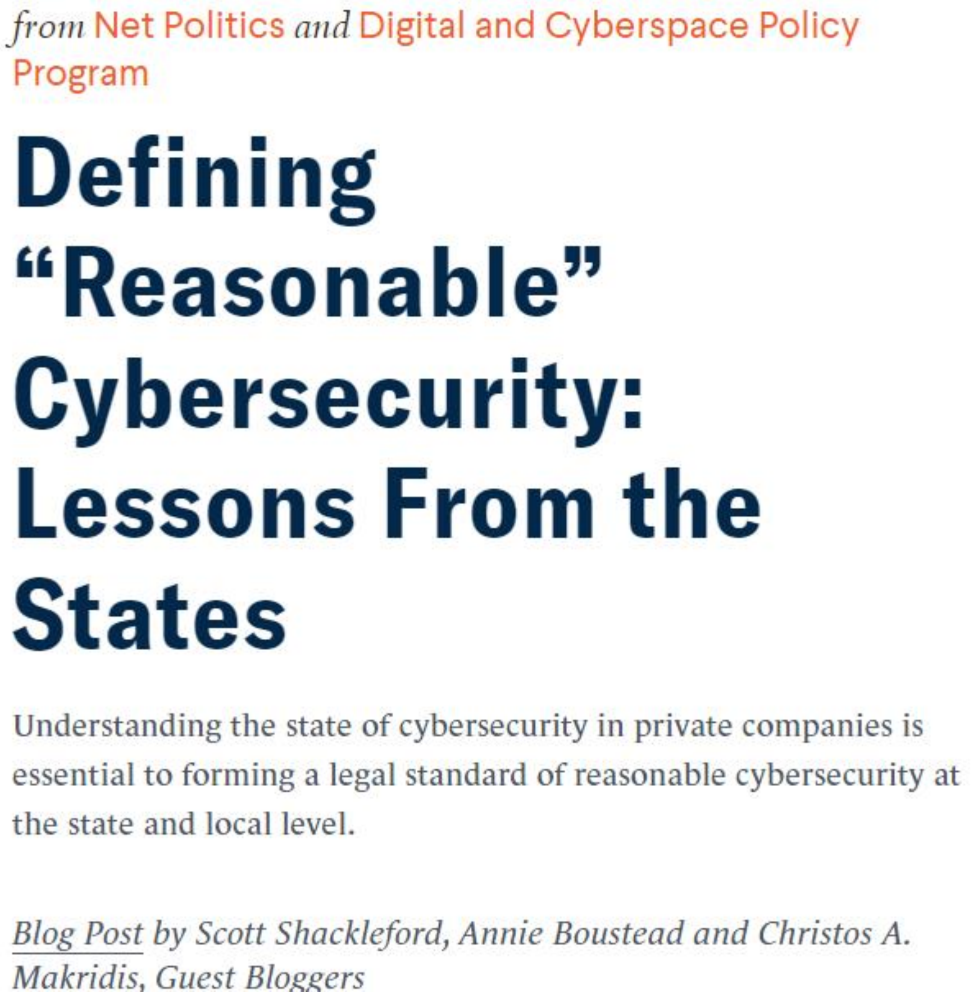
	Daily Volume Growth					
	KuCoin 1	KuCoin 2	KuCoin 3	SEC 1	SEC 2	SEC 3
(Intercept)	0.19			0.21***		
	(0.13)			(0.03)		
Post	0.01			0.05***		
	(0.02)			(0.01)		
DEX	0.05	0.05		0.12***	0.12	
	(0.08)	(0.07)		(0.02)	(0.07)	
Post*DEX	0.13	0.13	0.14*	0.05	0.06	0.04
	(0.13)	(0.07)	(0.07)	(0.10)	(0.09)	(0.08)
Trust Score Rank	−0.01*	−0.01*		−0.00	−0.00	
	(0.01)	(0.01)		(0.00)	(0.00)	
Year Established Controls	Yes	Yes	Yes	Yes	Yes	Yes
Time Fixed Effects	No	Yes	Yes	No	Yes	Yes
Exchange Fixed Effect	No	No	Yes	No	No	Yes

Note: —Sources: Coingecko, 2019-2020. The table documents the event study results associated with regressions of the daily trading volume growth on an indicator for whether the exchange is a decentralized exchange (DEX), an indicator for whether the day is on or after the specific event has happened, their interaction, and controls. The first shock we explore is the KuCoin breach, which highlighted a security flaw of centralized exchanges that does not plague decentralized exchanges. The second shock is a joint letter written by the SEC and two other U.S. regulators notifying centralized exchanges that they must follow customer compliance verification measures. We allow for a window of 10 days before and after the shock. We control for the trust score rank of the exchange, which measures the trust based on trading volume, orderbook spread, trade frequency, and more, computed by CoinGecko. Scale from 1-10 where 10 is the best. *** denotes significant at the 1% level, ** denotes significant at the 5% level, * denotes significant at the 10% level.

Cyber Insurance Has Grown, But Stifled by Lack of Regulatory Clarity

- “For cyber insurance to remain a viable business, insurers and their customers need a new pool of capital to help address the risk of large, generally unlikely (but possible) cyber catastrophes — events that hit multiple companies and cost insurers hundreds of millions of dollars.”
- “Don’t be fooled by the appearance of growth, even if that growth is up 10 percent year over year. Many companies have had to spend more to buy insurance that covers the same or less than it did last year, with premium increases of 25-75 percent — depending on the type of company buying insurance, how much protection they want, and other factors.”

https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money



from Net Politics *and* Digital and Cyberspace Policy Program

Defining “Reasonable” Cybersecurity: Lessons From the States

Understanding the state of cybersecurity in private companies is essential to forming a legal standard of reasonable cybersecurity at the state and local level.

Blog Post by Scott Shackleford, Annie Boustead and Christos A. Makridis, Guest Bloggers

FireEye CEO Kevin Mandia during an interview in Rome, Italy in 2017. FireEye was the first to detect a major Russian intrusion into the cybersecurity vendor SolarWinds. Reuters/Tony Gentile

Guest Lecture – Daniel Kim

UNIVERSITY of NICOSIA

Questions?

Contact:

Christos A. Makridis | Professor | Makridis.c@unic.ac.cy
Marios Touloupos | Teaching and Research Associate | touloupos.m@unic.ac.cy
Evgenia Kapassa | Teaching and Research Associate | kapassa.e@unic.ac.cy