Stevens Institue of Technology

Blockchain Research Review

Research Design Term Paper

Author: Ruming Liu*
Advisor: Chihoon Lee

December 19, 2022

1 Abstract

A blockchain is a virtual chain of ordered blocks, and it is a decentralized ledger which can let traders trade cryptocurrency through the network without a centralized intermediary. Bitcoin (BTC), one of the most famous and earliest cryptocurrency in blockchain was invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto[1], has reached more than $60,000/BTC in 2021. Cryptocurrencies have grown rapidly in price, popularity, and mainstream adoption. Over 1,800 cryptocurrencies exist with market capitalization exceeding $300 billion as at July 2018. Fiinancial markets and technology industry have put a lot of attention on this 'digital gold' FinTech. Recently, several researches talk about this innovation in academia. And in this paper, we will review below five of blockchain papers which are published on top finance journal.

- **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.

*rliu38@stevens.edu

[1]Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system.

- **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.

2 Risk And Return of Cryptocurrency [2]

Cryptocurrency now is becoming a mainstream investment asset with significant return but high volatility. This paper has a comprehensive analysis of cryptocurrency return and risk. The author constructing an index of cryptocurrrency market returns. The index is the value-weighted returns of all cryptocurrencies with capitalizations of more than 1 million USD and covers the period of January 1, 2011 to December 31, 2018.

During the sample period,, the average of the index returns at the daily, weekly, and monthly frequencies are 0.46%, 3.44%, and 20.44%, respectively. The daily, weekly, and monthly standard deviations of the index returns are 5.46%, 16.50% and 70.80%. The index return has positive skewness and kurtosis. We note that the mean and standard deviation of crypto index return are much higher than most of stock returns during the same period. The paper tries to explain the relationship between the crypto index return and the main crypto-specific factors. Below are the list of factor explaination and effect to the index return.

- **Cryptocurrency network factors**: We use four measures to proxy for the network effect: the number of wallet users, the number of active addresses, the number of transaction count, and the number of payment count. The regression results show the network factors that measure the network effect of user adoptions are important drivers of cryptocurrency prices. We find that coin market returns positively predict future cryptocurrency adoption growth.
- **Cryptocurrency production factors**: We construct production factors of cryptocurrency to proxy for the cost of mining. We separately construct proxies for electricity costs and computing costs. After the statistical test, we conclude index returns are not significantly exposed to the cryptocurrency production factor.
- **Cryptocurrency momentum**: We regress cumulative future coin market returns on current coin market returns from the one-week to eight-week horizons. The current index returns positively and statistically significanly predict cumulative future index returns.
- **Investor attention**: We construct the deviation of Google searches for the word "Bitcoin" in a given week compared with the average of those in the preceding four weeks. We standardize the Google search measure to have a mean of zero and a standard deviation of one. Our result is that a one-standard-deviation increase in searches leads to increases in weekly returns of about 3% for the one-week ahead cumulative coin market returns and about 5% for the two- week-ahead cumulative coin market returns.

[2] Risk And Return of Cryptocurrency, Yukun L, Aleh T, 2020. Review of Finance Studies.

- **Cryptocurrency valuation ratios**: We regress the coin market returns on the lagged cryptocurrency fundamental-to-market ratios, but there is only a very weak relationship between the future coin market returns and the current cryptocurrency fundamental-to-value ratio.

The author does a comprehensive statistical test for the return and risk of crypto returns. He uses a large sample data to test the factors effect. There is still some weakness can be expand to further research in this paper.

- The author uses google trend to proxy the investor attention, but some researches argue that google has much lag compared with social media. And the information in social media about crypto is noisier compared with the information about equity. So we think, we can do further test for the social media sentiment effect to the crypto index returns.

3 Trading and arbitrage in cryptocurrency markets[3]

In cryptocurrency market. There are many nonintegrated exchanges that are independently owned and exist in parallel across countries. On an individual basis the majority of these exchanges function like traditional equity markets where traders submit buy and sell orders, and the exchange clears trades based on a centralized order book. However, in contrast to traditional, regulated equity markets, the cryptocurrency market lacks any provisions to ensure that investors receive the best price when executing trades. The absence of such mechanisms increases the role of arbitrageurs who can trade across different markets, in this paper, the author analyze the arbitrage opportunity and activity in crypto market.

The author uses tock data from 34 exchanges across 19 countries of the period from January 1, 2017 to February 28, 2019. He calculates the arbitrage index in Figure 1 to represent the spread of the bitcoin, arbitrage index is larger or equal to 1, the larger index means higher price spread. Overall, the results show that the arbitrage opportunities are much smaller within regions than across regions. This result suggests that cryptocurrency exchanges within a given country or region seem to be much better integrated than across regions. To confirm that the arbitrage spread is driven by price deviations across regions, the author also tests that the arbitrage spread between U.S. and Asia are much bigger than the spread between U.S. and Europe. This is lead by the same set of exchanges both operate in the US and Europe. The next question is when the spread will appear? The author calculates the cryptocurrency buying power in U.S. and found that the arbitrage opportunity will appear when there is large buying power in U.S.

Author has several explanation for the anomaly.

- The aurthor tests the arbitrage between cryptocurrencies and doesn't find significant arbitrage opportunity. The author claims the arbitrage is caused by capital control, he finds that there is a significantly positive relation between the correlation of arbitrage spreads and capital controls.

[3]Trading and arbitrage in cryptocurrency markets, Igor M, Antoinette S, 2020. Journal of Financial Economics.

- The regions with capital control on average, have a higher convenience yield for bitcoin. So these countries respond more strongly in widening arbitrage deviations in times when buying pressure goes up in the US.

Some weakness for the data and methodology.

■ All of the trade comes from centralized exchange. But centralized exchange activity is off-chain. Decentralized exchange and Peer-to-peer trade can also be included for analysis.

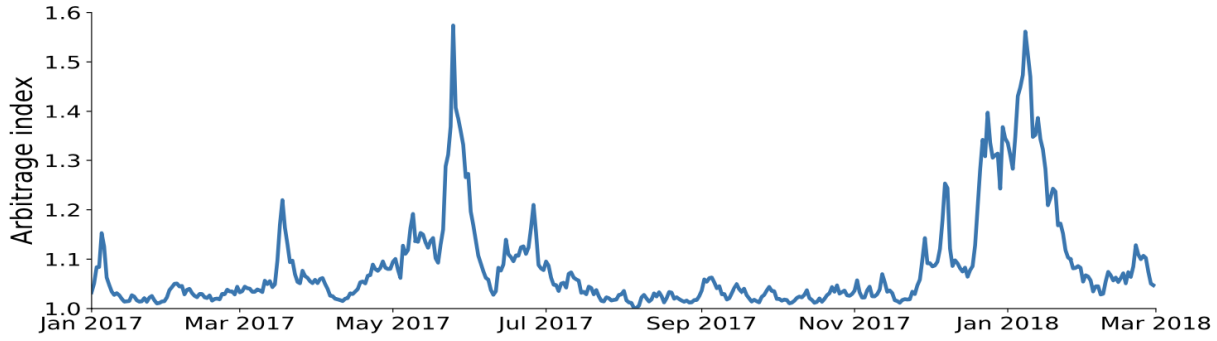
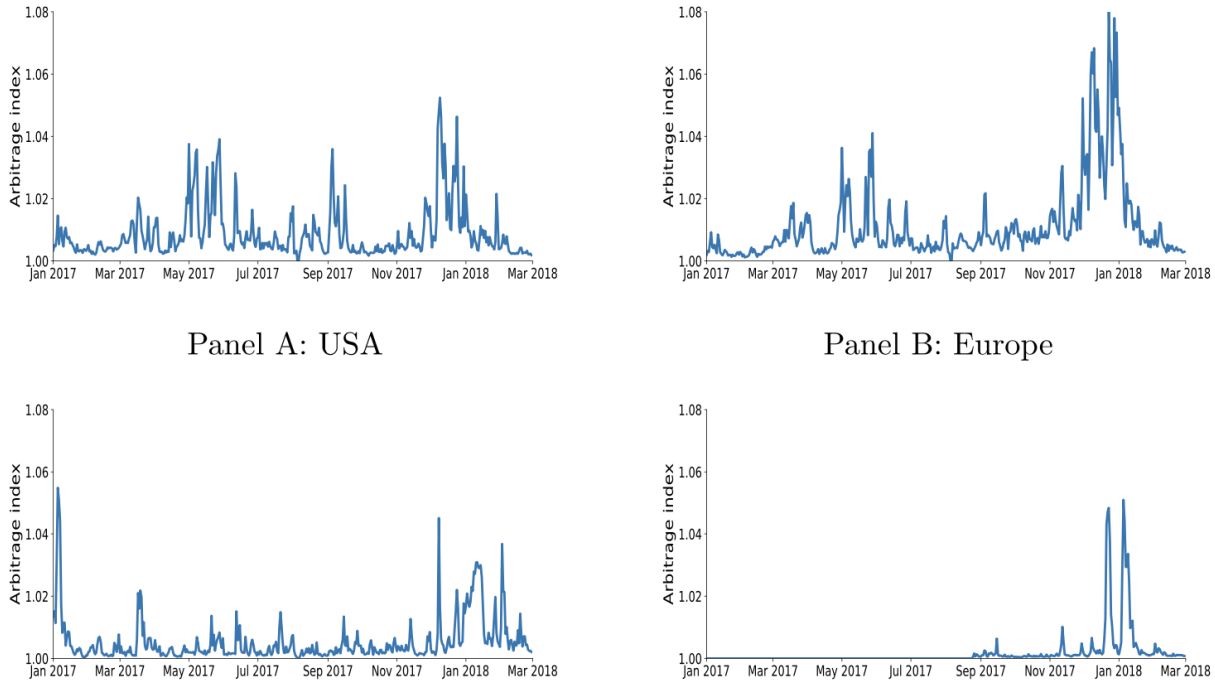


Fig. 2. Arbitrage index. The arbitrage index is calculated based on the volume-weighted price per minute for each exchange and averaged at the daily level. For a given minute the maximum volume-weighted price across all exchanges is divided by the minimum volume-weighted price in that minute. The set 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

Panel C: Japan

Panel D: Korea

Figure 1: Arbitrage index of whole market and different regions

4 Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies

Since the creation of bitcoin, there is a lot evidences that the crypto is involved with illegal trading and activities. In 2013, some illegal trades have been seized by government in Silk Road case. Illegal darknet marketplaces and users can also be detected. With above illegal users samples, the author use two methods to expand the illegal users search: 1. Network cluster analysis. 2. Detection-controlled estimation (DCE). The author uses above 'detected' users to train above two models. Then he uses the trained model to predict the whole bitcoin blockchain illegal users. Here are some general characteristics of illegal users:

- **Less 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.
- **Concentrated 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.
- **Ealier users in blockchain**: 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.

Some improvement in this paper:

- There is not enough backtesting for the prediction. The results in the paper are prediction based on the past information, if there is validation process, the result may be more robust.
- May not work well on other blockchain which has higher privacy.
- If the online market for illegal goods and services merely reflects a migration of activity that would have otherwise occurred "on the street" to the digital world of e-commerce. Will this migration cause welfare improvement for the society?

5 Decentralized Mining in Centralized Pools

In the design of bitcoin whitepaper, Satoshi anticipates at the begining, the blockchain miners are distributed. He also predicts in the future when the bitcoin price goes up, miners may collaborate to become a league. The prediction is valid in Fig 2, from the red line, we can see 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. It also reveals that pool sizes seem to exhibit a mean-reverting tendency, suggesting concurrent economic forces suppressing overcentralization. Autors have some explanation and proof for the mining activities:

- They illustrate the significant risk-sharing benefit offered by mining pools to individual miners: under reasonable parameters, the certainty equivalent of joining a pool more than doubles that of solo mining.
- They also explain why a large pool would not grow even larger. In a frictionless benchmark, 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.
- 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.

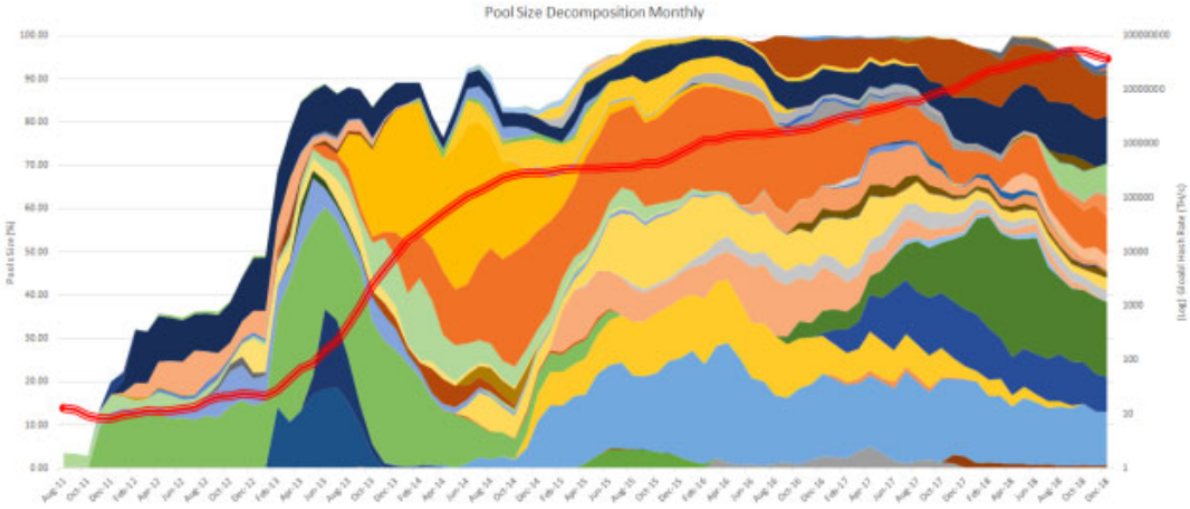


Figure 2: Arbitrage index of whole market and different regions

This paper formally develops a theory of mining pools that highlights risk sharing as a natural centralizing force. It explains why a blockchain system could remain decentralized over time and find empirical evidence from the Bitcoin mining industry that support the theory. Several future researches can be done in this topic:

- How does the reallocation happen in mining pool? Will the large miner quit the pool first or the small miner quit first?
- The block reward will be half around every four years, the model doesn't consider the long run block reward diminishing. Will the equilibrium still persist in the long run?

6 Blockchain without Waste: Proof-of-Stake

In blackchain, the most prominent proof-of-work (PoW) blockchain, consumes electricity at a level comparable with countries such as Austria and Ireland. In hopes of creating a sustainable permissionless blockchain (i.e., one that does not expend an exorbitant amount of energy), the blockchain community has bandied about several alternatives to PoW, one of them is proof-of-stake (PoS). A valid concern is that whether PoS can lead to consensus agreement in the miners game. This paper provides the first formal economic model of PoS and establishes conditions under which PoS generates consensus.

The most concern of PoS is the nothing-at-stake problem. The Nothing-at-Stake problem assumes an initial disagreement and argues that this disagreement will persist indefinitely for a PoS protocol. More formally, the setting assumes a fork exists on the blockchain and argues that each branch of the fork will receive a new block during each time period. The fact that the blockchain branches evolve in this way is taken as persistent disagreement because multiple branches are receiving regular updates, and each branch represents a different ledger.

The Nothing-at-Stake problem implicitly makes a price-taking assumption so that a validator does not internalize the effect of her decisions on the value of the blockchain's native coin. This assumption is not appropriate for a validator in a PoS setting. If a validator appends to the blockchain in a way that perpetuates disagreement, then she imposes a cost on all stakeholders because her action undercuts the ability of users to exchange the native coin and thereby lowers its value. PoS grants authority to update the blockchain to only stakeholders; thus, within PoS, a validator imposes a cost on herself if she updates the blockchain in a manner that persists disagreement.

After solving the nothing-at-stake concern, the aurthor prove seral conclusions for mechanism design:

- A minimum stake requirement requires that the PoS protocol restrict access to update the ledger to sufficiently large stakeholders. A modest block reward schedule requires that block rewards offered to validators for updating the ledger be kept small. Both the discussed measures help generate consensus within a PoS protocol.
- A PoS blockchain obtains consensus without further conditions if the blockchain possesses no block reward. This result arises because a player incurs a cost for delaying consensus but receives no off-setting reward for appending to the blockchain's shorter branch.
- A sufficiently modest block reward schedule precludes a persistent forking equilibrium. This situation is called soft fork in blockchain industry. There is only temporary fork, and the agreement will finally be obtained.

But several concerns are not solved in this paper:

- **Wealth concentration concern**: Will the wealthy validator become richer?
- **PoS blockchain security**: In the PoW protocol, there is a typical attack where a large computation power is controled by a single node. In the PoS protocol, will the rich validators control the blockchain in the long run?

7 Conclusion

As an emerging FinTech innovation, cryptocurrencies and the blockchain technology on which they are based could revolutionize many aspects of the financial system, ranging from smart contracts to settlement, interbank transfers to venture capital funds, as well as applications beyond the financial system. Like many innovations, cryptocurrencies also have their own problems should be solved, in this review, we recall some theoratical and empirical papers to enhance the potential of blockchain technology.

References

[1] Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system.

[2] Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2019. The blockchain folk theorem. Review of Financial Studies 32:1662–715.

[3] Fahad, S 2021. Blockchain without Waste: Proof-of-Stake.

[4] Cong, L. W., Z. He, and J. Li. 2020. Decentralized mining in centralized pools.

[5] Emiliano, P 2021. Decentralizing Money: Bitcoin Prices and Blockchain Security.

[6] Lowe D G. Distinctive image features from scale-invariant keypoints, International journal of computer vision, 2004, 60(2): 91-110.

[7] de Vries, A. 2018. Bitcoin's growing energy problem. Joule 2:801–5.

[8] Zamfir,V. 2017. Casper the Friendly Ghost: A correct-by-construction blockchain consensus protocol. Report, Ethereum Foundation, Zug, Switzerland. https://github.com/ethereum/research/blob/master/papers/CasperTFG/CasperTFG.pdf.

[9] Xiao et al. (2020) survey distributed consensus protocols and discuss the FTS algorithm within the PoS. section.

[10] Risk And Return of Cryptocurrency, Yukun L, Aleh T, 2020. Review of Finance Studies.

[11] Trading and arbitrage in cryptocurrency markets, Igor M, Antoinette S, 2020. Journal of Financial Economics.

[12] Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies, Sean F, Jonathan K, Talis P, 2019. Review of Finance Studies.