Ihssan Tinawi
Survey Paper
14.18 – Mathematical Economic Modeling
Professor Alexander Wolitzky

An Economic Analysis of Bitcoin Transactions: Guessing the Underlying Fiat of Cryptocurrency Transactions

Bitcoin is a decentralized payment system built on top of a distributed ledger known as a blockchain. Proposed in 2008 by Satoshi Nakamoto, the system employs a clever mix of cryptography and game theory to solve distributed consensus problems of who owns which coins and how they can spend them[1]. Since then, Bitcoin and other similar "cryptocurrencies" have gained tremendous attention from both the media and investors, with the price of Bitcoin increasing twenty-fold in 2017 alone to hit a peak of around 20,000 USD before correcting back to around 12,500 USD by the end of the year (a marvelous feat, nonetheless)[2]. Bitcoin has also caught the attention of academics who have taken to study topics like the technology behind it, the economics of its payments, among several other novel subject matters. In this paper, we carry out an economic analysis on the two aspects of Bitcoin data: exchange rates and mining revenues. For the exchange rates analysis, we analyze a period of Bitcoin transactions spanning from December 4 to 9 in 2017 using specific heuristics to predict the fiat currencies underlying those transactions. We find that 18.3% of transactions are carried out in US Dollars, 20.5% in Chinese Yuan, 19.9% in Japanese Yen, and 12% in Korean Won. The predictions were evaluated using an additional heuristic, that was based on time zones before making a decision on which

[1] https://bitcoin.org/bitcoin.pdf
[2] Prices provided by https://www.coindesk.com/price/, which averages Bitcoin prices across major exchanges

currency a transaction was made in. Finally, our analysis shows that miners have accumulated around 900,034 Bitcoins from partaking in the proof of work scheme that cements information into blocks, indicating a market size of around $3.65 bn in revenue.

At the core of bitcoin's infrastructure is a system of servers, each called a miner, that are trying to mint a block by solving cryptographic puzzles (this "proof-of-work" system is present in Bitcoin but not all cryptocurrencies). As shown in Figure 1 below, a block in Bitcoin is comprised of a hash of the previous block, a list of valid transactions, a nonce, and a timestamp. When a series of blocks point to each other, they form a "blockchain" that act as a public ledger of all previous transactions. Miners have an incentive to expend resources and energy to solve the mining problems, since they receive a predetermined number of Bitcoins for every block they mine from the starting transaction which is also known as the "coinbase" transaction. From the user's point of view, any pair of private/public keys can receive and send Bitcoins or parts of one. A user can only transact with Bitcoins he/she/it has and can prove ownership of by signing the transaction with the private key. To incentivize miners to process their transactions, users typically pay a transaction fee that's determined by supply and demand. We'll go further into these concepts later as needed, but for now we have a framework with which we can understand how Bitcoin functions.

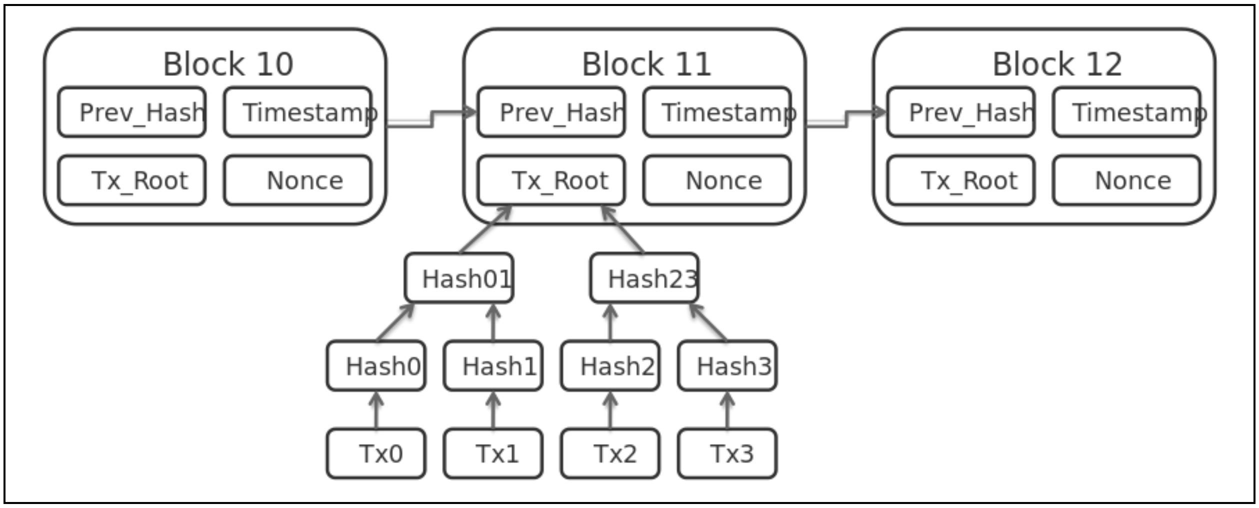

Figure 1: Bitcoin Blockchain Format
Source: https://commons.wikimedia.org/wiki/File:Bitcoin_Block_Data.png

Blocksci Blockchain Analysis Tool

Blocksci is an open-source project that was developed by a research group at Princeton University in 2017. The tool is meant to serve as a blockchain-agnostic analysis tool for several cryptocurrency transaction databases. By focusing on performance of the software system, the team was able to create a tool that is useful for both scientific and commercial research. In this paper, we use Blocksci as the primary tool for analysis. Using Blocksci's functionalities, we query the Bitcoin blockchain to filter out blocks in the range of dates we are interested in. After that, we can back out all the transaction data in each of these blocks and query them using simple Python code. For more information on how we used Blocksci, please refer to the project codebase which is linked in the Appendix.

Exchange Rate Analysis

One of the questions we were interested in answering in this paper was whether we could make any guesses about the fiat currency underpinning Bitcoin transactions. That is to say, if we look at the output of an unspent bitcoin transaction, can we try to infer what the underlying currency of the user is, i.e. what is the currency of the market that the user is transacting in? This research question immediately runs into some limitations, since cross-currency transactions might be taking place. However, answering it gives us insight into the volume of exchange happening in a certain currency on the Bitcoin blockchain. Our analysis develops a few heuristics to try and predict what percentage of transactions are carried out in currencies that have large cryptocurrency markets. The following markets have the largest Bitcoin transaction volume: US Dollar, Japanese Yen, South Korean Won, Euro, and Chinese Yuan. These currencies were determined by analyzing transaction volume online.[3] Note that Chinese Yuan was not on the top 5 currencies, but it was included because it controls a large number of mining compute power and is considered by people in the industry to be the leading country in mining.[4] In our analysis, we focus on the US Dollar, South Korean Won, Chinese Yuan, and Japanese Yen for the primary reason that our accuracy measure doesn't work well for Euro, since it spans a large timezone region.

In order to carry out such an analysis, we must first understand how Bitcoin transactions function. Bitcoin employs an unspent transaction output (UTXO) protocol, in which a user cannot exchange the amount in an unspent transaction for custom amounts, and they must spend the entire amount in one go. In that regard, Bitcoin transactions resemble how regular checks

[3] https://www.cryptocompare.com/coins/btc/analysis/USD
[4] https://www.buybitcoinworldwide.com/mining/pools/

work: you cannot give someone half a check, but you can cash it out and distribute the money in different outputs. A person can store and receive Bitcoin in public addresses for which he or she holds the private keys to. An address can store an infinite number of transactions, though it is not recommended to reuse addresses in case they are compromised. Users typically store multiple addresses in one ‘wallet’ for ease of usage. To further explain how UTXO works, we give an example of a user who has 10 Bitcoins stored in one address. When the user wants to spend the 10 Bitcoins, he or she must spend the entire amount. This does not mean, however, that they have to transfer full ownership of the unspent transaction to another user. Rather, it is possible to send fractions of the 10 Bitcoins to any number of recipients, including addresses that the user owns and even the initial address itself.

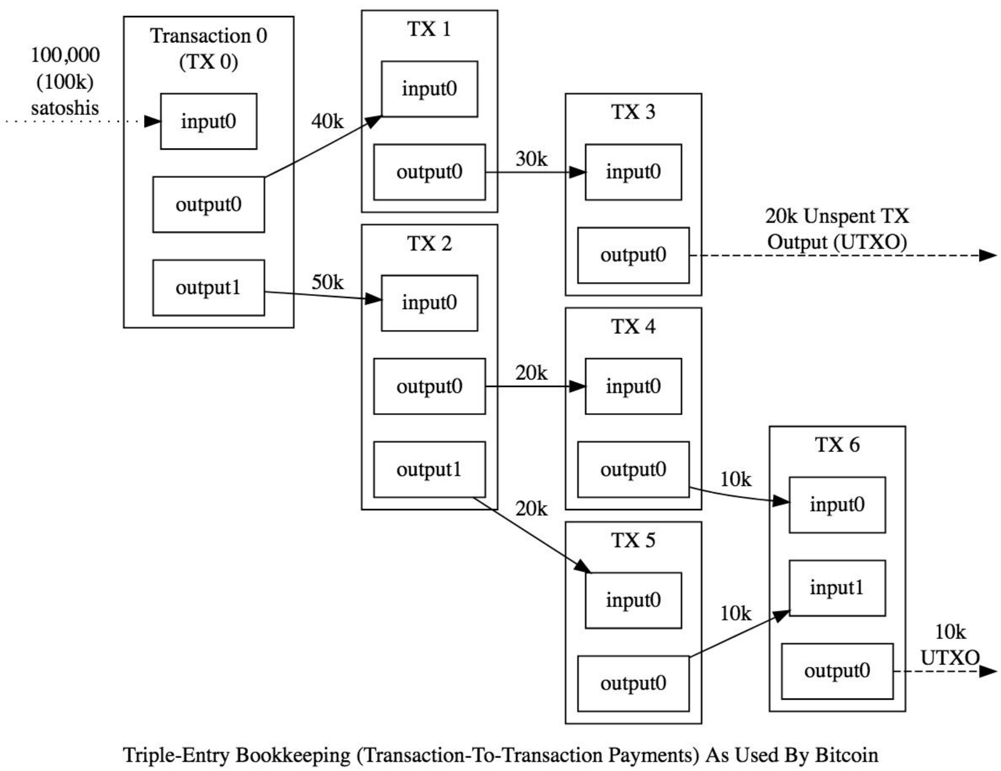

Figure 2: Example of Bitcoin UTXO being used.

Source: https://bitcoin.org/en/developer-guide#block-chain-overview

At the beginning, we wanted to look at the entirety of Bitcoin transactions in 2017. There were over 500,000 Bitcoin blocks in the chain in 2017 alone, which held information for 10,080,517 transactions. With the first implementation of our algorithm, it seemed obvious that such an analysis would require more advanced computing power and large number of hours of coding optimizations, which were beyond the scope of this project. With the starting code implementation, it would have required several days for the analysis to finish, which was not practical. Therefore, we decided to focus on a smaller time frame which would both make the analysis easier and also help answer an economic question of interest.

There is no question that the price of Bitcoin and the gains it made this year has caught the attention of investors from institutional to layman traders. The price of Bitcoin has gone through several rallies, especially in 2017, and one particularly significant period was between December 4 to December 9, 2017. Over that timeframe, the price of Bitcoin spiked from $11,616 to $16,057, a 38% increase. The price went on to increase to a peak of around $20,000 in the days following December 9th before correcting back to lower amounts. An exchange rate analysis of this period would enable us to gain insight into which fiat currency markets contributed the most to the Bitcoin price rally.

Figure 3: Bitcoin Price Chart, 2013 – 2018. The peak price was reached in December 2017.
Source: http://coinmarketcap.com

Data Collection

We compiled a dataset of average daily prices of Bitcoin in more than 20 currencies. The data was retrieved from Investing.com, which gets data from major exchanges and averages them to determine the price at a given instance.[5] The frequency of the data we took was daily prices (at midnight), and we filtered the datasets to only include days in 2017. We stored the data using the Python Pandas framework. More information can be found in the project code, linked in the Appendix.

Heuristics

There were two primary heuristics that were used in this analysis, and we call them the whole banknote amount heuristic and the time zone check ('operating hours') heuristic. The banknote amount heuristic is an assumption that when people purchase Bitcoin or use Bitcoin to

[5] https://www.investing.com/crypto/bitcoin/

purchase something, then they will do so in a whole banknote amount. That is to say, if someone noticed that the price of Bitcoin was going up and they had just received their paycheck, then our heuristic says that they are more likely to purchase a whole banknote amount. That is, you are more likely to invest $200 (2x $100 bills) in Bitcoin than $171.62 for instance. For the whole banknote amount, we use different values for each currency, but we primarily check to see if the amount is divisible by 10, 20, 50, or 100 (or just 10 because all the other numbers are divisible by 10). The assumption also holds if someone is using Bitcoin as a form of payment, due to the way that businesses leverage techniques such as psychological pricing, where things are more likely to be closer to the nearest $10 and priced at $9.99 instead of $10. The second heuristic used is checking whether a transaction happened within a window of operating hours from 9am to 11:59pm of the countries that use these currencies. The main idea here is that there will be more people awake during the day, so the chances of carrying out transactions increases. For regions that span multiple time zones, the bounds were defined as shown in Table 1 below. For example, in the United States, the bounds were expanded to account for Pacific Standard Time and Eastern Standard Time.

Country (Cities of Reference)	[Lower Bound, Upper Bound] (UTC Hours)
United States (New York, San Francisco)	4, 16
China (Beijing)	1, 15
Japan (Tokyo)	0, 14
South Korea (Seoul)	0, 14

Table 1: ‘operating hours’ for different countries, given in UTC hours.

Heuristics Limitations

The heuristics defined above are meant to be approximations of reality and not accurate representations of it. That is to say, there's no guarantee that no one will transact in non-whole banknote amounts of Bitcoin or that no one will purchase with Bitcoin during 'non-operating hours,' but what these heuristics give us is the ability to speculate about the nature of the transactions, since otherwise we would have no way to determine whether a transaction is carried out in US Dollars or in Japanese Yen. Nevertheless, the heuristics have limitations, which we address in this section.

The whole banknote amount heuristic is a strong assumption about the way people transact. There is no strong evidence backing the claim, and a leap of faith is required to jump from the argument of psychological pricing made earlier to the hypothesis that people transact in whole banknotes. In addition, another limitation is that our algorithm uses the price data at midnight, meaning that when we try to back out the amount from the exchange rate there is an inaccuracy because the rate was not instantaneous. Moreover, there is no data field for a Bitcoin transaction time on the blockchain, so even though a user may submit a transaction, it may not get processed until months later, depending on the transaction fee that the user is willing to pay. Therefore, until a transaction is processed (which takes around 60 minutes for the blockchain to confirm), a transaction is subject to change the time to confirmation and the instability of Bitcoin prices. This feature (or bug) of the Bitcoin transaction system means that we may never know for sure what the exchange rate was when someone placed a transaction. Finally, the 'operating hours' heuristic has the limitation that there's nothing stopping people from trading outside those hours. Since markets are open 24/7, someone may be closely following the price and place a trade late at night. There is also the possibility of algorithmic traders and pre-programmed trades such as stop-loss orders that several online exchanges offer.

Algorithm

The algorithm that we used to carry out our analysis looped through all the blocks in our defined range. After that, it looked at each transaction in the block, and in each transaction, it looked at all the unspent outputs. For each unspent output, we try out each of our currencies, check to see if any of them is a whole banknote amount, and inspect the time of the transaction block. If the two heuristic tests pass, then we consider this transaction to have been carried out in the currency we are using. Otherwise, we return False, and we don't count it as a success.

For every block, for every transaction in that block:

- Find exchange rate of best txn in utxo, where best is defined as:
  - If a multiple of whole banknote amount and in 'operating hours', then True
- If no fit found in all utxo outputs, then return False

Figure 4: Pseudocode of the exchange rate analysis algorithm

Results

We ran the model described above on 4 currencies that we decided to study, because they typically have the highest level of Bitcoin transaction volume on major exchanges. On Wednesday May 16, for instance, the level of transaction volume was very high for US markets, followed by Japan, and South Korea. USDT is US Dollar Tether, which is another cryptocurrency that is pegged to the US Dollar, and every Tethercoin is backed by $1 in the parent company bank accounts. It serves as a connector between the cryptocurrency world and fiat currencies, and it is very popular among non-US investors because it gives them the stability of the US Dollar. Our analysis, hence, chose to focus on the Japanese Yen, the US Dollar, the South Korean Won, and the Chinese Yuan. Even though the Yuan is not on the top-ten list, China is a large hub for Bitcoin and other cryptocurrency miners.[6] Therefore, it would be interesting to see how often Chinese investors and users trade, and if they contributed to the spike in price in early December 2017.

Bitcoin (BTC) Volume by Currency

Ƀ 249,826.70

#	Currency	Volume 24H	Volume 24H TO	Share
1	USD	Ƀ 82,060.27	$ 683,429,848.04	32.85%
2	JPY	Ƀ 71,734.73	¥ 67,547,154,038.91	28.71%
3	USDT	Ƀ 58,347.44	USDT 484,467,229.84	23.36%
4	KRW	Ƀ 15,652.51	₩ 145,325,844,370.95	6.27%
5	EUR	Ƀ 13,511.01	€ 95,149,907.09	5.41%
6	GBP	Ƀ 1,990.40	£ 12,269,982.52	0.80%
7	PLN	Ƀ 1,549.86	zł 46,766,899.78	0.62%
8	AIC*	Ƀ 1,382.21	AIC* 12,621,151.70	0.55%
9	CAD	Ƀ 542.58	CAD 5,609,842.47	0.22%
10	QC	Ƀ 485.98	QC 26,531,999.32	0.19%

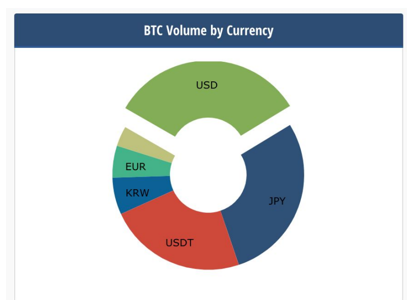

Figure 5: Bitcoin trading transaction volumes on May 16, 2018.
Source: https://www.cryptocompare.com/coins/btc/analysis/USD

The results of the analysis, shown in Table 2 below, show that the currencies we studied contributed to around 70.7% of trading in the period of study. If our heuristics are accurate, then this would show that trading was active in regions where the Dollar, Yen, and Yuan are used. Trading in Won was also active, albeit at a lower level. One thing to keep in mind is that the transactions that we studied are ones that happened on the chain, as opposed to off-chain transactions that are placed within an exchange. Transactions that hit the Bitcoin blockchain are more expensive than those which can be facilitated by exchanges when they match buyers and

[6] https://www.aljazeera.com/indepth/inpictures/world-chinese-bitcoin-mining-180116112117869.html

sellers in their markets. Otherwise, the trades incur transaction fees that are paid to miners. The transaction volume shown in Figure 5 above captures trading activity which happens off-the-chain and on exchange markets. Our analysis, on the other hand, tries to infer trading activity by fiat currency on-the-chain; therefore, it would be impossible to verify the authenticity of the numbers in Table 2, and the only way to critique the analysis and come up with a better one is by changing the heuristics or adding new ones.

Currency	% of total transactions
Chinese Yuan	20.5%
Japanese Yen	19.9%
US Dollar	18.3%
South Korean Won	12%

Table 2: Results of exchange rate analysis.

The analysis shows that the majority of the trading activity came from Chinese traders, followed by Japanese and then American users. The percentage of American traders was lower than chinese, though still significant. From this data, we can conclude that South Korean users are more likely to have used Bitcoin between December 4 to 9 for non-investing activity, since they didn't have large transaction volume as compared with US, Chinese, and Japanese counterparts.

Mining Analysis

We were interested in capturing the size of the Bitcoin mining market because it enables researchers to study the type of industry it is and analyze how much profit miners are making. To do so, we ran a query on the Bitcoin blockchain to see the total number of Bitcoins that miners have accumulated. Miners gain Bitcoins from two main sources: Coinbase transactions and mining fees. When miners are trying to add a block to the blockchain, they typically choose the transactions that have the highest associated fees and add them to the block that they are trying to mine. These fees are then transferred to the miners, which stand to gain from facilitating users' transactions. The other source of income is the Coinbase transaction, which is the inaugural transaction of any block. In this transaction, a miner transfers ownership of the mining reward to an address that the miner holds. Currently, the mining reward is 12.5 Bitcoins, but the number decreases with time, until it becomes negligible at which point miners get all their income from transaction fees. The creator of Bitcoin assumed that when the mining reward disappears, the price of Bitcoin would be high enough that transaction fees would be sufficient to sustain mining.

We ran a script and found that in 2017, miners made exactly 900,033.77648971 Bitcoins from coinbase transactions and mining fees. We also averaged the price of Bitcoin over 2017 and found that it was $4049.504793, making the value of the Bitcoins that they made on average around $3.65 billion. Putting a value on the market size of mining is important, because of the huge costs associated with mining. It is estimated that mining today takes up as much energy as the entire consumption of Nigeria.[7] With tools like Blocksci, the analysis of the size of this market becomes easier, and it enables miners to estimate whether they can produce with a profit, after they can approximate what size of the market they can capture with their hashing rate and the power of their computers.

---

[7] https://www.technologyreview.com/s/609480/bitcoin-uses-massive-amounts-of-energybut-theres-a-plan-to-fix-it/

Conclusion

The analysis we carried out showed that in the time period starting December 4 to December 9, 2017, which witnessed a 38% surge in the price of Bitcoin, market players from the US Dollar, Japanese Yen, South Korean Won, and Chinese Yuan contributed 18.3%, 19.9%, 12%, and 20.5% of the total market transactions respectively. These results cannot be independently verified, but if we had access to historical data on Bitcoin transaction volume on major exchanges, then we can do a comparison between on-chain versus off-chain transactions. Given that the accuracy of the method that we developed is hard to verify, then it should not serve as a sole indicator of market activity. This is the first attempt to try to classify on-chain market data, and opens up the door to other questions that can be raised from analyzing the public information available on the Bitcoin blockchain. For instance, given the fact that US Dollar traders transacted less in the period we studied, can it be said that due to the lower level of activity, US-based traders are using Bitcoin as a peer-to-peer payments system rather than as a vehicle of investment?

We also investigated the size of the Bitcoin mining industry, and found that miners in 2017 made upward of $3.65 bn on average. Having this information at hand enables researchers to study the mining industry and answer questions about whether it exhibits traits of an oligopoly, monopoly, or a perfectly competitive market.

Acknowledgements

- The Blocksci library was installed on a server provided by my friend Avery Lamp, whom I'd like to thank for all the technical support he provided throughout this project.
- I would also like to thank Professor Wolitzky for all the input he gave as I was writing this paper.

References

- https://bitcoin.org/bitcoin.pdf
- https://www.coindesk.com/price/
- https://www.cryptocompare.com/coins/btc/analysis/USD
- https://www.buybitcoinworldwide.com/mining/pools/
- https://bitcoin.org/en/developer-guide#block-chain-overview
- https://www.investing.com/crypto/bitcoin/
- http://coinmarketcap.com
- https://www.aljazeera.com/indepth/inpictures/world-chinese-bitcoin-mining-180116112117869.html
- https://www.technologyreview.com/s/609480/bitcoin-uses-massive-amounts-of-energybut-theres-a-plan-to-fix-it/

Appendix

Link to Code: https://github.com/itinawi/bitcoin_fiat_analysis

The analysis code can be found under the file named "14.18.ipynb"

The data used for this project can be found under the folder named "more_rates"