Blockchain Research Design Critique

Presenter: Ruming Liu

Stevens Institute of Technology[1]

MGT-719A Research Design
Dec 11, 2022

Outline

Papers to Discuss

- **Risk And Return of Cryptocurrency**, Yukun L, Aleh T, 2020. Review of Finance Studies.
- **Trading and arbitrage in cryptocurrency markets**, Igor M, Antoinette S, 2020. Journal of Financial Economics.
- **Decentralized Mining in Centralized Pools**, Lin C, Zhiguo H, Jiasun L, 2019. Review of Finance Studies.
- **Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?**, Sean F, Jonathan K, Talis P, 2019. Review of Finance Studies.
- **Blockchain without Waste: Proof-of-Stake**, Fahad S, 2020. Review of Finance Studies.

Cryptocurrency network factors

- Conclusion 1: Cryptocurrency returns are exposed to cryptocurrency network factors.
- Five measures to capture the network effect, including number of active addresses, transaction count, wallet users, payment count and their principle component.
- Coin market returns positively predict future cryptocurrency adoption growth. (See next page)

Cryptocurrency network factors

Predicting future network growth

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				Δuser				
cmkt	0.13***	0.21***	0.28***	0.32***	0.35***	0.36***	0.39**	0.44**
	(4.09)	(3.55)	(3.37)	(3.25)	(2.99)	(2.67)	(2.44)	(2.30)
Cons	0.09***	0.19***	0.28***	0.36***	0.45***	0.53***	0.61***	0.68***
	(7.39)	(6.25)	(5.51)	(5.00)	(4.66)	(4.40)	(4.23)	(4.12)
R^2	0.20	0.15	0.12	0.10	0.08	0.06	0.06	0.06
				Δaddress				
cmkt	0.24***	0.31*	0.29*	0.26	0.22	0.15	0.17	0.15
	(2.94)	(1.94)	(1.79)	(1.54)	(1.25)	(0.94)	(1.24)	(1.20)
Cons	0.04**	0.09***	0.14***	0.20***	0.25***	0.29***	0.33***	0.37***
	(2.61)	(2.78)	(2.85)	(3.15)	(3.54)	(3.98)	(4.24)	(4.36)
R^2	0.26	0.15	0.08	0.05	0.03	0.01	0.02	0.02
				Δtrans				
cmkt	0.14	0.15	0.04	0.04	0.05	−0.02	−0.05	−0.14
	(1.59)	(0.91)	(0.24)	(0.21)	(0.27)	(−0.10)	(−0.35)	(−0.90)
Cons	0.05**	0.10***	0.16***	0.22***	0.26***	0.30***	0.35***	0.40***
	(2.37)	(2.79)	(2.93)	(3.10)	(3.33)	(3.54)	(3.56)	(3.55)
R^2	0.07	0.03	0.00	0.00	0.00	0.00	0.00	0.01
				Δpayment				
cmkt	0.25**	0.32*	0.27	0.23	0.23	0.12	0.11	0.06
	(2.60)	(1.78)	(1.37)	(1.10)	(1.06)	(0.64)	(0.61)	(0.38)
Cons	0.04*	0.09**	0.15**	0.21**	0.26***	0.31***	0.34***	0.38***
	(1.79)	(2.11)	(2.33)	(2.57)	(2.85)	(3.13)	(3.22)	(3.22)
R^2	0.17	0.10	0.05	0.02	0.02	0.01	0.00	0.00

This table reports the results of predicting cumulative future coin network growth with coin market returns. The network factors include wallet user growth, active address growth, transaction count growth, and payment count growth. Data are monthly. The t-statistics are reported in parentheses and are Newey-West adjusted with $n-1$ lags. *, **, and *** denote significance levels at the 10%, 5%, and 1% levels. The data frequency is weekly.

Cryptocurrency production factors

- Conclusion 2: There is limited evidence that the computing factors are important drivers of cryptocurrency returns.
- Eight proxies (electricity costs): Three of the seven primary measures are U.S.-related. The other four measures are China-related.

Panel B. Electricity factor exposures

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
P^{US}	−1.06							
	(−0.34)							
Gen^{US}		0.30						
		(0.38)						
Con^{US}			0.17					
			(0.31)					
P^{CN}				−7.39				
				(−0.72)				
P^{SC}					3.24			
					(0.50)			
Gen^{CN}						0.11		
						(0.12)		
Gen^{SC}							−0.60	
							(−1.16)	
PC^{elec}								−0.00
								(−0.02)
R^2	0.00	0.00	0.00	0.01	0.00	0.00	0.01	0.00

This table reports the factor loadings of the coin market returns on the production factors that relate to electricity costs. Panel A shows the correlation matrix of the production factors. Panel B reports the factor loadings of the coin market returns on the production factors. Standard t-statistics are reported in parentheses. *, **, and *** denote significance levels at the 10%, 5%, and 1% levels based on the standard t-statistics. The data frequency is monthly.

Cryptocurrency production factors

- Conclusion 2: There is limited evidence that the computing factors are important drivers of cryptocurrency returns.
- Six proxies (computing costs):

Panel B. Computing factor exposures

	(1)	(2)	(3)	(4)	(5)	(6)
$\Delta P^{Antminer}$	0.31*					
	(1.90)					
Nvidia		0.50				
		(0.84)				
AMD			−0.02			
			(−0.03)			
TSMC				0.03		
				(0.02)		
ASE					0.45	
					(0.47)	
PC^{comp}						0.00
						(0.04)
R^2	0.09	0.06	0.03	0.00	0.01	0.00

This table reports the factor loadings of the coin market returns on the production factors that relate to computing costs. Panel A shows the correlation matrix of the production factors. Panel B reports the factor loadings of the coin market returns on the production factors. Standard t-statistics are reported in parentheses. *, **, and *** denote significance levels at the 10%, 5%, and 1% levels based on the standard t-statistics. The data frequency is monthly.

Cryptocurrency momentum

- Conclusion 3: The current coin market returns positively and statistically significantly predict cumulative future coin market returns. There is also some reverse effect.

Table 6
Time-series momentum

Panel A. Regression results

Weekly	$R_{t,t+1}$ (1)	$R_{t,t+2}$ (2)	$R_{t,t+3}$ (3)	$R_{t,t+4}$ (4)	$R_{t,t+6}$ (5)	$R_{t,t+8}$ (6)
R_t	0.20**	0.49***	0.81***	1.07***	1.55*	1.62*
	(2.53)	(2.73)	(3.01)	(2.65)	(1.94)	(1.75)
R^2	0.04	0.08	0.09	0.08	0.06	0.02

Cryptocurrency investor attention

- We use keyword 'Bitcoin' to proxy for investor attention in Google trend.
- Conclusion 4: The Google search measure statistically significantly predicts the one-week to six-week ahead cumulative coin market returns at the 5% level.

Table 8
Google searches

Panel A. Regression results

Weekly	$R_{t,t+1}$ (1)	$R_{t,t+2}$ (2)	$R_{t,t+3}$ (3)	$R_{t,t+4}$ (4)	$R_{t,t+6}$ (5)	$R_{t,t+8}$ (6)
$Google_t$	0.03***	0.05***	0.07***	0.10***	0.09**	0.07
	(3.92)	(4.33)	(4.23)	(3.99)	(1.98)	(1.30)
R^2	0.03	0.04	0.03	0.02	0.01	0.00

Cryptocurrency negative attention

- We use keyword 'Bitcoin Hack' to proxy for investor negative attention in Google trend.

Table 9
Bitcoin hack

Panel A. Regression results

Weekly	$R_{t,t+1}$ (1)	$R_{t,t+2}$ (2)	$R_{t,t+3}$ (3)	$R_{t,t+4}$ (4)	$R_{t,t+6}$ (5)	$R_{t,t+8}$ (6)
$Hack_t$	-0.02^{***}	-0.05^{***}	-0.08^{**}	-0.11^{**}	-0.20^{*}	-0.32
	(-3.05)	(-2.93)	(-2.39)	(-2.02)	(-1.67)	(-1.45)
R^2	0.02	0.03	0.03	0.03	0.04	0.03

Other conclusions

- Conclusion 5: There is no consistent evidence of systematic currency exposures in cryptocurrencies.
- Conclusion 6: There is no consistent evidence of systematic precious metal commodity exposures in cryptocurrencies.
- Conclusion 7: The cryptocurrency returns respond to negative regulative events but not to positive regulative events.

Weakness in evaluating investor attention

- The author use google trend to proxy the investor attention.
- But google has much lag compared with social media.
- The negative information about crypto is much noisy compared with the information about equity.

Some Anomaly in cryptocurrency market

- Large and recurring deviations in bitcoin prices across exchanges that open up across different exchanges and often persist for several hours, and, in some instances, days and weeks.
- Price deviations are much larger across countries (or regions) than within the same country.
- Deviations in bitcoin prices across countries are highly asymmetric.
- Price deviations occur during periods of a particularly quick appreciation(buying pressure) of bitcoin prices.

Arbitrage index

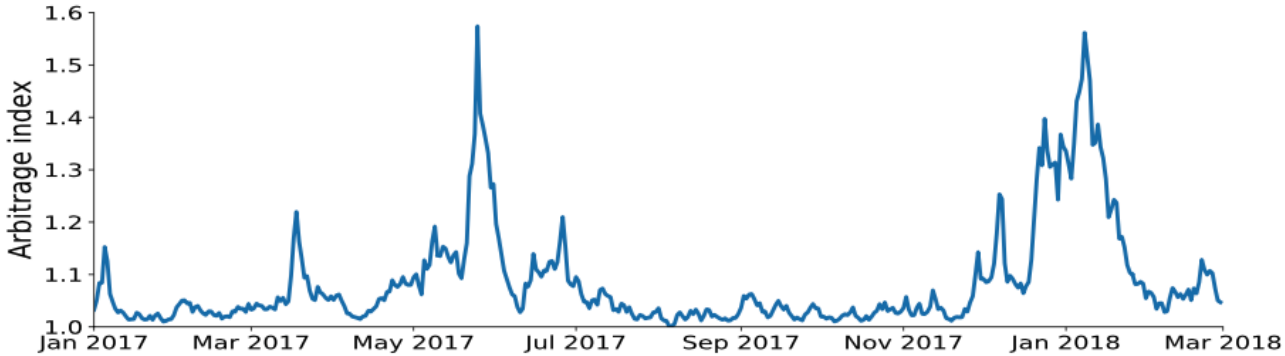
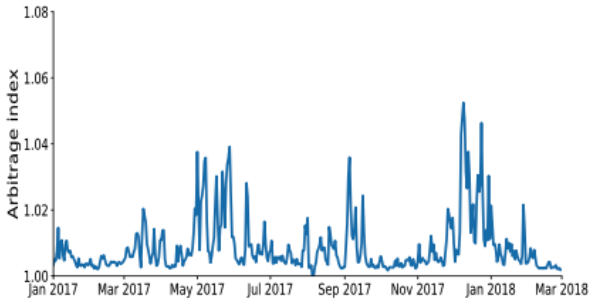
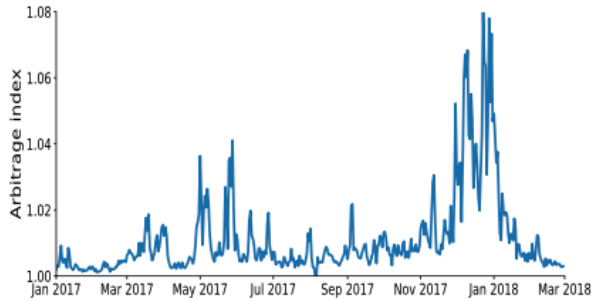


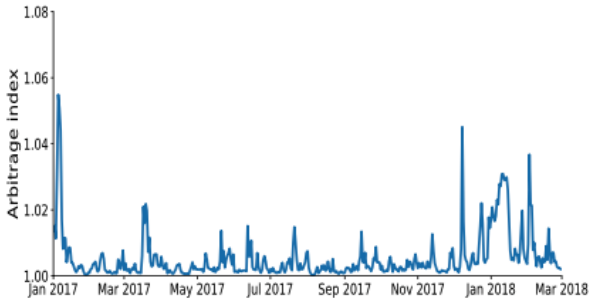
Fig. 2. Arbitrage index. The arbitrage index is calculated based on the volume-weighted price per minute for each exchange and averaged at the daily level. For a given minute the maximum volume-weighted price across all exchanges is divided by the minimum volume-weighted price in that minute. The set of exchanges include Binance, Bitfinex, bitFlyer, Bithumb, Bitstamp, Bittrex, Coinbase, Gemini, Kraken, Korbit, Poloniex, Quoine, and Zaif from January 2017 until February 28, 2018.

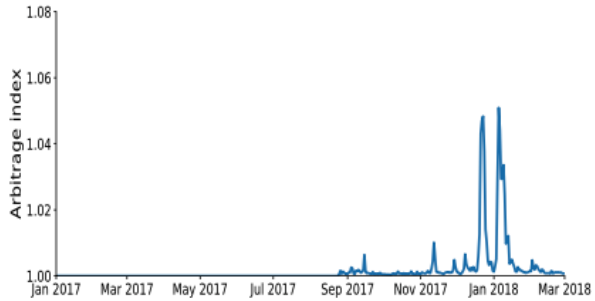


Panel A: USA

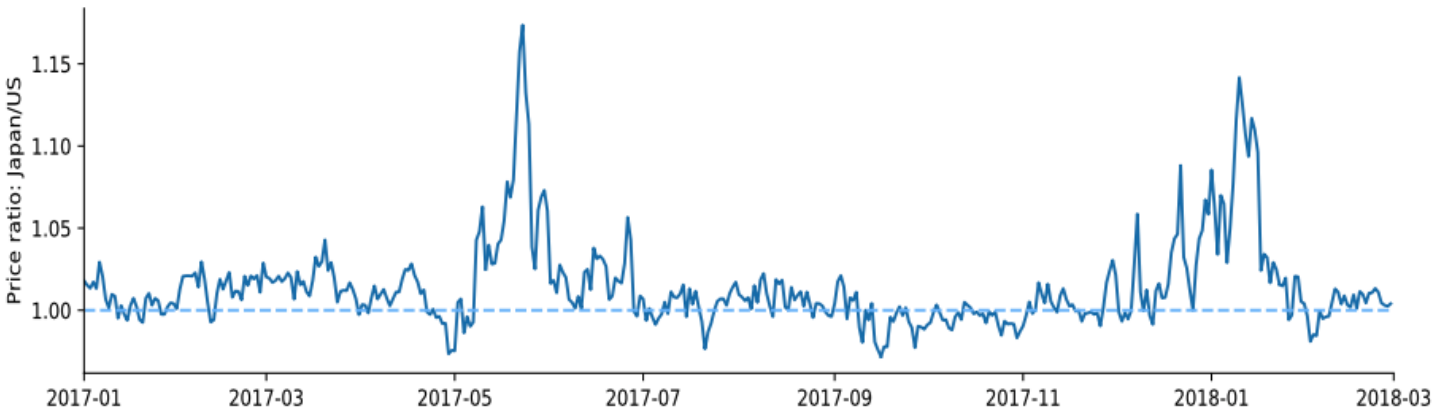


Panel B: Europe

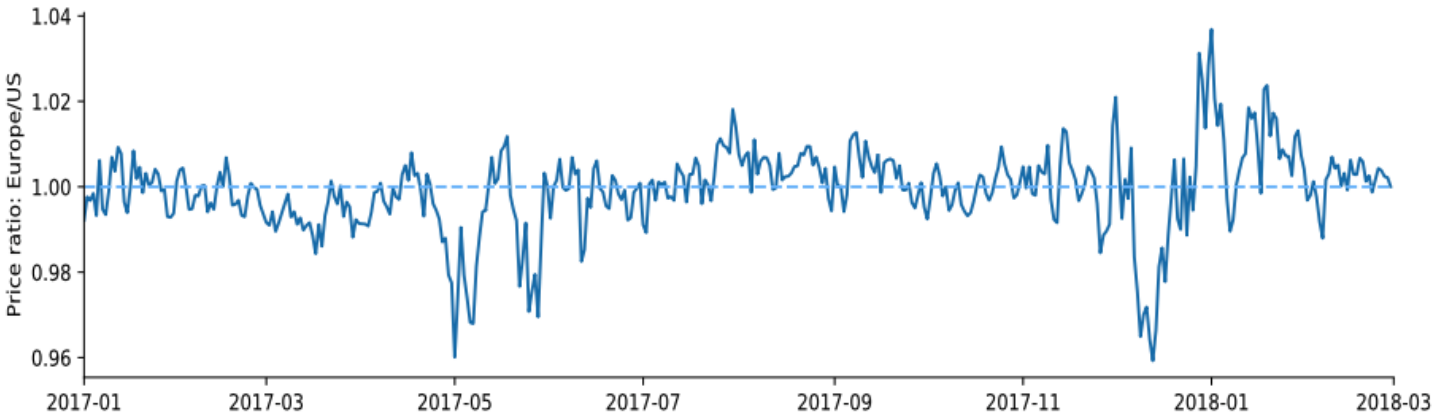




Price ratio across regions

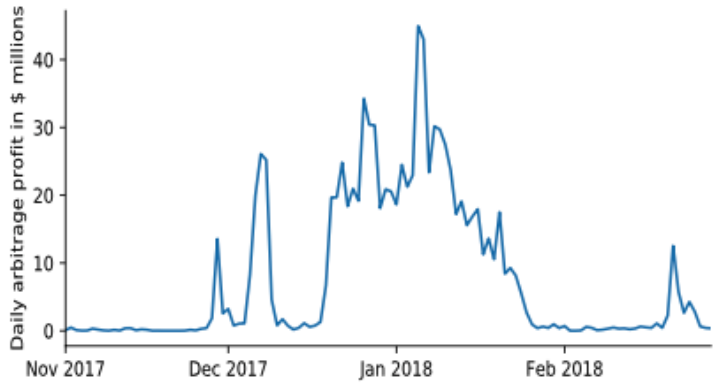


Panel B: US vs. Japan

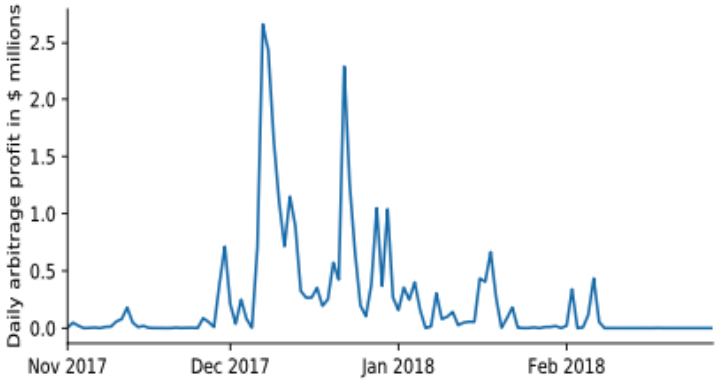


Panel C: US vs. Europe

Arbitrage profit across regions



Panel A: US and Korea



Panel C: US and Europe

- Above results not hold for crypto to crypto.

Capital control

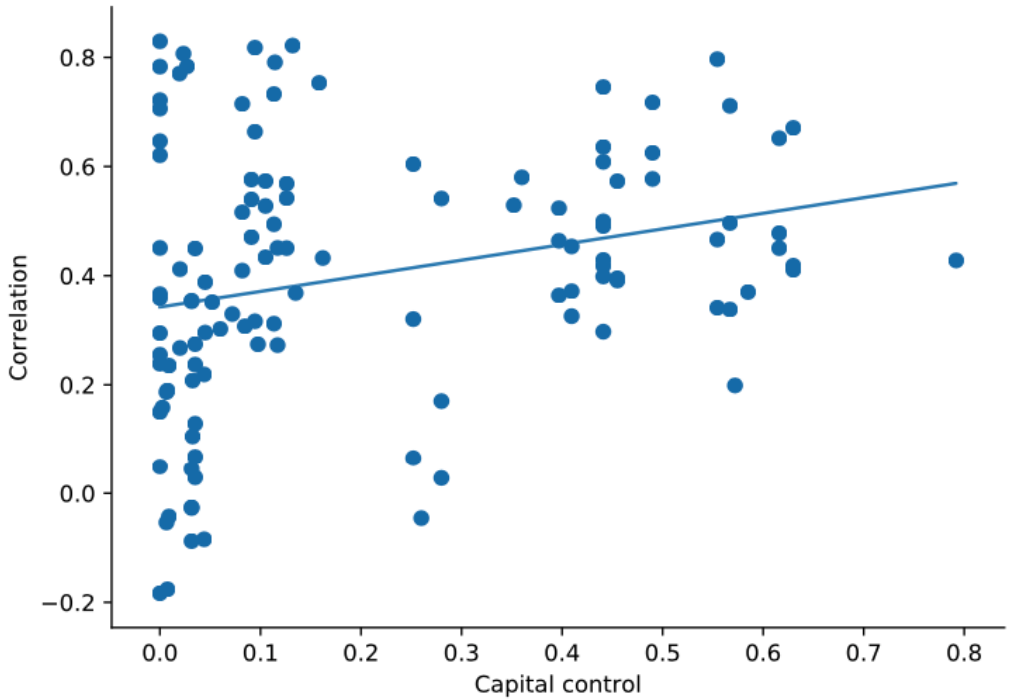


Fig. 9. Correlation in arbitrage spreads and capital control. The results in this figure are based on a data set of pairwise correlations in arbitrage spreads between two countries and a measure or pairwise capital controls, which is the product of the capital control index of the two countries. The capital control measure is based on the measure of capital market openness from the NBER database by Fernández et al. (2015). The closer both countries are the closer the measure to one. The slope of this regression is 0.29 with a t-statistic of 3 and a R^2 of 0.07.

- Captial control can explain some arbitrage opportunity.
- Two countries that are both relatively closed to capital flows have a higher correlation in arbitrage spreads.

Conclusions

- The lack of of regulatory oversight may create impediments for large public institution to enter the cryptocurrency space and slow down the supply of arbitrage capital.
- The spreads in the rest of the world are almost always positive relative to the US and Europe and go up more during times of large bitcoin appreciation.
- This pattern suggests that the marginal investors who price cryptocurrencies in countries with less developed capital markets value cryptocurrencies more highly, possibly because they have a higher convenience yield for bitcoin.

Weakness

- All of the trade comes from centralized exchange.
- But centralized exchange activity is off-chain.
- DEX and P2P trade can also be included for analysis.
- Stable coin arbitrage.

How many illegal activities in blockchain?

- Some illegal trades have been seized by government in Silk Road case.
- Illegal darknet marketplaces and users can also be detcetd.
- Based on above illegal samples, two methods to expand the search:
- 1. Network cluster analysis
- 2. Detection-controlled estimation (DCE)
- At the early stage of bitcoin, bitcoin is cheap and number of users are small, illegal users held 60% volume of bitcoin. When bitcoin became more valuable. and volatile since 2015, their holding mount is decreasing.

Characteristics of illegal user

- Holding amount: Illegal users predominantly using bitcoin to buy and sell goods and services, whereas some legal users also use bitcoin for investment and speculation.
- Counterparties: Illegal users are more likely to repeatedly transact with a given counterparty. This characteristic might be a reflection of illegal users repeatedly transacting with a given illegal darknet marketplace or other illegal user once trust is established from a successful initial exchange.
- Illegal users tend to become involved in bitcoin earlier than legal users. Similarly, the differences in means also show a higher proportion of pre-Silk-Road users among the illegal users than the legal users.

Implications and Conclusion

- The paper can help to reduce the uncertainty about the negative consequences of cryptocurrencies, allowing for more informed decisions by policy makers that assess both the costs and benefits.
- A second contribution of this paper is the models can be applied by law enforcement authorities.
- Our finding that a substantial amount of illegal activity is facilitated by bitcoin suggests that bitcoin has contributed to the emergence of an online black market, which raises several welfare considerations.
- Our results also have implications for the intrinsic value of bitcoin.

Weakness

- There is no enough backtesting for the result.
- May not work well on other blockchain which has higher privacy.
- Will the illegal e-commerce makes community safer?

Mining pool growth

- Mining pools grew from constituting only 5% of global hash rates (a measure of computation power devoted to mining) in June 2011 to almost 100% since late 2015

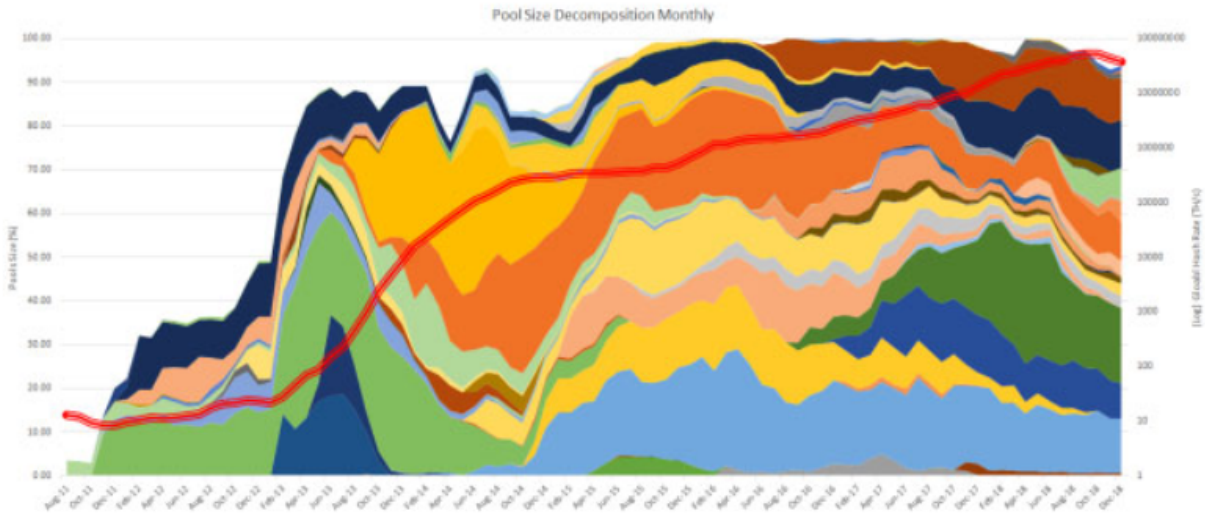


Figure 1
The evolution of Bitcoin mining

Mining pool growth

- Pool sizes seem to exhibit a mean-reverting tendency, suggesting concurrent economic forces suppressing overcentralization.

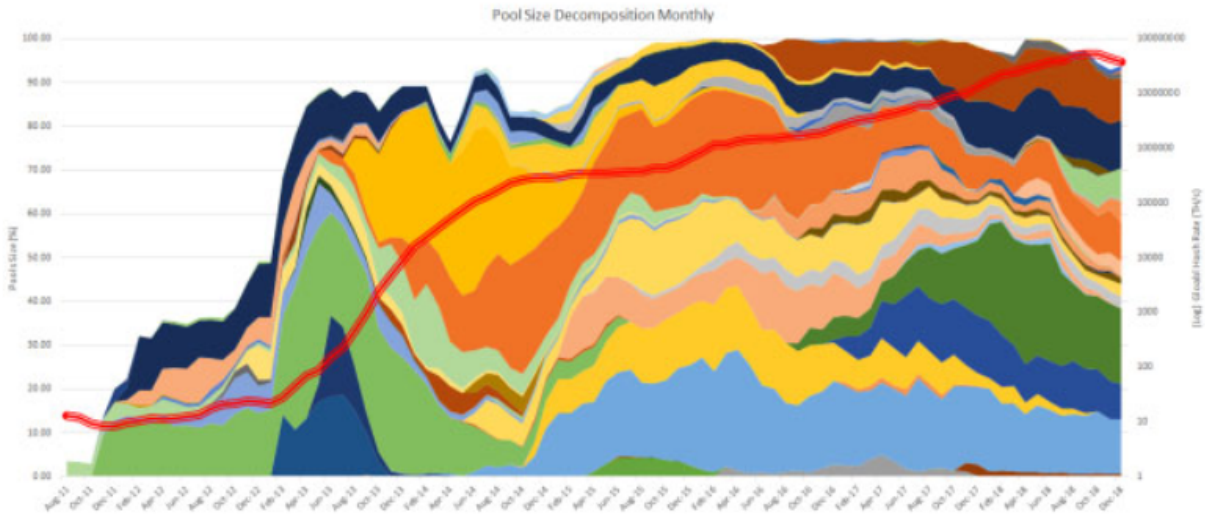


Figure 1
The evolution of Bitcoin mining

Why miner join the mining pool

- Why miner join mining pool?
- The significant risk-sharing benefit offered by mining pools to individual miners.
- Will miner only join one mining pool?
- Not necessary. Perfect risk sharing could be obtained, and the exact pool size distribution is irrelevant. The risk-sharing benefit within a large pool could be alternatively obtained through miner's diversification across multiple small pools.

Fee contracts in mining pools

- Management fee: Mining pool is often maintained by a pool manager, who takes a percentage cut from miners' rewards at payout.
- All classes of fee contracts effectively use a miner's hash rate as a contracting variable.
- Two types of payoffs.
- Payoff based on bonus sharing. (Our focus)
- Payoff based on fixed salary.

Over centralization

- If each miner could only join one pool, then in practice a larger pool would always charge a low enough fee to attract more miners, leading to a single pool dominating the entire industry.
- Agents in traditional industries can decide how much effort or input to provide, they can rarely work for multiple firms at the same time (the concept of diversification). But miners can join multiple pools.
- As long as miners can join pools in a frictionless way, one should not expect a single large pool to emerge.
- miners with a given level of risk aversion would acquire hash rates more aggressively when mining in pools, which escalates the mining arms race and amplifies the energy consumption associated with cryptocurrency mining.

Weakness

- How does the reallocation happen in mining pool?
- Didn't consider the long run block reward diminishing.

Proof-of-Stake Protocol

- PoS replaces PoW's competition by offering a randomly selected stakeholder the authority to update the blockchain. As such, PoS omits any incentive for validators to engage in a computational arms race.
- Detractors assert that this lack of an explicit cost coupled with the explicit benefit of the block reward implies that a validator will always update the ledger whenever given the opportunity even if the update necessarily perpetuates disagreement. This assertion is known as the **Nothing-at-Stake problem**.

Nothing-at-Stake

- Miners who has received the opportunity to append a block on a branch of the blockchain. The argument highlights that a player receives a block reward if she appends the block and nothing if she does not append the block.
- This may casue the **tragedy of the commons**.
- This will not happen in the PoS protocol.
- Some PoS implementations (e.g., Ethereum's Casper) combat the Nothing-at-Stake problem with explicit punishment schemes
- Minimum stake requirement.

Solve the disagreement (Fork)

- Developers should restrict players with small stakes from appending to the blockchain.
- The condition given above also may be read as a restriction on block rewards instead of a restriction on eligible stakeholders.
- A more typical resolution: a PoS blockchain obtains consensus without further conditions if the blockchain possesses no block reward.
- Soft fork: Sufficiently modest block reward schedule precludes a persistent forking equilibrium
- Conclusion: To generate consensus more easily, PoS protocols should impose minimum stake requirements and maintain low block reward schedules. This guidance does not apply to PoW protocols.

Weakness

- Wealth concentration issue?
- PoS blockchain security?

Thanks!

E-mail: rliu38@stevens.edu